

Le Frido 2021,
volume 1
Laurent Claessens

Plusieurs extensions et versions de ce livre.

1. La version courante, régulièrement mise à jour et qui deviendra petit à petit le Frido 2022.
Téléchargeable sur

<https://laurent.claessens-donadello.eu/pdf/lefrido.pdf>

2. La version la plus complète, contenant des exercices ainsi que de la mathématique de plus haut niveau :

<https://laurent.claessens-donadello.eu/pdf/giulietta.pdf>

3. Et bien entendu les sources $\text{\LaTeX}$

<https://github.com/LaurentClaessens/mazhe>

Copyright 2011-2021 Laurent Claessens, and many contributors. A complete list could be retrieved from the git log.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the chapter entitled “GNU Free Documentation License”.

(c) 2015 David Revoy pour les illustrations de couverture CC-BY,
<https://www.peppercarrot.com/>

ISBN : 979-10-97085-26-1

Thèmes

Ceci est une sorte d'index thématique.

1 : Cardinalité	41 : transformée de Fourier
2 : tribu, algèbre de parties, λ -systèmes et co.	42 : méthode de Newton
3 : théorie de la mesure	43 : méthodes de calcul
4 : intégration	44 : espaces vectoriels
5 : suites et séries	45 : valeurs propres, définie positive
6 : polynôme de Taylor	46 : norme matricielle, norme opérateur et rayon spectral
7 : normes	47 : série de matrices
8 : caractérisations séquentielles	48 : rang
9 : topologie produit	49 : extension de corps et polynômes
10 : espaces métriques, normés	50 : décomposition de matrices
11 : gaussienne	51 : systèmes d'équations linéaires
12 : compacts	52 : formes bilinéaires et quadratiques
13 : densité	53 : arithmétique modulo, théorème de Bézout
14 : espaces de fonctions	54 : polynômes
15 : fonctions Lipschitz	55 : zoologie de l'algèbre
16 : formule des accroissements finis	56 : invariants de similitude
17 : limite et continuité	57 : réduction, diagonalisation
18 : suite de fonctions	58 : endomorphismes cycliques
19 : dérivation	59 : déterminant
20 : différentiabilité	60 : polynôme d'endomorphismes
21 : Morphismes et compagnie	61 : exponentielle
22 : points fixes	62 : types d'anneaux
23 : Intégration sur des variétés	63 : sous-groupes
24 : permuter des limites	64 : groupe symétrique
25 : applications continues et bornées	65 : action de groupe
26 : inégalités	66 : classification de groupes
27 : connexité	67 : produit semi-direct de groupes
28 : suite de Cauchy, espace complet	68 : théorie des représentations
29 : application réciproque	69 : isométries
30 : déduire la nullité d'une fonction depuis son intégrale	70 : caractérisation de distributions en probabilités
31 : équations différentielles	71 : théorème central limite
32 : injections	72 : lemme de transfert
33 : logarithme	73 : probabilités et espérances conditionnelles
34 : inversion locale, fonction implicite	74 : dénombrements
35 : convexité	75 : enveloppes
36 : fonction puissance	76 : équations diophantiennes
37 : dualité	77 : changement de variables
38 : opérations sur les distributions	78 : techniques de calcul
39 : convolution	
40 : séries de Fourier	

Thème 1 : Cardinalité Le Frido ne définit pas la notion de nombre cardinal ; ça nous mènerait trop loin. Au lieu de cela, nous allons nous contenter des notions d'équipotence, surpotence et subpotence, et démontrer un certain nombre de résultats en utilisant sans retenue le lemme de Zorn 1.17.

- (1) Définition d'équipotence, surpotence et subpotence, notations $A > B$ et $A \approx B$, définition 1.93.
- (2) Toute partie d'une ensemble fini est finie, lemme 1.97.

- (3) Si A est un ensemble fini ou dénombrable, alors il existe une surjection $\mathbb{N} \rightarrow A$, lemme 1.107.
- (4) Si A est un ensemble infini et si $f: A \rightarrow B$ est une application injective, alors $f(A)$ est infini, proposition 1.101.
- (5) Toute partie infinie de $\mathbb{N}$ est dénombrable, proposition 1.108
- (6) Une bijection $\mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$, proposition 1.111.
- (7) Une décomposition de $\mathbb{N}$ en une infinité de parties équipotentes à $\mathbb{N}$, corolaire 1.112.
- (8) Si il existe une surjection $\mathbb{N} \rightarrow A$, alors A est fini ou dénombrable, lemme 1.113.
- (9) Une union dénombrable d'ensembles finis ou dénombrables est finie ou dénombrable, proposition 1.114
- (10) Tout ensemble infini contient une partie en bijection avec $\mathbb{N}$, proposition 1.117.
- (11) Toute partie d'un ensemble fini est finie, et toute partie d'un ensemble dénombrable est finie ou dénombrable, proposition 1.118.
- (12) Si $A \geq B$ et $B \geq A$, alors $A \approx B$, théorème de Cantor-Schröder-Bernstein 1.121
- (13) Le théorème de Cantor 1.124 dit qu'il n'existe pas de surjection d'un ensemble vers son ensemble des parties. On en déduit qu'il n'existe pas d'ensemble contenant tous les ensembles (corolaire 1.126).
- (14) Si A est infini et si $A \geq B$, alors $A \approx A \cup B$ par le lemme 1.128.
- (15) Si S est un ensemble infini alors il existe une bijection $\varphi: \{0, 1\} \times S \rightarrow S$, proposition 1.129.
- (16) Si A est infini, alors $A \times \mathbb{N} \approx A$, proposition 1.131.
- (17) Si A est infini et si $B < A$, alors $A \setminus B \approx A$, lemme 1.133.
- (18) Si A est infini, alors $A \approx A \times A$, théorème 1.137.

Il y a aussi des résultats de cardinalité autour des extensions de corps.

- (1) Si $\mathbb{K}$ est un corps infini, alors $\mathbb{K}[X] \approx \mathbb{K}$.
- (2) Le théorème de Steinitz 6.127 affirme que tout corps admet une unique clôture algébrique. La preuve utilise pas mal de cardinalité ainsi que le lemme de Zorn 1.17.

Thème 2 : tribu, algèbre de parties, λ -systèmes et co. Il existe des centaines de notions de mesures et de classes de parties.

- (1) Le plus souvent lorsque nous parlons de mesure est que nous parlons de mesure positive, définition 14.20 sur un espace mesuré avec une tribu, définition 14.1.
- (2) Une mesure extérieure est la définition 14.13
- (3) Une algèbre de partie : définition 14.16. Une mesure sur une algèbre de parties : définition 14.14. L'intérêt est que si on connaît une mesure sur une algèbre de parties, elle se prolonge en une mesure sur la tribu engendrée par le théorème de prolongement de Hahn 14.68.
- (4) Un λ -système : définition 14.30.
- (5) Une mesure complexe : définition 14.204.

En théorie de l'intégration, si X est une partie de $\mathbb{R}^n$, la convention est de considérer des fonctions

$$f: (X, \mathcal{L}eb(X)) \rightarrow (\mathbb{R}, \mathcal{B}or(\mathbb{R})).$$

Voir les points 14.107 et 14.151 pour les conventions à ce propos.

À propos d'applications mesurables :

- (1) Définition d'une application mesurable, définition 14.41.
- (2) Une fonction continue est borélienne, théorème 14.49.

À propos de tribu induite :

- (1) Définition 14.6.
- (2) Les boréliens induits sont bien les boréliens de la topologie induite : $\mathcal{B}or(Y) = \mathcal{B}or(X)_Y$, théorème 14.50.

Thème 3 : théorie de la mesure

Mesure À propos de mesure.

- (1) Mesure positive, mesure finie et σ -finie, c'est la définition 14.20.
- (2) Le produit de tribus est donné par la définition 14.113,
- (3) Produit d'une mesure par une fonction, définition 14.191.
- (4) le produit d'espaces mesurés est donné par la définition 14.214.
- (5) Mesure de Lebesgue sur $\mathbb{R}$, définition 14.128.
- (6) Une partie de $\mathbb{R}$ non mesurable au sens de Lebesgue : l'exemple 14.142.
- (7) Mesure de Lebesgue sur $\mathbb{R}^N$, définition 14.216.
- (8) Mesure à densité, définition 14.191.

Théorèmes d'approximation Il est important de pouvoir approcher des fonctions continues ou L^p par des fonctions étagées, sinon on ne parvient pas à faire tourner la machine de l'intégration de Lebesgue.

- (1) Si $(S, \mathcal{A}, \mu)$ est un espace mesuré et si $f: S \rightarrow [0, +\infty]$ est une fonction mesurable, le théorème fondamental d'approximation 14.106 dit qu'il existe une suite croissante de fonctions étagées qui converge vers f .
- (2) Les fonctions simples sont denses dans L^p , proposition 27.46.
- (3) Encadrement d'un borélien A par un fermé F et un ouvert V par le lemme 14.207 : $F \subset A \subset V$ avec $\mu(V \setminus F) < \epsilon$.
- (4) Approximation L^p de la fonction caractéristique d'un borélien par une fonction continue par le théorème 14.209.

Thème 4 : intégration À propos d'intégration.

L'ordre dans lequel les choses sont faites — Nous commençons par considérer des fonctions $f: \Omega \rightarrow [0, +\infty]$ dans la définition 14.152.

— Nous donnerons ensuite quelques propriétés restreintes aux fonctions à valeurs positives, par exemple

- (1) La convergence monotone 14.162,
- (2) Lemme de Fatou 14.166.
- (3) (presque) linéarité pour les fonctions positives, théorème 14.167.

— La définition pour les fonctions à valeurs dans $\mathbb{R}$ puis $\mathbb{C}$ est 14.170.

— Pour les fonctions à valeurs dans un espace vectoriel, c'est la définition 14.179.

Quelque résultats (1) Intégrale associée à une mesure, définition 14.152

- (2) L'existence d'une primitive pour toute fonction continue est le théorème 12.341.
- (3) La définition d'une primitive est la définition 12.151.
- (4) Primitive et intégrale, proposition 14.241.
- (5) Intégrale impropre, définition 14.253.

Intégrale et mesure (1) L'intégrale de la fonction 1 donne la mesure : $\int_B 1 d\mu = \mu(B)$, c'est le lemme 14.159.

(2) Le théorème de Radon-Nikodym 14.200 donne une densité pour certaines mesures.

(3) Le produit d'une mesure par une fonction donné par la définition 14.191 introduit aussi une densité : $(w \cdot \mu)(A) = \int_A w d\mu$.

Autre résultats (1) Si $A, B \subset \Omega$ sont des parties disjointes, alors $\int_{A \cup B} f = \int_A f + \int_B f$, proposition 14.176.

(2) La σ -additivité dénombrable, $\int_{\bigcup_i A_i} f d\mu = \sum_{i=0}^{\infty} \int_{A_i} f d\mu$ est dans les propositions 14.189 et 14.190.

Thème 5 : suites et séries

Suites Les suites réelles sont en général dans la proposition 10.22 et ce qui s'ensuit. Cette proposition est souvent prise comme définition lorsque seules les suites réelles ne sont considérées.

- (1) Les suites adjacentes, c'est la définition 10.35.
- (2) Les séries alternées, théorème 11.131. Il s'agit de dire que $\sum_{k=0}^{\infty} (-1)^k a_k$ converge quand a_k est décroissante et tend vers zéro.
- (3) Le concept de suite adjacente sert à étudier la série de Taylor de $\ln(x+1)$, voir le lemme 15.89 et ce qui l'entoure.
- (4) La définition de la convergence absolue est la définition 11.108.
- (5) Une suite réelle croissante et majorée converge, proposition 10.31.
- (6) Toute suite dans un compact admet une sous-suite convergente, théorème 7.201.
- (7) Pour tout réel, il existe une suite croissante de rationnels qui y converge, proposition 10.15.

Produit de Cauchy (1) Dans une algèbre normée, proposition 11.119,

- (2) Dans $\mathbb{C}$, théorème 15.26.

Calcul de suites (1) Somme : $x_n + y_n \rightarrow x + y$ est la proposition 10.26.

Série Les séries sont en général dans la section 11.6.

- (1) Quelques séries usuelles en 11.7.3 : série harmonique, géométrique, de Riemann, et la mythique arithmético-géométrique.
 - (1a) La série est associative : $\sum_k (a_k + b_k) = \sum_k a_k + \sum_k b_k$. C'est la proposition 11.117.
 - (1b) La série harmonique diverge : $\sum_k \frac{1}{k} = \infty$, exemple 11.125.
 - (1c) La série géométrique : $\sum_{k=0}^N q^k = \frac{1-q^{N+1}}{1-q}$, proposition 11.126.
 - (1d) Une autre cool série : $\sum_{k=1}^N \frac{1}{k(k+1)} = \frac{N}{N+1}$, lemme 11.130.
- (2) Critère des séries alternées, théorème 11.131.
- (3) Convergence d'une série implique convergence vers zéro du terme général, proposition 11.115.
- (4) Dans une algèbre normée : $(\sum_{k=0}^{\infty} a_k)b = \sum_{k=0}^{\infty} (a_k b)$, proposition 11.118.
- (5) Produit de Cauchy : théorème 15.26 et proposition 11.119.

Sommes infinies En ce qui concerne les sommes finies, la notation $\sum_{i=1}^N$ est définie en 1.68. Pour permuter les termes d'une somme avec un élément du groupe symétrique, nous avons la proposition 1.207.

Voici quelques résultats à propos de sommes infinies.

- (1) Une somme indexée par un ensemble quelconque est la définition 11.157.
- (2) La définition de la somme d'une infinité de termes est donnée par la définition 11.105.
- (3) Une somme de termes positifs indexée par un ensemble indénombrable est toujours infinie par le lemme 11.164.
- (4) si la série converge, on peut regrouper ses termes sans modifier la convergence ni la somme (associativité) ; Pour les sommes infinies l'associativité et la commutativité dans une série sont perdues. Néanmoins, il subsiste que
 - (4a) si la série converge absolument, on peut modifier l'ordre des termes sans modifier la convergence ni la somme (commutativité, proposition 11.154).
- (5) Permuter une somme infinie avec une application linéaire : $f(\sum_{i \in I} v_i) = \sum_{i \in I} f(v_i)$, c'est la proposition 11.171.

Série entières (1) Rayon de convergence, définition 15.11.

- (2) Convergence absolue à l'intérieur du rayon de convergence, lemme d'Abel 15.15.
- (3) La fonction définie par la série entière $z \mapsto \sum_{k=0}^{\infty} a_n z^n$ est holomorphe dans son disque de convergence par la proposition 15.36.
- (4) La série entière pour $\frac{1}{1-z^k}$ et pour $\frac{1}{\omega-z}$ et pour $\frac{1}{(\omega-z)^k}$ sont dans le lemme 15.41.

Thème 6 : polynôme de Taylor

Énoncés Il existe de nombreux énoncés du théorème de Taylor, et en particulier beaucoup de formules pour le reste.

- (1) Énoncé : théorème 12.394.
- (2) Une majoration du reste est dans le théorème 15.47
- (3) De classe C^2 sur $\mathbb{R}^n$, proposition 12.401.
- (4) Avec un reste donné par un point dans $]x, a[$, proposition 12.405.
- (5) Avec reste intégral, proposition 20.151 et théorème 20.148 pour le cas simple $\mathbb{R} \rightarrow \mathbb{R}$.
- (6) Le polynôme de Taylor généralise à l'utilisation de toutes les dérivées disponibles le résultat de développement limité donné par la proposition 12.122.
- (7) Pour les fonctions holomorphes, il y a le théorème 26.28 qui donne une série de Taylor sur un disque de convergence.

Utilisation Des polynômes de Taylor sont utilisés pour démontrer des théorèmes par-ci par-là.

- (1) Il est utilisé pour justifier la méthode de Newton autour de l'équation (34.95).
- (2) On utilise pas mal de Taylor dans les résultats liant extrémum et différentielle/hessienne. Par exemple la proposition 17.72.

Quelques développements Voici quelques développements limités à savoir. Ils sont calculables en utilisant la formule de Taylor-Young (proposition 12.410).

$$\begin{aligned}
 e^x &= \sum_{k=0}^n \frac{x^k}{k!} + x^n \alpha(x) && \text{ordre } n, \text{ proposition 15.84} \\
 \cos(x) &= \sum_{k=0}^p \frac{(-1)^k x^{2k}}{(2k)!} + x^{2p+1} \alpha(x) && \text{ordre } 2p+1, \text{ proposition 18.63} \\
 \sin(x) &= \sum_{k=0}^p \frac{(-1)^k x^{2k+1}}{(2k+1)!} + x^{2p+2} \alpha(x) && \text{ordre } 2p+1, \text{ proposition 18.63} \\
 \ln(1+x) &= \sum_{k=1}^n \frac{(-1)^{k+1}}{k} x^k + \alpha(x) x^n && \text{ordre } n, \text{ proposition 15.88} \\
 \ln(1+x) &= \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} x^k && \text{exact proposition 15.90} \\
 \ln(2) &= \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} && \text{exact proposition 15.90} \\
 (1+x)^l &= \sum_{k=0}^l \binom{l}{k} x^k && \text{exact si } l \text{ est entier.} \\
 (1+x)^\alpha &= 1 + \sum_{k=1}^n \frac{\alpha(\alpha-1)\dots(\alpha-k+1)}{k!} x^k + x^n \alpha(x) && \text{ordre } n.
 \end{aligned}$$

Dans toutes ces formules, la fonction $\alpha: \mathbb{R} \rightarrow \mathbb{R}$ vérifie $\lim_{t \rightarrow 0} \alpha(t) = 0$.

Le développement limité en 0 d'une fonction paire ne contient que les puissances de x d'exposant paire. Voir comme exemple le développement de la fonction cosinus.

Thème 7 : normes

Définition Espace vectoriel normé : définition 7.118.

Équivalence de norme (1) Définition de l'équivalence de norme 11.48.

- (2) La proposition 11.50 sur l'équivalence des normes $\|\cdot\|_2$, $\|\cdot\|_1$ et $\|\cdot\|_\infty$ dans $\mathbb{R}^n$.

- (3) En général pour les normes $\|\cdot\|_p$, il y a des inégalités dans 12.383 et 17.98 ; voir aussi le thème 7.
- (4) La proposition 17.108 donne l'inégalité $\|x\|_q \leq n^{\frac{1}{q}-\frac{1}{p}} \|x\|_p$ dès que $0 < q < p$.
- (5) Toutes les normes sur un espace vectoriel de dimension finie sont équivalentes par le théorème 11.52.
- (6) Montrer que le problème $a - b$ est stable dans l'exemple 34.27.
- (7) La proposition 11.70 donnant $\rho(A) \leq \|A\|$ utilise l'équivalence de toutes les normes sur un espace vectoriel de dimension finie (théorème 11.52.).

Norme opérateur et d'algèbre voir le thème 46.

Thème 8 : caractérisations séquentielles

- (1) Fonction séquentiellement continue, définition 7.82.
- (2) La continuité implique la continuité séquentielle, proposition 7.84 et corolaire 7.85.
- (3) Pour des espaces métriques, la continuité séquentielle d'une fonction est équivalente à la continuité, proposition 7.164. Une version spéciale pour $\mathbb{R}^m$ est donnée par le théorème 12.171.

Thème 9 : topologie produit

- (1) La définition de la topologie produit est 7.15.
- (2) Pour les espaces vectoriels normés, le produit est donné par la définition 7.128.
- (3) L'équivalence entre la topologie de la norme produit et la topologie produit est le lemme 7.128.
- (4) Quand V et W sont des espaces métriques, la topologie considérée sur $V \times W$ est celle de la définition 7.128. C'est à la fois la topologie de la norme produit et la topologie produit.
- (5) La convergence dans un espace vectoriel est si et seulement si il y a convergence composante par composante, proposition 7.40.

Thème 10 : espaces métriques, normés

- (1) Un espace métrique est un espace muni d'une distance, définition 7.98.
- (2) La distance entre un point et un ensemble est la définition 7.112.
- (3) Le théorème-définition 7.99 donne la topologie sur un espace métrique en disant que les boules ouvertes sont une base de la topologie (définition 7.2).
- (4) La définition de la convergence d'une suite est la définition 7.13.
- (5) Dans un espace vectoriel normé, une application est continue si et seulement si elle est bornée, proposition 11.73.
- (6) Un espace vectoriel topologique qui possède en tout point une base dénombrable de topologie accepte une distance, théorème 7.193.

Thème 11 : gaussienne

- (1) Le calcul de l'intégrale

$$\int_{\mathbb{R}} e^{-x^2} dx = \sqrt{\pi}$$

est fait de deux façons dans l'exemple 14.270. Dans les deux cas, le théorème de Fubini 14.267 est utilisé.

- (2) Le lemme 29.22 calcule la transformée de Fourier de $g_\epsilon(x) = e^{-\epsilon\|x\|^2}$ qui donne $\hat{g}_\epsilon(\xi) = \left(\frac{\pi}{\epsilon}\right)^{d/2} e^{-\|\xi\|^2/4\epsilon}$.
- (3) Le lemme 29.23 donne une suite régularisante à base de gaussienne.
- (4) Elle est utilisée pour régulariser une intégrale dans la preuve de la formule d'inversion de Fourier 29.26

Thème 12 : compacts

Propriétés générales Quelques propriétés de compacts.

- (1) La définition d'un ensemble compact est la définition 7.50.
- (2) Ne pas confondre le compactifié d'Alexandrov 7.68 avec la droite réelle achevée 12.25.
- (3) Si M est un compact de $A \times B$, alors $M \subset K \times L$ où K est compact de A et L de B , proposition 7.66.
- (4) Un fermé dans un compact est compact, lemme 7.63
- (5) Tout compact d'un espace topologique séparé est fermé, lemme 7.63(2).
- (6) Dans un espace vectoriel réel de dimension finie, les compacts sont les fermés bornés par le théorème 10.20.
- (7) Le théorème de Borel-Lebesgue 10.17 dit qu'un intervalle¹ de $\mathbb{R}$ est compact si et seulement si il est de la forme $[a, b]$.
- (8) Théorème des fermés emboîtés dans le cas compact, corolaire 7.60. À ne pas confondre avec celui dans le cas des espaces métrique, théorème 7.209.
- (9) L'image d'un compact par une fonction continue est un compact, théorème 7.97.
- (10) Suites dans un compact
 - (10a) Toute suite dans un compact admet une sous-suite convergente, théorème 7.201.
 - (10b) Dans $\mathbb{R}^n$, toute suite dans un compact admet une sous-suite convergente, théorème 10.50. La démonstration de ce théorème est non seulement plus compliquée que le cas général, mais utilise en plus le cas dans $\mathbb{R}$; lequel cas n'est pas démontré de façon directe dans le Frido.
 - (10c) Un espace métrique est compact si et seulement si toute suite contient une sous-suite convergente. C'est le théorème de Bolzano-Weierstrass 7.108. La démonstration de ce théorème est indépendante.
- (11) Une fonction continue sur un compact est bornée et atteint ses bornes, théorème 7.110.
- (12) Une fonction continue sur un compact y est uniformément continue, théorème de Heine 12.77.

Produits de compacts À propos de produits de compacts. C'est un compact dans tous les cas métriques².

- (1) Les produits d'espaces métriques compacts sont compacts. Il s'agit du théorème de Tychonov que nous verrons ce résultat dans les cas suivants.
 - $\mathbb{R}$, lemme 10.19.
 - Produit fini d'espaces métriques compacts, théorème 7.225.
 - Produit dénombrable d'espaces métriques compacts, théorème 7.227.

Thème 13 : densité

- (1) Densité de $\mathbb{Q}$ dans $\mathbb{R}$, proposition 10.14.
- (2) Densité des polynômes dans $(C^0([0, 1]), \|\cdot\|_\infty)$, théorème de Bernstein 36.143.
- (3) Densité des polynômes dans $(C^0(I), \|\cdot\|_\infty)$ lorsque $I = [a, b]$, corolaire 36.144.
- (4) Densité de $\mathcal{D}(\mathbb{R}^d)$ dans $L^p(\mathbb{R}^d)$ pour $1 \leq p < \infty$, théorème 27.49.
- (5) Densité de $\mathcal{S}(\mathbb{R}^d)$ dans l'espace de Sobolev $H^s(\mathbb{R}^d)$, proposition 31.15.
- (6) Densité de $\mathcal{D}(\mathbb{R}^d)$ dans l'espace de Sobolev $H^s(\mathbb{R}^d)$, proposition 31.17.

Cela est utilisé pour le théorème de trace 31.19.

1. Définition 1.15.

2. Si vous connaissez des exemples non métriques de produits de compacts qui ne sont pas compacts, écrivez-moi.

- (7) Les applications étagées dans les applications mesurables (qui plus est avec limite croissante), théorème fondamental d'approximation 27.52.
- (8) Les fonctions continues à support compact dans $L^2(I)$, théorème 27.53.
- (9) Les polynômes trigonométriques sont denses dans $L^p(S^1)$ pour $1 \leq p < \infty$. Deux démonstrations indépendantes par le théorème 28.6 et le théorème 27.73.

Les densités sont bien entendu utilisées pour prouver des formules sur un espace en sachant qu'elles sont vraies sur une partie dense. Mais également pour étendre une application définie seulement sur une partie dense. C'est par exemple ce qui est fait pour définir la trace γ_0 sur les espaces de Sobolev $H^s(\mathbb{R}^d)$ en utilisant le théorème d'extension 17.123.

Comme presque tous les théorèmes importants, le théorème de Stone-Weierstrass possède de nombreuses formulations à divers degrés de généralité.

- Le lemme 12.332 le donne pour la racine carrée.
- Le théorème 12.338 donne la densité des polynômes dans les fonctions continues sur un compact.
- Le théorème 12.335 est une généralisation qui donne la densité uniforme d'une sous-algèbre de $C(X, \mathbb{R})$ dès que X sépare les points.
- Le théorème 12.336 donne le même résultat pour la densité dans $C(X, \mathbb{C})$.
- Le lemme 28.1 est une version pour les polynômes trigonométriques.
- Le lemme 12.332 est un cas particulier du théorème 12.338, mais nous en donnons une démonstration indépendante afin d'isoler la preuve de la généralisation 12.336. Une version pour les polynômes trigonométriques sera donnée dans le lemme 28.1.

Le théorème de Stone-Weierstrass est utilisé, entre autres nombreuses choses, pour prouver la densité des polynômes trigonométriques dans les fonctions continues sur S^1 , voir la proposition 27.90.

Thème 14 : espaces de fonctions En ce qui concerne les densités, voir le thème 13.

- (1) $C^\infty(A)$ est l'ensemble des fonctions de classe C^∞ sur A . Les éléments de $C^\infty(A)$ peuvent être à valeurs dans $\mathbb{R}$ ou dans $\mathbb{C}$ selon le contexte.
- (2) $\mathcal{D}(A)$ est l'ensemble des fonctions de classe C^∞ dont le support est un compact dans A .

Pour les ensembles $\mathcal{S}(A)$, $\mathcal{D}(A)$ et $L^p(A)$, les fonctions sont à valeurs dans $\mathbb{C}$. La raison est que, de toutes façons, le passage à la transformée de Fourier produit en général des fonctions à valeurs dans $\mathbb{C}$ même si les fonctions de départ sont à valeurs dans $\mathbb{R}$.

Topologie Les espaces de fonctions sont souvent munis de topologies définies par des semi-normes.

- (1) La topologie des semi-normes est la définition 7.233.
- (2) La définition 30.13 donne les topologies sur $C^\infty(\Omega)$, $\mathcal{D}(K)$ et $\mathcal{D}(\Omega)$.
- (3) La topologie *-faible sur $\mathcal{D}'(\Omega)$ est donnée par la définition 30.21.

L'espace $L^2([0, 2\pi])$ C'est un espace très important, entre autres parce qu'il est de Hilbert et est bien adapté à la transformée de Fourier.

- (1) Un rappel de la construction en 27.75.
- (2) Le produit scalaire $\langle f, g \rangle$ est donné en (27.386) et la base trigonométrique est (27.387).
- (3) La densité des polynômes trigonométriques dans $L^p(S^2)$ est le théorème 27.73 ou le théorème 28.6, au choix.
- (4) Une conséquence de cette densité est que le système trigonométrique est une base hilbertienne³ de L^2 par le lemme 27.114.

L'espace L^2 est discuté en analyse fonctionnelle, dans la section 27.5 et les suivantes parce que l'étude de L^2 utilise entre autres l'inégalité de Hölder 27.34.

Le fait que L^2 soit une espace de Hilbert est utilisé dans la preuve du théorème de représentation de Riesz 27.152.

3. Définition 25.26.

Thème 15 : fonctions Lipschitz

- (1) Définition : 12.276.
- (2) La notion de Lipschitz est utilisée pour définir la stabilité d'un problème, définition 34.26.

Thème 16 : formule des accroissements finis Il en existe plusieurs formes :

- (1) Une version adaptée aux espaces normés de dimension finie, avec hypothèse de différentiabilité, est le théorème 12.274. La formule $\|f(b) - f(a)\|_n \leq \sup_{x \in [a, b]} \|df_x\|_{\mathcal{L}(\mathbb{R}^m, \mathbb{R}^n)} \|b - a\|_m$.
- (2) Une version pour les dérivées partielles est dans le lemme 12.193. Pour rappel, la définition de la dérivation partielle est 12.180.
- (3) La formule $f(a + \epsilon e_i) = f(a) + \epsilon(\partial_i f)(a) + \epsilon\alpha(\epsilon)$, proposition 12.194.
- (4) L'existence de $c \in]a, b[$ tel que

$$f'(c) = \frac{f(b) - f(a)}{b - a} \quad (-2.2)$$

est le théorème des accroissements finis proprement dit. C'est le théorème 12.145.

- (5) Il existe un c entre a et b tel que

$$f(b) = f(a) + (b - a)(\partial_\beta f)(c) \quad (-2.3)$$

où $\beta = b - a$ est la proposition 12.192.

- (6) La formule $f(a + h) = f(a) + hf'(a) + \alpha(h)$ pour une fonction $\mathbb{R} \rightarrow \mathbb{R}$ en le théorème 12.122.
- (7) Une généralisation pour les intervalles non bornés : théorème 12.146.
- (8) Espaces vectoriels normés, théorème 11.216

Thème 17 : limite et continuité

- (1) Limite d'une fonction en un point : définition 7.70. Il n'y a pas unicité en général comme le montre l'exemple 7.35 dans un espace non séparé.
- (2) Caractérisation de la limite dans $\mathbb{R}$, proposition 12.1.
- (3) Unicité de la limite d'une suite dans un espace séparé : proposition 7.38. Unicité de la limite d'une fonction, toujours dans le cas d'un espace séparé : proposition 7.73.
- (4) La proposition 7.242 donne l'unicité de la limite dans le cas des espaces duaux pour la topologie *-faible. La proposition 7.73 nous dira qu'il y a unicité dès que l'espace d'arrivée est séparé.
- (5) Définition de la continuité d'une fonction en un point et sur une partie de l'espace de départ : définition 7.75.
- (6) Continuité sur une partie si et seulement si continue en chaque point, c'est le théorème 7.79.
- (7) Voir l'exemple 12.51 traité en détail pour la (non) continuité d'une fonction qui fait un saut en un point.
- (8) La fonction $f(x, y) = x + y$ est continue, lemme 10.27.

Thème 18 : suite de fonctions

- (1) Une limite uniforme de fonctions continues est continue, proposition 12.311.
- (2) Sous certaines hypothèses, si $f_i \rightarrow f$, alors $f'_i \rightarrow f'$, théorème 12.328.

Thème 19 : dérivation

- (1) Définition de la dérivée, définition 12.114.
- (2) Dérivée de fonction composée, proposition 12.136 dans le cas réel.
- (3) Dérivée partielle de fonction composée, théorème 12.262.
- (4) $f(\lambda x)' = \lambda f'(x)$, lemme 12.128.

Thème 20 : différentiabilité

Généralités (1) La différentielle est définie en général pour des espaces vectoriels normés par la proposition 11.194

- (2) Différentielle de fonction composée, formule $f(g \circ f)_a = dg_{f(a)} \circ df_a$, théorème 11.205.
- (3) Nous parlons de différentielle en dimension finie et donnons une interprétation géométrique en 12.19.1.
- (4) La recherche d'extrémums d'une fonction sur $\mathbb{R}^n$ passe par la seconde différentielle, proposition 17.72.
- (5) Lien entre différentielle seconde (hessienne) et convexité en la proposition 17.96 et le corolaire 17.98.
- (6) La différentielle est liée aux dérivées partielles par les formules données au lemme 12.212

$$df_a(u) = \frac{\partial f}{\partial u}(a) = \frac{d}{dt} \left[f(a + tu) \right]_{t=0} = \sum_{i=1}^m u_i \frac{\partial f}{\partial x_i}(a) = \nabla f(a) \cdot u. \quad (-2.4)$$

Je ne vous cache pas que cette suite d'égalités est une de mes préférées.

Différentielle et dérivées partielles À propos de fonctions de classe C^k , définition 11.195.

- (1) Une fonction est de classe C^1 si et seulement si ses dérivées partielles sont continues, théorème 12.255.
- (2) Une fonction est C^n si et seulement si ses dérivées partielles sont C^{n-1} , c'est le théorème 12.289.
- (3) Différentiabilité en un seul point si les dérivées partielles sont continues en ce point : proposition 12.253.

Fonctions composées À propos de la formule $d(f \circ g)_a = dg_{f(a)} \circ df_a$, il y a deux théorèmes très semblables.

- (1) Le théorème 11.205 insiste sur des hypothèses locales.
- (2) Le théorème 11.206 fait des hypothèses plus globales pour s'aléger l'esprit, mais fait une récurrence pour dire que $f \circ g$ est de classe C^r si f et g le sont.

Thème 21 : Morphismes et compagnie

- (1) Un morphisme est un concept algébrique. Il s'agit d'une application (pas spécialement inversible) qui préserve la structure.
- (2) Un homéomorphisme est continue d'inverse continue. C'est ce qu'on appelle un isomorphisme d'espaces topologiques. Définition 7.90.
- (3) Un difféomorphisme est différentiable d'inverse différentiable, définition 11.197.
- (4) Un C^k -difféomorphisme est une application C^k d'inverse C^k . Définition 11.197.

Thème 22 : points fixes

- (1) Il y a plusieurs théorèmes de points fixes.

Théorème de Picard 17.35 donne un point fixe comme limite d'itérés d'une fonction Lipschitz. Il aura pour conséquence le théorème de Cauchy-Lipschitz 17.41, l'équation de Fredholm, théorème 17.40 et le théorème d'inversion locale dans le cas des espaces de Banach 17.49.

Théorème de Brouwer qui donne un point fixe pour une application d'une boule vers elle-même. Nous allons donner plusieurs versions et preuves.

- (1a) Dans $\mathbb{R}^n$ en version C^∞ via le théorème de Stokes, proposition 20.35.
- (1b) Dans $\mathbb{R}^n$ en version continue, en s'appuyant sur le cas C^∞ et en faisant un passage à la limite, théorème 20.36.

- (1c) Dans $\mathbb{R}^2$ via l'homotopie, théorème 26.20. Oui, c'est très loin. Et c'est normal parce que ça va utiliser la formule de l'indice qui est de l'analyse complexe⁴.

Théorème de Markov-Kakutani 20.41 qui donne un point fixe à une application continue d'un convexe fermé borné dans lui-même. Ce théorème donnera la mesure de Haar 20.42 sur les groupes compacts.

Théorème de Schauder C'est une version valable en dimension infinie du théorème de Brouwer. Théorème 20.37

- (2) Pour les équations différentielles
- (2a) Le théorème de Schauder a pour conséquence le théorème de Cauchy-Arzela 20.38 pour les équations différentielles.
 - (2b) Le théorème de Schauder 20.37 permet de démontrer une version du théorème de Cauchy-Lipschitz (théorème 17.41) sans la condition Lipschitz, mais alors sans unicité de la solution. Notons que de ce point de vue nous sommes dans la même situation que la différence entre le théorème de Brouwer et celui de Picard : hors hypothèse de type « contraction », point d'unicité.
- (3) En calcul numérique
- La convergence d'une méthode de point fixe est donnée par la proposition 34.48.
 - La convergence quadratique de la méthode de Newton est donnée par le théorème 34.54.
 - En calcul numérique, section 34.5
 - Méthode de Newton comme méthode de point fixe, sous-section 34.6.2.
- (4) D'autres utilisations de points fixes.
- Processus de Galton-Watson, théorème 38.53.
 - Dans le théorème de Max-Milgram 25.59, le théorème de Picard est utilisé.

Thème 23 : Intégration sur des variétés

orientation La notion d'orientation commence avec l'orientation des bases d'un espace vectoriel et continue jusqu'à orienter des variétés à partir de ses cartes.

- (1) Classe d'orientation sur les bases d'un espace vectoriel, définition 9.21.
- (2) Orientation sur une surface, définition 20.65.
- (3) Variété orientable, définition 20.16.

théorèmes de Stokes, Green et compagnie (1) Forme générale, théorème 20.76.

- (2) Rotationnel et circulation, théorème 24.8.

Le théorème de Stokes peut être utilisé pour montrer le théorème de Brouwer, proposition 20.35.

Thème 24 : permuter des limites

Permuter des dérivées partielles Si une fonction est de classe C^2 , le théorème de Schwarz 12.299 dit que

$$\partial_k \partial_l f = \partial_l \partial_k f. \quad (-2.5)$$

Fonctions définies par une intégrale Les théorèmes sur les fonctions définies par une intégrale, section 17.4. Nous avons entre autres

- (1) $\partial_i \int_B f = \int_B \partial_i f$, avec B compact, proposition 17.26.
- (2) Si f est majorée par une fonction ne dépendant pas de x , nous avons le théorème 17.15 pour la continuité de $x \mapsto \int_\Omega f(x, \omega) d\mu(\omega)$.

4. On aime bien parce que ça ne demande pas Stokes, mais quand même hein, c'est pas gratos non plus.

- (3) Pour la fonction $F(x) = \int_{\Omega} f(x, \omega) d\mu(\omega)$, nous avons la dérivation sous l'intégrale par la formule de Leibnitz

$$F'(a) = \int_{\Omega} \frac{\partial f}{\partial x}(a, \omega) d\mu(\omega) \quad (-2.6)$$

démontrée en le théorème 17.18.

Des variations avec des dérivées partielles et des différentielles sont dans 17.26 et dans 17.27.

- (4) Si $f: \mathbb{C} \times \Omega \rightarrow \mathbb{C}$ est holomorphe (pour $\mathbb{C}$), alors F est holomorphe et

$$F'(z) = \int_{\Omega} \frac{\partial f}{\partial z}(z, \omega) d\mu(\omega). \quad (-2.7)$$

- (5) Pour des dérivées partielles multiples, nous avons la formule

$$(\partial^{\alpha} F)(x) = \int_{\Omega} (\partial^{\alpha} f_{\omega})(a) d\mu(\omega) \quad (-2.8)$$

dans la proposition 17.20.

- (6) Si l'intégrale est uniformément convergente, nous avons le théorème 17.16 qui donne la continuité de $F(x) = \int_{\Omega} f(x, \omega) d\mu(\omega)$.
- (7) Pour dériver $\int_B g(t, z) dt$ avec B compact dans $\mathbb{R}$ et $g: \mathbb{R} \times \mathbb{C} \rightarrow \mathbb{C}$, il faut aller voir la proposition 26.18.
- (8) En ce qui concerne le x dans la borne, le théorème 14.241 lie primitive et intégrale en montrant que $F(x) = \int_a^x f(t) dt$ est une primitive de f (sous certaines conditions). Le théorème fondamental de l'analyse 14.242 en est une conséquence.
- (9) Si T est une **distribution**, alors nous avons

$$T(x \mapsto (\partial_y^{\alpha} \phi)(x, y_0)) = \partial_y^{\alpha} \left(T(x \mapsto \phi(x, y)) \right)_{y=y_0}. \quad (-2.9)$$

C'est la proposition 30.44.

Limite et intégrale (1) Théorème de la convergence monotone, théorème 14.162.

Fubini Le théorème de Fubini permet non seulement de permuter des intégrales, mais également des sommes parce que ces dernières peuvent être vues comme des intégrales sur $\mathbb{N}$ muni de la tribu des parties et de la mesure de comptage⁵. Nous utilisons cette technique pour permuter une somme et une intégrale dans l'équation (26.125).

L'utilisation de Fubini pour permuter des intégrales (sur deux variables différentes) ou deux sommes est expliquée dans 14.268.

C'est par exemple utilisé pour permuter deux sommes dans le cadre des chaînes de Markov en 38.8.

- le théorème de Fubini-Tonelli 14.264 demande que la fonction soit mesurable et positive ;
- le théorème de Fubini 14.267 demande que la fonction soit intégrable (mais pas spécialement positive) ;
- le corolaire 14.266 demande l'intégrabilité de la valeur absolue des intégrales partielles pour déduire que la fonction elle-même est intégrable.

Limite et dérivées, différentielle (1) Permuter limite et dérivée dans le cas $\mathbb{R} \rightarrow \mathbb{R}$, théorème 12.328.

- (2) Permuter limite et dérivées partielles, théorème 12.331.
- (3) Permuter limite et différentielle, théorème 15.8.

Quelques remarques sur les techniques de démonstration.

5. Mesure de comptage, définition 14.235.

- (1) Le résultat fondamental 12.328 est démontré sans recourir à des intégrales. Une preuve alternative, plus courte, avec des intégrales est donnée en 14.249.
- (2) Permuter limite et dérivée partielle, théorème 12.331.
- (3) Permuter série et différentielle, théorème 15.8.

Somme et dérivée Permuter somme et différentielle, théorème 15.8.

Limite et mesure Une mesure n'est pas toujours une limite, mais la définition d'une mesure positive sur un espace mesurable parle de permuter limite et mesure : définition 14.20(2).

Thème 25 : applications continues et bornées

- (1) Une application linéaire non continue : exemple 11.85 de $e_k \mapsto ke_k$. Les dérivées partielles sont calculées en (25.135).
- (2) La dérivation sur les polynômes (exemple 11.86) donne un autre exemple d'application linéaire non continue.
- (3) Une application linéaire est bornée si et seulement si elle est continue, proposition 11.73.

Thème 26 : inégalités Dans $\mathbb{C}$ nous avons $|a + b| \leq |a| + |b|$ par la proposition 10.85(5).

Inégalité de Young Nous avons

$$ab \leq \frac{a^p}{p} + \frac{b^q}{q} \quad (-2.10)$$

par la proposition 27.31.

Inégalité de Jensen (1) Une version discrète pour $f(\sum_i \lambda_i x_i)$, la proposition 17.102.

(2) Une version intégrale pour $f(\int \alpha d\mu)$, la proposition 27.32.

(3) Une version pour l'espérance conditionnelle, la proposition 36.60.

Inégalité pour les normes ℓ^p (1) Hölder pour L^p : $\|fg\|_1 \leq \|f\|_p \|g\|_q$, proposition 27.34.

(2) Hölder pour ℓ^p : $\|x\|_q \leq n^{\frac{1}{q} - \frac{1}{p}} \|x\|_p$, proposition 17.108.

Inégalité de Minkowsky (1) Pour une forme quadratique⁶ q sur $\mathbb{R}^n$ nous avons $\sqrt{q(x+y)} \leq \sqrt{q(x)} + \sqrt{q(y)}$. Proposition 11.12.

(2) Si $1 \leq p < \infty$ et si $f, g \in L^p(\Omega, \mathcal{A}, \mu)$ alors $\|f + g\|_p \leq \|f\|_p + \|g\|_p$. Proposition 27.39.

(3) L'inégalité de Minkowsky sous forme intégrale s'écrit sous forme déballée

$$\left[\int_X \left(\int_Y |f(x, y)| d\nu(y) \right)^p d\mu(x) \right]^{1/p} \leq \int_Y \left(\int_X |f(x, y)|^p d\mu(x) \right)^{1/p} d\nu(y).$$

ou sous forme compacte

$$\left\| x \mapsto \int_Y f(x, y) d\nu(y) \right\|_p \leq \int_Y \|f_y\|_p d\nu(y)$$

Transformée de Fourier Pour tout $f \in L^1(\mathbb{R}^n)$ nous avons $\|\hat{f}\|_\infty \leq \|f\|_1$, lemme 29.12.

Inégalité des normes Inégalité de normes : si $f \in L^p$ et $g \in L^1$, alors $\|f * g\|_p \leq \|f\|_p \|g\|_1$, proposition 27.59.

6. Définition 9.222.

Thème 27 : connexité

- (1) Définition 7.44
- (2) L'image d'un connexe par une fonction continue est connexe, proposition 7.95.
- (3) Connexité par arcs, définition 10.56.
- (4) Une partie de $\mathbb{R}^2$ qui est connexe, mais pas connexe par arcs, proposition 21.56.
- (5) Une partie de $\mathbb{R}$ est connexe si et seulement si elle est un intervalle, proposition 10.47.
- (6) Le groupe $SL(n, \mathbb{K})$ est connexe par arcs : proposition 13.17.
- (7) Le groupe $GL(n, \mathbb{C})$ est connexe par arcs : proposition 13.18.
- (8) Le groupe $GL(n, \mathbb{C})$ est connexe par arcs, proposition 13.18.
- (9) Le groupe $GL(n, \mathbb{R})$ a exactement deux composantes connexes par arcs, proposition 13.19.
- (10) Le groupe $O(n, \mathbb{R})$ n'est pas connexe, lemme 13.14.
- (11) Les groupes $U(n)$ et $SU(n)$ sont connexes par arcs, lemme 13.15.
- (12) Pour tout $n \geq 2$, le groupe $SO(n)$ est connexe, le groupe $O(n)$ a deux composantes connexes, proposition 13.4.
- (13) Connexité des formes quadratiques de signature donnée, proposition 17.114.

Thème 28 : suite de Cauchy, espace complet Nous parlons d'espaces topologiques complets. À ne pas confondre avec un espace mesuré complet, définition 14.56.

- (1) Corps complet : définition 1.253(5), espace métrique complet : définition 7.172.
- (2) La définition 7.171 donne la notion de suite de Cauchy dans un espace métrique.
- (3) La définition 7.169 donne la notion de suite de τ -Cauchy dans un espace vectoriel topologique.
- (4) Deux espaces métriques (avec une distance) peuvent être isomorphes en tant qu'espaces topologiques, mais ne pas avoir les mêmes suites de Cauchy, exemple 7.175.
- (5) La proposition 7.176 donne l'équivalence entre les suites de Cauchy et les suites τ -Cauchy dans le cas des espaces vectoriels topologiques *normés*.
- (6) L'exemple 7.175 est un exemple pire que simplement une suite de Cauchy qui ne converge pas. Le problème de convergence de cette suite n'est pas simplement que la limite n'est pas dans l'espace ; c'est que la suite de Cauchy donnée ne convergerait même pas dans $\mathbb{R}$.
- (7) Le théorème 17.127 est un théorème de complétion d'un espace métrique.
- (8) Dans $\mathbb{R}$, une suite est convergente si et seulement si elle est de Cauchy, théorème 7.198(2).
- (9) Toute suite convergente dans un espace métrique est de Cauchy, proposition 7.177.

Quelques espaces qui sont complets sont listés ci-dessous. Attention : la complétude est bien une propriété de la métrique ; le même ensemble peut être complet pour une distance et pas pour une autre. Souvent, cependant la distance à considérer est donnée par le contexte.

(1) Les réels $\mathbb{R}$, théorème 7.198.	(4) Le lemme 12.313 dit que $(C^0(A, B), \ \cdot\ _\infty)$ est complet dès que A est compact et B est complet.
(2) Un espace vectoriel normé sur un corps complet est complet, proposition 7.203.	(5) L'espace $\mathcal{D}(K)$ est complet tant pour la topologie des semi-normes que pour la topologie métrique (qui sont les mêmes). C'est la proposition 30.18.
(3) La proposition 12.312 donne quelques espaces complets. Soit X un espace topologique métrique (Y, d) un espace espace métrique complet. Alors les espaces	(6) L'espace $\mathcal{S}(\Omega)$ est complet et métrisable par la proposition 30.68.
(3a) $(C_b^0(X, Y), \ \cdot\ _\infty)$	(7) L'espace $L^p(\Omega, \mathcal{A}, \mu)$ par le théorème 27.42.
(3b) $(C_0^0(X, Y), \ \cdot\ _\infty)$	
(3c) $(C_0^k(X, Y), \ \cdot\ _\infty)$	
sont complets.	

La limite uniforme d'une suite de fonctions dérivables n'est pas spécialement dérivable. Même si les fonctions sont de classe C^∞ , la limite n'est pas spécialement mieux que continue. En effet, le théorème de Stone-Weierstrass 12.338 nous dit que les polynômes (qui sont C^∞) sont denses dans les fonctions continues sur un compact pour la norme uniforme. Vous ne pouvez donc pas espérer que $(C^p(X, Y), \|\cdot\|_\infty)$ soit complet en général.

Thème 29 : application réciproque

- (1) Définition 7.87.
- (2) Dans le cas des réels, des exemples sont donnés en 10.7.
- (3) Continuité, proposition 7.89.
- (4) Théorème de la bijection 12.48 (qui contient aussi de la continuité).
- (5) Dérivabilité, proposition 12.130.

Thème 30 : déduire la nullité d'une fonction depuis son intégrale Des résultats qui disent que si $\int f = 0$ c'est que $f = 0$ dans un sens ou dans un autre.

- (1) Il y a le lemme 14.181 qui dit ça.
- (2) Un lemme du genre dans L^2 existe aussi pour $\int f\varphi = 0$ pour tout φ . C'est le lemme 27.62.
- (3) Et encore un pour L^p dans la proposition 27.156.
- (4) Si $\int f\chi = 0$ pour tout χ à support compact alors $f = 0$ presque partout, proposition 30.1.
- (5) La proposition 27.22 donne $f = 0$ dans L^p lorsque $\int fg = 0$ pour tout $g \in L^q$.
- (6) Une fonction $h \in C_c^\infty(I)$ admet une primitive dans $C_c^\infty(I)$ si et seulement si $\int_I h = 0$. Théorème 17.2.

Thème 31 : équations différentielles L'utilisation des théorèmes de point fixe pour l'existence de solutions à des équations différentielles est fait dans le chapitre sur les points fixes.

- (1) Le théorème de Schauder a pour conséquence le théorème de Cauchy-Arzelà 20.38 pour les équations différentielles.
- (2) Le théorème de Schauder 20.37 permet de démontrer une version du théorème de Cauchy-Lipschitz (théorème 17.41) sans la condition Lipschitz
- (3) Le théorème de Cauchy-Lipschitz 17.41 est utilisé à plusieurs endroits :
 - Pour calculer la transformée de Fourier de $e^{-x^2/2}$ dans le lemme 29.22.
- (4) Théorème de stabilité de Lyapunov 32.37.
- (5) Le système proie-prédateur de Lotka-Volterra 32.38
- (6) Équation de Schrödinger, théorème 32.45.
- (7) L'équation $(x - x_0)^\alpha u = 0$ pour $u \in \mathcal{D}'(\mathbb{R})$, théorème 30.40.
- (8) La proposition 32.40 donne un résultat sur $y'' + qy = 0$ à partir d'une hypothèse de croissance.
- (9) Équation de Hill $y'' + qy = 0$, proposition 32.42.

Thème 32 : injections

- (1) L'espace de Sobolev $H^1(I)$ s'injecte de façon compacte dans $C^0(\bar{I})$, proposition 31.6.
- (2) L'espace de Sobolev $H^1(I)$ s'injecte de façon continue dans $L^2(I)$, proposition 31.6.
- (3) L'espace $L^2(\Omega)$ s'injecte continument dans $\mathcal{D}'(\Omega)$ (les distributions), proposition 30.24.

Thème 33 : logarithme

- (1) Le logarithme pour les réels strictement positifs $\ln:]0, \infty[\rightarrow \mathbb{R}$ est donné en la définition 15.73.
- (2) Les principales propriétés sont dans la proposition 15.75 : $\ln(xy) = \ln(x) + \ln(y)$ etc.
- (3) La proposition 15.90 donne la série

$$\ln(1+x) = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} x^k. \quad (-2.11)$$

- (4) L'exemple 20.150 donne l'encadrement $0.644 \leq \ln(2) \leq 0.846$.
- (5) La proposition 15.114 dit que toute matrice complexe admet un logarithme. En particulier une série explicite est donnée pour le logarithme d'un bloc de Jordan.
- (6) Sur les complexes, le logarithme $\ln: \mathbb{C}^* \rightarrow \mathbb{C}$ est la définition 26.63. Attention : ce n'est pas la seule définition possible.
- (7) La série harmonique diverge à vitesse logarithmique, et la série des inverses des nombres premiers, c'est encore plus lent : théorème 15.103.

Thème 34 : inversion locale, fonction implicite

- (1) Théorème d'inversion locale dans un Banach : théorème 17.49.
- (2) Fonction implicite dans un Banach : théorème 17.50.
- (3) Utilisé pour montrer que le flot d'une équation différentielle est un C^p -difféomorphisme local, voir 32.33.
- (4) Pour le théorème de Von Neumann 17.63.

Thème 35 : convexité L'essentiel des résultats sur les fonctions convexes sont dans la section 17.11. On a surtout :

- (1) Définition des fonctions convexes : 17.78 et 17.94 en dimension supérieure.
 - (2) En termes de différentielles, 17.95 pour la différentielle première et 17.98 pour la hessienne.
 - (3) Une courbe paramétrée convexe est la définition 21.90.
 - (4) L'enveloppe convexe d'une courbe fermée simple et convexe : 21.92.
 - (5) Courbure et convexité d'une courbe paramétrée : section 21.13.4.
 - (6) Une courbe paramétrée convexe est localement le graphe d'une fonction convexe par le lemme 21.91.
 - (7) La convexité est utilisée dans la méthode du gradient à pas optimal de la proposition 17.111.
- En termes de parties convexes, on :
- (1) Définition 8.25 d'une partie convexe d'un espace vectoriel.
 - (2) Une boule est convexe, proposition 8.26.

Thème 36 : fonction puissance Il y a beaucoup de choses à dire...

Définition Nous considérons, pour $a > 0$, la fonction $g_a: \mathbb{R} \rightarrow \mathbb{R}$ donnée par $g_a(x) = a^x$. La définition de cette fonction se fait en de nombreuses étapes.

- (1) a^n pour $n \in \mathbb{N}$ en la définition 1.175.
- (2) a^n pour $n \in \mathbb{Z}$ en la définition 12.342.
- (3) $a^{1/n}$ pour $n \in \mathbb{Z}$ en la définition 12.344.
- (4) a^q pour $q \in \mathbb{Q}$ en la définition 12.344.
- (5) $\sqrt[n]{x}$ en la définition 12.346.

- (6) La fonction g_a est Cauchy-continue sur $\mathbb{Q}$, c'est la proposition 12.357.
- (7) a^x pour $a > 0$ et $x \in \mathbb{R}$ en la définition 12.359.
- (8) a^z pour $a > 0$ et $z \in \mathbb{C}$ en la définition 18.5.

Quelques propriétés (1) Pour tout $q \in \mathbb{Q}$, il y a un $\sqrt[q]{a}$ dans $\mathbb{R}$, proposition 1.333.

- (2) Pour $a > 0$ et $x, y \in \mathbb{R}$ nous avons $a^x a^y = a^{x+y}$, proposition 12.360.
- (3) Si $a > 0$ et $x, y \in \mathbb{R}$ nous avons $(a^x)^y = (a^y)^x = a^{xy}$ par la proposition 12.370.
- (4) La fonction puissance est strictement croissante (en ses deux arguments), proposition 12.365.
- (5) La formule $a^{-x} = 1/a^x$ est la proposition 12.360(3).

Dérivation Comme toutes les choses sur la fonction puissance, les preuves sont assez différentes selon que l'on parle de a^x ou de x^a .

- (1) La fonction puissance est strictement croissante, proposition 12.365
- (2) La fonction a^x est dérivable et sa dérivée vérifie $g'_a(x) = g_a(x)g'_a(0)$, proposition 12.373.
- (3) La formule de dérivation pour $x \mapsto x^q$ avec $q \in \mathbb{Q}$ est la proposition 12.382.
- (4) La dérivation de $x \mapsto x^\alpha$ avec $\alpha \in \mathbb{R}$ est la proposition 14.250. Si elle est tellement loin, c'est parce qu'elle nécessite de permuter une limite de fonctions avec une dérivée.
- (5) Pour la formule générale de dérivation de $x \mapsto a^x$ demande de savoir les logarithmes (proposition 15.82).

L'équation fonctionnelle L'exponentielle et plus généralement la fonction puissance $g_a(x) = a^x$ peut être introduite au moyen d'une équation fonctionnelle au lieu de l'équation différentielle usuelle. Cette fameuse équation fonctionnelle est

$$f(x+y) = f(x)f(y) \quad (-2.12)$$

en la définition 12.375.

- (1) L'équivalence entre l'équation fonctionnelle et l'équation différentielle est donnée par la proposition 12.380.
- (2) La fonction $g_a(x) = a^x$ vérifie l'équation fonctionnelle $g_a(x+y) = g_a(x)g_a(y)$ et les conséquences. C'est la définition 12.375 et les choses qui suivent.
- (3) L'équation fonctionnelle pour une fonction continue $f: \mathbb{R} \rightarrow S^1$ est traitée dans la proposition 12.386.

Une définition alternative de la fonction puissance serait de poser directement

$$a^x = e^{x \ln(a)}.$$

De là les propriétés se déduisent facilement. Dans cette approche, les choses se mettent dans l'ordre suivant :

- Définir $\exp(x)$ par sa série pour tout x .
- Démontrer que $\exp(q) = \exp(1)^q$ pour tout rationnel q (première partie de la proposition 15.72).
- Définir $e = \exp(1)$.
- Définir, pour x irrationnel, $a^x = \exp(x \ln(a))$.
- Prouver que $e^x = \exp(x)$ pour tout x .

Thème 37 : dualité Ne pas confondre dual algébrique et dual topologique d'un espace vectoriel.

- (1) Définition de la base duale 4.126.
- (2) Base préduale (existence, unicité) : proposition 4.129.

Dual topologique et algébrique Ils sont définis par 4.125. Le dual algébrique est l'ensemble des formes linéaires, et le dual topologique ne considère que les formes linéaires continues (en dimension infinie, les applications linéaires ne sont pas toutes continues).

Topologie Une topologie possible sur le dual d'un espace vectoriel topologique est celle $*$ -faible de la définition 7.240.

Nous comparons les topologies faibles et de la norme en la section 11.13.

Théorèmes de dualité Quelques théorèmes établissent des dualités entre des espaces courants.

- (1) Le théorème de représentation de Riesz 25.17 pour les espaces de Hilbert.
- (2) La proposition 27.152 pour les espaces $L^p([0, 1])$ avec $1 < p < 2$.
- (3) Le théorème de représentation de Riesz 27.154 pour les espaces L^p en général.

Tous ces théorèmes donnent la dualité par l'application $\Phi_x = \langle x, \cdot \rangle$.

Thème 38 : opérations sur les distributions

- (1) Convolution d'une distribution par une fonction, définition par l'équation (30.186).
- (2) Dérivation d'une distribution, proposition-définition 30.26.
- (3) Produit d'une distribution par une fonction, définition 30.25.

Thème 39 : convolution

- (1) Définition 27.54, et principales propriétés sur $L^1(\mathbb{R})$ dans le théorème 27.55.
- (2) Inégalité de normes : si $f \in L^p$ et $g \in L^1$, alors $\|f * g\|_p \leq \|f\|_p \|g\|_1$, proposition 27.59.
- (3) $\varphi \in L^1(\mathbb{R})$ et $\psi \in \mathcal{S}(\mathbb{R})$, alors $\varphi * \psi \in \mathcal{S}(\mathbb{R})$, proposition 27.171.
- (4) Les suites régularisantes : $\lim_{n \rightarrow \infty} \rho_n * f = f$ dans la proposition 29.18.
- (5) Convolution d'une distribution par une fonction, définition par l'équation (30.186).

Thème 40 : séries de Fourier

- Formule sommatoire de Poisson, proposition 29.15.
- Inégalité isopérimétrique, théorème 28.19.
- Fonction continue et périodique dont la série de Fourier ne converge pas, proposition 28.18.
- Nous allons montrer la convergence de $\sum_{k \in \mathbb{Z}} c_k(f) e^{inx}$ vers $f(x)$ dans divers cas :
 - (1) Si f est continue et périodique, convergence au sens de Cesaro, théorème de Fejèr 28.5.
 - (2) Convergence au sens $L^2([0, 2\pi])$ dans le théorème 27.115.
 - (3) Si f est continue, périodique et si sa série de Fourier converge uniformément, théorème 28.13.
 - (4) Si f est périodique et la série des coefficients converge absolument pour tout x , proposition 28.14.
 - (5) Si f est périodique et de classe C^1 , théorème 28.15.

Il est cependant faux de croire que la continuité et la périodicité suffisent à obtenir une convergence, comme le montre dans la proposition 28.18.

Thème 41 : transformée de Fourier

- (1) Définition sur L^1 , définition 29.1.
- (2) La transformée de Fourier d'une fonction $L^1(\mathbb{R}^d)$ est continue, proposition 29.11.
- (3) L'espace de Schwartz est stable par transformée de Fourier. L'application $\mathcal{F}: \mathcal{S}(\mathbb{R}^d) \rightarrow \mathcal{S}(\mathbb{R}^d)$ est continue. Proposition 29.20
- (4) L'application $\mathcal{F}: \mathcal{S}(\mathbb{R}^d) \rightarrow \mathcal{S}(\mathbb{R}^d)$ est une bijection. Formule d'inversion, proposition 29.26.

Thème 42 : méthode de Newton

- (1) Nous parlons un petit peu de méthode de Newton en dimension 1 dans 34.6.
- (2) La méthode de Newton fonctionne bien avec les fonctions convexes par la proposition 34.56.
- (3) La méthode de Newton en dimension n est le théorème 34.63.
- (4) Un intervalle de convergence autour de α s'obtient par majoration de $|g'|$, proposition 34.48.
- (5) Un intervalle de convergence quadratique s'obtient par majoration de $|g''|$, théorème 34.54.
- (6) En calcul numérique, section 34.6.
- (7) Méthode de Newton pour calculer $\sqrt{A}$, exemple 34.57.

Thème 43 : méthodes de calcul

- (1) Théorème de Rothstein-Trager 20.98.
- (2) Algorithme des facteurs invariants 4.109.
- (3) Méthode de Newton, théorème 34.63
- (4) Calcul d'intégrale par suite équirépartie 28.8.

Thème 44 : espaces vectoriels

- (1) Existence d'une base. Pour un espace vectoriel quelconque, proposition 4.21.
- (2) Théorème de la base incomplète. Pour un espace vectoriel quelconque, théorème 4.22.

Thème 45 : valeurs propres, définie positive

À propos de valeurs propres (1) Définition des valeurs propres d'une forme quadratique : définition 9.235.

- (2) Définition de valeur propre et vecteur propre pour un endomorphisme $f: V \rightarrow V$, définition 9.82.

À propos de choses définies positives (1) Une application bilinéaire est définie positive lorsque $g(u, u) \geq 0$ et $g(u, u) = 0$ si et seulement si $u = 0$ est la définition 9.223.

- (2) Un opérateur ou une matrice est défini positif si toutes ses valeurs propres sont positives, c'est la définition 9.148.
- (3) Pour une matrice symétrique, définie positive si et seulement si $\langle Ax, x \rangle > 0$ pour tout x . C'est le lemme 9.152.
- (4) Une application linéaire est définie positive si et seulement si sa matrice associée l'est. C'est la proposition 9.229.

Remarque : nous ne définissons pas la notion de matrice définie positive dans le cas d'une matrice non symétrique.

Thème 46 : norme matricielle, norme opérateur et rayon spectral Quelques définitions

- (1) Définition de la norme opérateur : définition 11.57.
- (2) Définition du rayon spectral 11.63.

La norme matricielle n'est rien d'autre que la norme opérateur de l'application linéaire donnée par la matrice.

- (1) Lien entre norme matricielle et rayon spectral, le théorème 11.78 assure que $\|A\|_2 = \sqrt{\rho(A^t A)}$.
- (2) Lien entre valeurs propres et norme opérateur : le lemme 11.79 pour les matrices symétriques strictement définies positives donne $\|A\|_2 = \lambda_{\max}$.
- (3) Pour toute norme algébrique nous avons $\rho(A) \leq \|A\|$, proposition 11.70.
- (4) Dans le cadre du conditionnement de matrice. Voir en particulier la proposition 34.110 qui utilise le théorème 11.78.
- (5) Rayon spectral et convergence de méthode itérative, proposition 34.148.

Pour la norme opérateur nous avons les résultats suivants.

- (1) La majoration $\|Au\| \leq \|A\|\|u\|$ est le lemme 11.65.
- (2) Définition d'une algèbre : 1.228 et pour une norme d'algèbre : 11.62.
- (3) La norme opérateur est une norme d'algèbre, lemme 11.68.
- (4) Pour des espaces vectoriels normés, être borné est équivalent à être continu : proposition 11.73.
- (5) Le lemme à propos d'exponentielle de matrice 15.137 donne :

$$\|e^{tA}\| \leq P(|t|) \sum_{i=1}^r e^{t \operatorname{Re}(\lambda_i)}.$$

La norme opérateur est utilisée pour donner une norme sur les produits tensoriels, définition 11.190.

Une norme matricielle donne une topologie. Il y a donc également des liens entre rayon spectral et convergence de série. Dans cette optique, pour les séries de matrices, voir le thème 47.

Thème 47 : série de matrices

- (1) Rayon spectral et norme opérateur : thème 46.
- (2) Exponentielle de matrices : thème 61.
- (3) Série entière de matrices : section 15.13.
- (4) Pour la série $\sum_k A^k = (1 - A)^{-1}$.
 - Pour un espace de Banach : proposition 11.223.
 - Pour les matrices nilpotentes : proposition 9.124.
 - En lien avec le rayon spectral (si et seulement si $\rho(A) < 1$) dans la proposition 15.133.
 - Le lemme 15.41 parle de la série entière $\sum_{n \in \mathbb{N}} z^{nk} = (1 - z^k)^{-1}$.

Cette série est utilisée entre autres dans la proposition 34.168 pour prouver qu'une M-matrice irréductible vérifie $A^{-1} > 0$.

Thème 48 : rang

- (1) Définition pour une application linéaire : 4.41, pour une matrice : 4.101. L'équivalence est la proposition 4.105.
- (2) Le théorème du rang, théorème 4.42
- (3) Pour une application linéaire entre deux espaces vectoriels de même dimension finie, il est équivalent d'être injectif, surjectif ou bijectif, c'est le corolaire 4.44.

- (4) Pour prouver que des matrices sont équivalentes et pour les mettre sous des formes canoniques, nous avons le lemme 4.107 et son corolaire 4.108.
- (5) Tout hyperplan de $M(n, \mathbb{K})$ coupe $GL(n, \mathbb{K})$, corolaire 4.108. Cela utilise la forme canonique sus-mentionnée.
- (6) Le lien entre application duale et orthogonal de la proposition 4.138 utilise la notion de rang.
- (7) Le lemme 9.199 parle de commutant et utilise la notion de rang. Ce lemme sert à prouver diverses conditions équivalentes à être un endomorphisme cyclique dans le théorème 9.200.

Thème 49 : extension de corps et polynômes

- (1) Définition d'une extension de corps 6.54.
- (2) Définition de polynôme minimal : 6.59.
- (3) Pour l'extension du corps de base d'un espace vectoriel et les propriétés d'extension des applications linéaires, voir la section 9.10.
- (4) Extension de corps de base et similitude d'application linéaire (ou de matrices, c'est la même chose), théorème 9.202.
- (5) Extension de corps de base et cyclicité des applications linéaires, corolaire 9.201.
- (6) À propos d'extensions de $\mathbb{Q}$, le lemme 6.169.
- (7) Corps de rupture : définition 6.106 existence par la proposition 6.112. Il n'y a pas unicité.
- (8) Corps de décomposition : définition 6.133. Attention : le plus souvent nous parlons de corps de décomposition d'un seul polynôme. Cette définition est un peu surfaite. Existence par la proposition 6.134 qui le donne même comme extension par toutes les racines, et unicité à isomorphisme près par le théorème 6.136, énoncé de façon plus simple (mais pas indépendante!) en la proposition 6.137.
- (9) Si $\mathbb{K}$ est algébrique clos et si $\alpha: \mathbb{K} \rightarrow \mathbb{L}$ est une extension algébrique, alors $\alpha(\mathbb{K}) = \mathbb{L}$ par le lemme 6.73.

Un trio de résultats d'enfer est :

- (1) Dans un anneau principal qui n'est pas un corps, un idéal est maximal si et seulement si il est engendré par un irréductible (proposition 3.78).
- (2) Dans un anneau, un idéal I est maximal si et seulement si A/I est un corps (proposition 3.50)
- (3) Si $\mathbb{K}$ est un corps, $\mathbb{K}[X]$ est principal (lemme 3.127).

Thème 50 : décomposition de matrices

- (1) Décomposition de Bruhat, théorème 13.37.
- (2) Décomposition de Dunford, théorème 9.162.
- (3) Décomposition polaire 13.31 des matrices symétriques et la proposition 17.59 pour la régularité.

Thème 51 : systèmes d'équations linéaires

- Algorithme des facteurs invariants 4.109.
- La méthode du gradient à pas optimal permet de résoudre par itérations $Ax = b$ lorsque A est symétrique strictement définie positive. Il s'agit de minimiser une fonction bien choisie. Propositions 17.110 pour l'existence et 17.111 pour la méthode.

Thème 52 : formes bilinéaires et quadratiques

- (1) Les formes bilinéaires sont définies en 9.213.
- (2) Forme quadratique, définition 9.222. Sa matrice, définition 9.227.
- (3) Équivalence de forme quadratiques, définition 9.258. Deux formes quadratiques sont équivalentes si et seulement si elles ont même signature, proposition 9.259.
- (4) Une isométrie d'une forme bilinéaire est affine ou linéaire, théorème 9.246.
- (5) Forme bilinéaire dégénérée, définition 9.216.
- (6) Une forme bilinéaire est non-dégénérée si et seulement si sa matrice associée est inversible, c'est la proposition 9.218.
- (7) Une isométrie d'une forme bilinéaire est linéaire ou affine par le théorème 9.246.
- (8) Toute forme quadratique admet des bases orthogonales, théorème 9.240 pour le cas général ; proposition 9.241 pour le cas de $\mathbb{R}^n$, en se basant sur le théorème spectral.
- (9) Théorème de Sylvester à propos de signature (définition 9.251) de forme quadratique réelle : 9.257.
- (10) Base q -orthogonale pour une forme quadratique, théorème 9.240.
- (11) Le concept de projection orthogonale est la définition 12.104 en dimension fini et la définition 25.5 dans le cas des espaces de Hilbert.

Thème 53 : arithmétique modulo, théorème de Bézout

- (1) Pour $\mathbb{Z}^*$ c'est le théorème 1.181.
- (2) Théorème de Bézout dans un anneau principal : corolaire 3.87.
- (3) Théorème de Bézout dans un anneau de polynômes : théorème 6.43.
- (4) En parlant des racines de l'unité et des générateurs du groupe unitaire dans le lemme 19.6. Au passage nous y parlerons de solfège.
- (5) La proposition 1.184 qui donne tout entier assez grand comme combinaisons de a et b à coefficients positifs est utilisée en chaînes de Markov, voir la définition 38.47 et ce qui suit.
- (6) PGCD et PPCM sont dans la définition 1.169.
- (7) Calcul effectif du PGCD puis des coefficients de Bézout : sous-sections 3.2.1.1 et 3.2.1.2.

Thème 54 : polynômes

Définitions Soient un anneau A , un corps $\mathbb{K}$, une extension $\mathbb{L}$ de $\mathbb{K}$ et un élément $\alpha \in \mathbb{L}$.

- (1) La définition la plus formelle est en tant que module produit $A^{(\mathbb{N})}$, définition 1.240. Le produit et l'évaluation sont définis en 1.242 et la formule $(PQ)(x) = P(x)Q(x)$ dans 1.243.
- (2) Si A est commutatif, alors $A[X]$ est également commutatif, lemme 1.244.
- (3) En ce qui concerne la notation $A[X]$, elle ne devrait pas être utilisée, voir 1.14.2. L'ensemble des polynômes sera noté $\mathcal{P}(A)$ et ceux de degré n (définition 1.241), $\mathcal{P}_n(A)$.
- (4) $A[X]$, définition 1.240 ; l'anneau $\mathbb{K}[X]$ a même définition parce que c'est un cas particulier. L'évaluation d'un polynôme en un élément de l'anneau, $P(\alpha)$ est définie en 1.242.
- (5) Liens entre $\mathbb{K}[\alpha]$, $\mathbb{K}[X]$, $\mathbb{K}(\alpha)$ et $\mathbb{K}(X)$ lorsque α est transcendant, proposition 6.87. Et la proposition 6.90 pour le cas où α est algébrique⁷.
- (6) Si A est un anneau et si α est un élément d'une extension de A (comme anneau), nous écrivons $A[\alpha]$ pour le plus petit sous-anneau de B contenant A et α . C'est la définition 3.119.

7. Définition 6.65.

- (7) $\mathbb{K}(X)$, le corps des fractions de $\mathbb{K}[X]$, définition 6.77. Si $R = P/Q$ dans $\mathbb{K}(X)$, l'évaluation est $R(\alpha) = P(\alpha)Q(\alpha)^{-1}$, définition 6.78.
- (8) $\mathbb{K}(\alpha)_{\mathbb{L}}$ est le plus petit corps de $\mathbb{L}$ contenant $\mathbb{K}$ et α , définition 6.79.
- (9) À propos de polynômes à plusieurs variables.
 - Anneau de polynômes : $A[X_1, \dots, X_n]$ est la définition 3.51.
 - Corps engendré : $\mathbb{K}(\alpha_1, \dots, \alpha_n)$ est la définition 6.130.
 - Corps des fractions rationnelles : $\mathbb{K}(X_1, \dots, X_n)$ est la définition 6.131.

Coefficients dans un anneau commutatif (1) Les polynômes à coefficients dans un anneau commutatif sont à la section 3.10.

Coefficients dans un corps Les polynômes à coefficients dans un corps sont à la section 6.3.

- (1) Nous parlons de l'idéal des polynômes annulateurs dans le théorème 6.39.
- (2) Le théorème 6.39 dit que $\mathbb{K}[X]$ est un anneau principal et que tous ses idéaux sont engendrés par un unique polynôme unitaire.
- (3) Le polynôme minimal est irréductible, proposition 6.62.
- (4) Quelques formules sur le pgcd, lemme 6.52.

Polynôme primitif (1) Un polynôme est irréductible sur A si et seulement si irréductible et primitif sur le corps des fractions, corolaire 3.147.

Polynôme d'endomorphisme C'est la section 9.6.

- Racines et factorisation** (1) Si $\mathbb{A}$ est un anneau, la proposition 3.137 factorise une racine.
- (2) Si $\mathbb{A}$ est un anneau, la proposition 3.141 factorise une racine avec sa multiplicité.
 - (3) Si $\mathbb{A}$ est un anneau, le théorème 3.143 factorise plusieurs racines avec leurs multiplicités.
 - (4) Le théorème 3.143 nous indique que lorsqu'on a autant de racines (multiplicité comprise) que le degré, alors nous avons toutes les racines.
 - (5) Si $\mathbb{K}$ est un corps et α une racine dans une extension, le polynôme minimal de α divise tout polynôme annulateur par la proposition 6.88.
 - (6) Le théorème 6.103 annule un polynôme de degré n ayant $n + 1$ racines distinctes.
 - (7) La proposition 6.172 nous annule un polynôme à plusieurs variables lorsqu'il a trop de racines.
 - (8) En analyse complexe, le principe des zéros isolés 17.128 annule en gros toute série entière possédant un zéro non isolé.
 - (9) Polynômes irréductibles sur $\mathbb{F}_q$.

Thème 55 : zoologie de l'algèbre Nous listons ici un peu tous les termes qui arrivent en algèbre.

Structures Les structures.

(0a) Algèbre, définition 1.228.

<++>

Éléments Pour les éléments, nous avons :

(0a) Élément irréductible en 3.64.

(0b) Élément premier en 1.201.

Anneaux Pour les anneaux, nous avons :

(0a) Anneau factoriel en 3.68.

(0b) Anneau principal en 3.72.

(0c) Anneau intègre en 1.174.

(0d) Anneau noetherien en 3.90.

Idéaux Pour les idéaux, nous avons :

(0a) Idéal principal en 3.71.

(0b) Idéal premier en 3.73.

Thème 56 : invariants de similitude

- (1) Théorème 9.188.
- (2) Pour prouver que la similitude d'applications linéaires résiste à l'extension du corps de base, théorème 9.202.
- (3) Pour prouver que la dimension du commutant d'un endomorphisme de E est de dimension au moins $\dim(E)$, lemme 9.199.
- (4) Nous verrons dans la remarque 9.189 à propos des invariants de similitude que toute matrice est semblable à la matrice bloc-diagonale constituée des matrices compagnon (définition 9.183) de la suite des polynômes minimaux.

Thème 57 : réduction, diagonalisation Des résultats qui parlent diagonalisation

- (1) Définition d'un endomorphisme diagonalisable : 9.126.
- (2) Conditions équivalentes au fait d'être diagonalisable en termes de polynôme minimal, y compris la décomposition en espaces propres : théorème 9.129.
- (3) Diagonalisation simultanée 9.132, pseudo-diagonalisation simultanée 11.42.
- (4) Diagonalisation d'exponentielle 15.115 utilisant Dunford.
- (5) Décomposition polaire théorème 13.31. $M = SQ$, S est symétrique, réelle, définie positive, Q est orthogonale.
- (6) Décomposition de Dunford 9.162. $u = s + n$ où s est diagonalisable et n est nilpotent, $[s, n] = 0$.
- (7) Réduction de Jordan (bloc-diagonale) 9.191.
- (8) L'algorithme des facteurs invariants 4.109 donne $U = PDQ$ avec P et Q inversibles, D diagonale, sans hypothèse sur U . De plus les éléments de D forment une chaîne d'éléments qui se divisent l'un l'autre.

Le théorème spectral et ses variantes :

- (1) Théorème spectral, matrice symétrique, théorème 9.146. Via le lemme de Schur complexe 9.138.
- (2) Théorème spectral autoadjoint (c'est le même, mais vu sans matrices), théorème 11.5
- (3) Théorème spectral hermitien, lemme 11.20.
- (4) Théorème spectral, matrice normales, théorème 11.23.

Pour les résultats de décomposition dont une partie est diagonale, voir le thème 50 sur les décompositions. Réduction de quadriques :

- (1) Réduction de Gauss, théorème 9.237.

Thème 58 : endomorphismes cycliques

- (1) Définition 9.100.
- (2) Son lien avec le commutant donné dans la proposition 9.197 et le théorème 9.200.
- (3) Utilisation dans le théorème de Frobenius (invariants de similitude), théorème 9.188.

Thème 59 : déterminant

- (1) Déterminant d'une matrice : définition 4.72.
- (2) Déterminant d'un endomorphisme 9.8.
- (3) Le lemme 11.4 donne la formule $\det(f) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^n \langle e_{\sigma(i)}, f(e_i) \rangle$.
- (4) Principales propriétés algébriques du déterminant : la proposition 9.9.
- (5) La formule $\det(AB) = \det(A)\det(B)$ est la proposition 4.97 pour des matrices et la proposition 9.9(1) pour les applications linéaires.

- (6) Déterminant et manipulations de lignes et colonnes, section 4.3.10 et les propositions qui précèdent à partir du lemme 4.74 qui dit que $\det(A) = \det(A^t)$.
 - (7) Les n -formes alternées forment un espace de dimension 1, proposition 9.3.
 - (8) Déterminant d'une famille de vecteurs 9.4.
 - (9) Calcul d'un déterminant de taille 2×2 : équation (4.97).
 - (10) Interprétations géométriques
 - (10a) À propos d'orthogonalité, le déterminant est très lié au produit vectoriel en dimension 3. Et il le généralise en dimension supérieure.
 - i. Liaison au produit vectoriel (orthogonalité) dans la proposition 11.39.
 - ii. En particulier le lemme 11.40 nous dit comment un déterminant donne un vecteur orthogonal à une famille donnée de vecteurs.
 - (10b) Déterminant et aires, volumes
 - i. Déterminant et mesure de Lebesgue : théorème 14.259.
 - ii. Aire du parallélogramme : il y a la formule avec le produit vectoriel dans la proposition 18.49, mais l'autre proprement dire, avec une intégrale est dans la proposition 20.31.
 - iii. Volume du parallélépipède avec le produit mixte et le déterminant 3×3 , 18.50.
- Tant que nous en sommes dans les interprétations géométriques, il faut lier déterminant, produit vectoriel, orthogonalité et mesure en notant que l'élément de volume lors de l'intégration en dimension 3 est donné par (20.199) : $dS = \|T_u \times T_v\|$ qui est la norme du produit vectoriel des vecteurs tangents au paramétrage.
- Nous voyons dans l'équation (20.196) que l'élément de volume pour une partie de dimension n dans $\mathbb{R}^m$ (à l'occasion d'y intégrer une fonction) est donné par un déterminant mettant en jeu les vecteurs tangents du paramétrage.
- (11) Le déterminant de Vandermonde est à la proposition 9.11. Il est utilisé à divers endroits :
 - (11a) Pour prouver que u est nilpotente si et seulement si $\text{Tr}(u^p) = 0$ pour tout p (lemme 9.122)
 - (11b) Pour prouver qu'un endomorphisme possédant $\dim(E)$ valeurs propres distinctes est cyclique (proposition 9.197).

Thème 60 : polynôme d'endomorphismes

- (1) Endomorphismes cycliques et commutant dans le cas diagonalisable, proposition 9.197.
- (2) Racine carrée d'une matrice hermitienne positive, proposition 13.26.
- (3) Théorème de Burnside sur les sous-groupes d'exposant fini de $\text{GL}(n, \mathbb{C})$, théorème 9.209.
- (4) Décomposition de Dunford, théorème 9.162.
- (5) Algorithme des facteurs invariants 4.109.

Thème 61 : exponentielle Toutes les exponentielles sont définies par la série

$$\exp(x) = \sum_{k=0}^{\infty} \frac{x^k}{k!},$$

tant que la somme a un sens.

Réels Voici le plan que nous suivons dans le Frido :

- L'exponentielle est définie par sa série en 15.53.
- Nous démontrons qu'elle vérifie l'équation différentielle $y' = y$, $y(0) = 1$ (théorème 15.69).

- Nous démontrons l'unicité de la solution à cette équation différentielle.
- Nous démontrons qu'elle est égale à $x \mapsto y(1)^x$. Cela donne la définition du nombre e comme valant $y(1)$.
- Nous définissons le logarithme comme l'application réciproque de l'exponentielle (définition 15.73).
- Les fonctions trigonométriques (sinus et cosinus) sont définies par leurs séries. Il est alors montré que $e^{ix} = \cos(x) + i \sin(x)$.

Propriétés — La formule $a^{-x} = 1/a^x$ est la proposition 12.360(3).

Complexes (1) La définition de $\exp(a + bi)$ est la définition 15.53.

- (2) Les principales propriétés, dont $e^{z+w} = e^z e^w$, sont dans la proposition 18.9.
- (3) Nous avons $e^{ix} = e^{iy}$ si et seulement si il existe $k \in \mathbb{Z}$ tel que $y = x + 2k\pi$, corolaire 18.21.
- (4) Le fait que $e^{i\theta}$ donne tous les nombres complexes de norme 1 est la proposition 18.53.
- (5) Le groupe des racines de l'unité est donné par l'équation (19.1).

Algèbre normée commutative Pour la définition c'est la proposition 15.53 et pour la régularité C^∞ c'est la proposition 15.58.

Idem non commutatif Il y a une tentative de théorème 15.59, mais c'est principalement pour les matrices qu'il y a des résultats.

Matrices De nombreux résultats sont disponibles pour les exponentielles de matrices.

- (1) $e^{sA} e^{tA} = e^{(s+t)A}$, proposition 15.63.
- (2) Si A est une matrice, alors $(e^t A)'(u) = A e^{uA}$, proposition 15.65.
- (3) Les sections 11.12 et 15.5.3 parlent d'exponentielle de matrices.
- (4) L'exponentielle donne lieu à une fonction de classe C^∞ , proposition 15.134.
- (5) Le lemme à propos d'exponentielle de matrice 15.137 donne :

$$\|e^{tA}\| \leq P(|t|) \sum_{i=1}^r e^{t \operatorname{Re}(\lambda_i)}.$$

- (6) La proposition 15.115 : si $A \in \mathbb{M}(n, \mathbb{R})$ a un polynôme caractéristique scindé, alors A est diagonalisable si et seulement si e^A est diagonalisable.
- (7) La section 15.13.3 parle des fonctions exponentielle et logarithme pour les matrices. Entre autres la dérivation et les séries.
- (8) Pour résoudre des équations différentielles linéaires : sous-section 32.6.1.
- (9) La proposition 15.114 dit que l'exponentielle est surjective sur $\operatorname{GL}(n, \mathbb{C})$.
- (10) La proposition 11.226 : si u est un endomorphisme, alors $\exp(u)$ est un polynôme en u .
- (11) Calcul effectif : sous-section 15.13.4.
- (12) Proposition 13.22 : si $A \in \mathbb{M}(n, \mathbb{C})$ alors $e^{\operatorname{Tr}(A)} = \det(e^A)$.
- (13) Les séries entières de matrices sont traitées autour de la proposition 15.131.

Thème 62 : types d'anneaux

- (1) Définition d'anneau : définition 1.30.
- (2) La définition d'anneau principal est 3.72 ; pour un idéal principal, c'est 3.71.
- (3) $\mathbb{Z}$ est intègre, exemple 1.198, principal et euclidien (proposition 3.103).
- (4) $\mathbb{Z}[X]$ n'est pas principal (voir (5)).
- (5) Si A est un anneau intègre⁸ qui n'est pas un corps, alors $A[X]$ n'est pas principal, lemme 3.104.

8. Définition 1.174.

- (6) L'anneau des fonctions holomorphes sur un compact donné est principal, proposition 26.22.
- (7) L'anneau $\mathbb{Z}[i\sqrt{3}]$ n'est pas factoriel, exemple 3.70.
- (8) L'anneau $\mathbb{Z}[i\sqrt{5}]$ n'est ni factoriel ni principal, exemple 3.94.
- (9) Tous les idéaux de $\mathbb{Z}/6\mathbb{Z}$ sont principaux, mais $\mathbb{Z}/6\mathbb{Z}$ n'est pas principal. Exemple 3.82.

Thème 63 : sous-groupes

- (1) Théorème de Burnside sur les sous-groupes d'exposant fini de $\mathrm{GL}(n, \mathbb{C})$, théorème 9.209.
- (2) Sous-groupes compacts de $\mathrm{GL}(n, \mathbb{R})$, lemme 13.38 ou proposition 13.39.

Thème 64 : groupe symétrique

- (1) Définition 1.146.
- (2) La signature $\epsilon: S_n \rightarrow \{-1, 1\}$ est l'unique homomorphisme surjectif de S_n sur $\{-1, 1\}$, proposition 1.159(1).
- (3) La table des caractères du groupe symétrique S_4 est donné dans la section 16.5.
- (4) Le groupe symétrique S_4 est le groupe des symétries affines du tétraèdre régulier⁹, proposition 18.170.
- (5) Le groupe alterné A_5 est l'unique groupe simple d'ordre 60, proposition 5.40.
- (6) La proposition 5.30 donne la position du groupe alterné dans le groupe symétrique : A_n est un sous-groupe caractéristique de S_n et l'unique sous-groupe d'indice 2.

Thème 65 : action de groupe

- (1) Définition d'une action de groupe sur un ensemble : 1.246.
- (2) Action du groupe modulaire sur le demi-plan de Poincaré, théorème 23.95.
- (3) La formule de Burnside (théorème 2.59) parle du nombre d'orbites pour l'action d'un groupe fini sur un ensemble fini.
- (4) Des applications de la formule de Burnside : le jeu de la roulette et l'affaire du collier, 18.8.2.1 et 18.8.2.2.
- (5) Le groupe symétrique S_n agit sur l'anneau $\mathbb{K}[T_1, \dots, T_n]$, lemme 1.247.

Thème 66 : classification de groupes

- (1) Structure des groupes d'ordre pq , théorème 5.25.
- (2) Le groupe alterné est simple, théorème 5.36.
- (3) Définition 5.6 d'un p -groupe.
- (4) Théorème de Sylow 5.11.
- (5) Théorème de Burnside sur les sous-groupes d'exposant fini de $\mathrm{GL}(n, \mathbb{C})$, théorème 9.209.
- (6) $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$, corolaire 19.37.

Thème 67 : produit semi-direct de groupes

- (1) Définition 2.64.
- (2) Le corolaire 2.66 donne un critère pour prouver qu'un produit NH est un produit semi-direct.
- (3) L'exemple 18.93 donne le groupe des isométries du carré comme un produit semi-direct.
- (4) Le théorème 5.25 classe les groupes d'ordre pq (p, q premiers distincts) à grands coups de produit semi-directs.
- (5) Le théorème 18.69 donne les isométries de $\mathbb{R}^n$ par $\mathrm{Isom}(\mathbb{R}^n) = T(n) \times_{\rho} O(n)$ où $T(n)$ est le groupe des translations.

9. Définition 12.109.

- (6) La proposition 18.71 donne une décomposition du groupe orthogonal $O(n) = SO(n) \times_{\rho} C_2$ où $C_2 = \{\text{Id}, R\}$ où R est de déterminant -1 .
- (7) La proposition 8.58 donne $\text{Aff}(\mathbb{R}^n) = T(n) \times_{\rho} GL(n, \mathbb{R})$ où $\text{Aff}(\mathbb{R}^n)$ est le groupe des applications affines bijectives de $\mathbb{R}^n$.

Thème 68 : théorie des représentations

- (1) Définition 4.145.
- (2) Table des caractères du groupe diédral, section 18.16.
- (3) Table des caractères du groupe symétrique S_4 , section 16.5.

Thème 69 : isométries Il y a $(\mathbb{R}^n, \|\cdot\|)$ et $\mathbb{R}^n, d$.

Les isométries de $\|\cdot\|$ sont linéaires, tandis que les isométries de la distance contiennent aussi les translations et les rotations de centre différent de l'origine.

Ne pas confondre une isométrie d'un espace affine avec une isométrie d'un espace euclidien¹⁰. Les isométries d'un espace euclidien préservent le produit scalaire et fixent donc l'origine (lemme 11.17). Les isométries des espaces affines par contre conservent les distances (définition 8.59) et peuvent donc déplacer l'origine de l'espace vectoriel sur lequel il est modélisé ; typiquement les translations sont des isométries de l'espace affine mais pas de l'espace euclidien.

Parfois, lorsqu'on coupe les cheveux en quatre, il faut faire attention en parlant de $\mathbb{R}^n$: soit on en parle comme d'un espace métrique (muni de la distance), soit on en parle comme d'un espace normé (muni de la norme ou du produit scalaire).

Général Quelques résultats généraux et en vrac à propos d'isométries.

- (1) Définition d'une isométrie pour une forme bilinéaire, 9.244. Pour une forme quadratique : définition 9.243.
- (2) Définition du groupe orthogonal 9.39, et le spécial orthogonal $SO(n)$ en la définition 9.42. Le groupe $SO(2)$ est le groupe des rotations, par corolaire 18.140.
- (3) La rotation $R_A(\theta)$ d'un angle θ autour du point $A \in \mathbb{R}^2$ est donnée par la définition 18.129.
- (4) La proposition 18.141 donne à toute rotation $R_0(\theta)$ une matrice de la forme connue. C'est autour de cela que nous définissons les angles, définition 18.159.
- (5) Le groupe orthogonal est le groupe des isométries de $\mathbb{R}^n$, proposition 9.41.
- (6) Les isométries de l'espace euclidien sont affines, 9.246.
- (7) Les isométries de l'espace euclidien comme produit semi-direct : $\text{Isom}(\mathbb{R}^n) \simeq T(n) \times_{\rho} O(n)$, théorème 18.69.
- (8) Isométries du cube, section 5.7.
- (9) Nous parlons des isométries affines du tétraèdre régulier dans la proposition 18.170.

Groupe diédral Le groupe diédral est un peu central dans la théorie des isométries de $(\mathbb{R}^2, d)$ parce que beaucoup de sous-groupes finis des isométries de $(\mathbb{R}^2, d)$ sont en fait isomorphes au groupe diédral.

- (1) Générateurs du groupe diédral, proposition 18.91.
- (2) Un sous-groupe fini des isométries de $(\mathbb{R}^2, d)$ contenant au moins une réflexion est isomorphe au groupe diédral par le théorème 18.175.
- (3) Le théorème 18.177 dit que le groupe des isométries propres d'une partie quelconque de $(\mathbb{R}^2, d)$ est soit cyclique soit isomorphe au groupe diédral.

Isométries et réflexions Dans un espace euclidien, toute isométrie peut être décomposée en réflexions autour d'hyperplans. Voici quelques énoncés à ce propos.

- (1) Définition d'une réflexion dans $\mathbb{R}^2$ 18.122.

10. Définition 9.263.

- (2) La caractérisation en termes de projection orthogonale est le lemme 18.109 ; en termes de médiatrice c'est le lemme 18.114.
- (3) Définition d'un hyperplan 9.203.
- (4) En dimension 2, une rotation est définie comme composée de deux réflexions en la définition 18.119.
- (5) En dimension 2, les réflexions ont un déterminant -1 par le lemme 18.133.
- (6) Les isométries du plan $(\mathbb{R}^2, d)$ sont données dans le théorème 18.166, et sont au plus 3 réflexions par le théorème 18.164.
- (7) Décomposition des isométries de $\mathbb{R}^n$ en réflexions par le lemme 18.76.
- (8) En particulier, les éléments de $\text{SO}(3)$ sont des compositions de deux réflexions par le corolaire 18.78.
- (9) Une isométrie de $\mathbb{R}^n$ préserve l'orientation si et seulement si est elle composition d'un nombre pair de réflexions. C'est le théorème 18.80.

Sous-groupe fini (1) Les sous-groupes finis des isométries de $(\mathbb{R}^2, d)$ sont cycliques, théorème 18.175.

- (2) Les sous-groupes finis de $\text{SO}(3)$ sont listés dans 18.199.
- (3) Les sous-groupes finis de $\text{SO}(2)$ sont cycliques, lemme 18.144.

Thème 70 : caractérisation de distributions en probabilités

- (1) La probabilité conjointe est la définition 36.19.
- (2) La fonction de répartition est la définition 36.61.
- (3) La fonction caractéristique est la définition 36.63.

Thème 71 : théorème central limite

- (1) Pour les processus de Poisson, théorème 40.5.

Thème 72 : lemme de transfert Il y a deux résultats qui portent ce nom. Le premier est dans la théorie de Fourier, le résultat $\hat{f}' = i\xi\hat{f}$.

- (1) Lemme 29.19 sur $\mathcal{S}(\mathbb{R}^d)$
- (2) Lemme 31.10 pour L^2 .

L'autre lemme de transfert est en théorie des tribus, le résultat $\sigma(f^{-1}(\mathcal{C})) = f^{-1}(\sigma(\mathcal{C}))$ du lemme 14.47. Celui-ci est d'ailleurs plutôt nommé « lemme de transport ».

Thème 73 : probabilités et espérances conditionnelles Les deux définitions de base, sur lesquelles se basent toutes les choses conditionnelles sont :

- L'espérance conditionnelle d'une variable aléatoire sachant une tribu : $E(X|\mathcal{F})$ de la définition 36.37.

Les autres sont listées ci-dessous.

Probabilité conditionnelle .

Plusieurs probabilités conditionnelles.

- D'un événement en sachant un autre : la définition 36.33 donne

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

Cela est la définition de base. L'autre est une définition dérivée.

- D'un événement vis-à-vis d'une variable aléatoire discrète. C'est par la définition 36.55 qui définit la variable aléatoire

$$P(A|X)(\omega) = P(A|X = X(\omega)).$$

Dans le cas continu, c'est la définition 36.56 :

$$P(A|X) = P(A|\sigma(X)) = E(\mathbb{1}_A|\sigma(X)).$$

- D'un événement par rapport à une tribu. C'est la variable aléatoire

$$P(A|\mathcal{F}) = E(\mathbb{1}_A|\mathcal{F}).$$

Espérances conditionnelles Plusieurs espérances conditionnelles.

- D'une variable aléatoire par rapport à un événement, définition 36.49 :

$$E(X|A) = \frac{E(X\mathbb{1}_A)}{P(A)}. \quad (-2.13)$$

- d'une variable aléatoire par rapport à une tribu. La variable aléatoire $E(X|\mathcal{F})$ est la variable aléatoire $\mathcal{F}$ -mesurable telle que

$$\int_B E(X|\mathcal{F}) = \int_B X$$

pour tout $X \in \mathcal{F}$. Si $X \in L^2(\Omega, \mathcal{A}, P)$ alors $E(X|\mathcal{F}) = \text{proj}_K(X)$ où K est le sous-ensemble de $L^2(\Omega, \mathcal{A}, P)$ des fonctions $\mathcal{F}$ -mesurables (théorème 36.37). Cela au sens des projections orthogonales.

- d'une variable aléatoire par rapport à une autre. La définition 36.39 est une variation sur le même thème :

$$E(X|Y) = E(X|\sigma(Y)),$$

Notons que partout, si X est une variable aléatoire, la notation « sachant X » est un raccourci pour dire « sachant la tribu engendrée par X ».

Quelques formules.

- (1) Pour l'espérance conditionnelle d'une variable aléatoire prenant seulement une quantité dénombrable de valeurs : $E(X|A) = \sum_{k=0}^{\infty} y_k P(X = y_k|A)$ par le lemme 36.50.
- (2) La probabilité conditionnelle se factorise par rapport à l'union disjointe par le lemme 36.36 : $P(\bigcup_{i=0}^{\infty} A_i|B) = \sum_{i=0}^{\infty} P(A_i|B)$.

Thème 74 : dénombrements

- Coloriage de roulette (18.8.2.1) et composition de colliers (18.8.2.2).
- Nombres de Bell, théorème 15.151.
- Le dénombrement des solutions de l'équation $\alpha_1 n_1 + \dots + \alpha_p n_p = n$ utilise des séries entières et des décompositions de fractions en éléments simples¹¹, théorème 26.50.

Thème 75 : enveloppes

- (1) L'ellipse de John-Loewner donne un ellipsoïde de volume minimum autour d'un compact dans $\mathbb{R}^n$, théorème 17.119.
- (2) Le cercle circonscrit à une courbe donne un cercle de rayon minimal contenant une courbe fermée simple, proposition 21.89.
- (3) Enveloppe convexe du groupe orthogonal 13.36.
- (4) Enveloppe convexe d'une courbe fermée plane comme intersection des demi-plans tangents, proposition 21.95.

11. Éléments simples, lemme 19.18.

Thème 76 : équations diophantiennes

- (1) Équation $ax + by = c$ dans $\mathbb{N}$, équation (3.44).
- (2) Dans 3.2.7, nous résolvons $ax + by = c$ en utilisant Bézout (théorème 1.181).
- (3) L'exemple 3.108 donne une application de la pure notion de modulo pour $x^2 = 3y^2 + 8$. Pas de solutions.
- (4) L'exemple 3.109 résout l'équation $x^2 + 2 = y^3$ en parlant de l'extension $\mathbb{Z}[i\sqrt{2}]$ et de stathme.
- (5) Les propositions 3.113 et 3.115 parlent de triplets pythagoriciens.
- (6) Le dénombrement des solutions de l'équation $\alpha_1 n_1 + \dots + \alpha_p n_p = n$ utilise des séries entières et des décompositions de fractions en éléments simples, théorème 26.50.
- (7) La proposition 1.111 donne une bijection $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ en résolvant dans $\mathbb{N}$ (entre autres) l'équation $k = y^2 + x$ pour k fixé.

Thème 77 : changement de variables Un des moto du Frido est qu'il n'existe rien qui s'appelle « changement de variables ». Il n'existe que des composition de fonctions. Ce snobisme terminologique étant, voici un certain nombre de résultats de changement de variables.

- (1) Dans des intégrales, théorème 14.260.
- (2) Dans des limites, le lemme 7.74 donne que si $\lim_{x \rightarrow a} f(x) = \lim_{x \rightarrow b} f(x + a - b)$.
- (3) Dans une équation aux dérivées partielles, exemple 33.132.

Thème 78 : techniques de calcul Il y en a pour tous les goûts.

Primitives et intégrales Toute la section 17.12 donne des trucs et astuces pour trouver des primitives et des intégrales.

Limite à deux variables Les exemples de limites à plusieurs variables font souvent intervenir des coordonnées polaires (du théorème 18.202) ou autres fonctions trigonométriques. Ils sont donc placés beaucoup plus bas que la théorie.

- Méthode du développement asymptotique, sous-section 18.13.2.
- Méthode des coordonnées polaires, sous-section 18.13.1.
- Utilisation du théorème de la fonction implicite, dans l'exemple 18.204.

-2.1 Conventions sur les matrices et changement de bases

-2.1.1 Matrices et applications linéaires

Le lien entre matrice et application linéaire est donné par la définition 4.63. L'application d'une matrice à un vecteur est (4.79). Le lien le plus simple entre l'application linéaire et les éléments de matrice est donné par la proposition 4.66. Voici les relations :

$$T_{\alpha i} = T(e_i)_\alpha \quad (-2.14a)$$

$$T(e_i) = \sum_{\alpha} T_{\alpha i} f_{\alpha} \quad (-2.14b)$$

$$T(x) = \sum_{i, \alpha} T_{\alpha i} x_i f_{\alpha} \quad (-2.14c)$$

$$T(x)_\alpha = \sum_i T_{\alpha i} x_i. \quad (-2.14d)$$

Cela définit une application $\psi: M(n \times m, \mathbb{K}) \rightarrow \mathcal{L}(E, F)$ qui a plein de propriétés.

- (1) C'est une bijection, proposition 4.66(4).
- (2) C'est un isomorphisme d'algèbre, proposition 4.69.
- (3) C'est un isomorphisme d'espaces vectoriels, proposition 4.67.

- (4) Isomorphisme d'algèbres et d'anneaux, proposition 4.69.
- (5) Isomorphisme d'espaces topologiques, proposition 4.69.

Lorsque nous avons une base orthonormée nous avons aussi les propositions 4.119 et 4.119 qui donnent des formules avec produit scalaire :

- (1) $T_{\alpha i} = e_{\alpha} \cdot T(e_i)$
- (2) $x \cdot Ay = \sum_{kl} A_{kl} x_k y_l$.

où le point est le produit scalaire usuel de $\mathbb{R}^n$.

-2.1.2 Le changement de base

Soit un espace vectoriel V muni de deux bases $(e_i)_{i=1,\dots,n}$ et $(f_{\alpha})_{\alpha=1,\dots,n}$. Le lemme 4.110 donne le lien entre les vecteurs de base :

- (1) $f_{\alpha} = \sum_i Q_{i\alpha} e_i$
- (2) $e_i = \sum_{\alpha} Q_{\alpha i}^{-1} f_{\alpha}$

La proposition 4.111 donne un certain nombre de formules pour les coordonnées des vecteur :

- (1) $y_{\alpha} = \sum_i Q_{\alpha i}^{-1} x_i$
- (2) $x_i = \sum_{\alpha} Q_{i\alpha} y_{\alpha}$.
- (3) $x_i = (Qy)_i$
- (4) $x = Qy$

La transformation de la matrice d'une application linéaire lors d'un changement de base est la proposition 4.114. Soit une application linéaire $T: V \rightarrow V$ de matrices A et B dans les bases $\{e_i\}$ et $\{f_{\alpha}\}$. Si les bases sont liées par $f_{\alpha} = \sum_i Q_{i\alpha} e_i$, alors les matrices A et B sont liées par

$$B = Q^{-1} A Q. \quad (-2.15)$$

-2.1.3 Changement de base : matrice d'une forme bilinéaire

La proposition 9.233 fait le changement de matrice d'une forme bilinéaire lors d'un changement de base. Si la matrice de q dans la base $\{e_i\}$ est A et celle dans la base $\{f_{\alpha}\}$ est B , alors

$$B = Q^t A Q. \quad (-2.16)$$

Pour comparaison avec la loi de transformation des matrices des applications linéaires, voir la remarque 9.234.

-2.2 Multiindice et liste d'indices

-2.1.

Je crois qu'il y a quelque incohérences de notations/dénominations dans le texte[1]. En principe quand on parle de $\mathbb{R}^n$, un **multiindice** [2] est un vecteur d'entiers positifs à n composantes. Si $\alpha = (2, 1)$ alors nous avons la notation

$$\partial^{\alpha} f = \frac{\partial^2}{\partial x_1} \frac{\partial}{\partial x_2} f \quad (-2.17)$$

Cette notation pose problème lorsque, par exemple, $\partial_1^2 \partial_2 f \neq \partial_1 \partial_2 \partial_1 f$.

Elle pose également problème lorsque l'on veut faire une récurrence sur l'ordre de dérivation en ajoutant une seule dérivation à la fois.

C'est pourquoi nous introduisons le concept de **liste d'indices**. En parlant de $\mathbb{R}^n$, une liste d'indices est un vecteur arbitrairement long (mais fini) d'entiers dans $\{1, \dots, n\}$. Si, dans $\mathbb{R}^7$, $\alpha = (1, 3, 1, 5)$, alors

$$\partial^{\alpha} f = \partial_1 \partial_3 \partial_1 \partial_5 f. \quad (-2.18)$$

Si α est une liste d'indices de longueur p , une **queue de** α est une liste d'indices de la forme $(\alpha_{p-k}, \alpha_{p-k+1}, \dots, \alpha_{p-k})$.

Table des matières

Thématique	2
-2.1 Conventions sur les matrices et changement de bases	32
-2.1.1 Matrices et applications linéaires	32
-2.1.2 Le changement de base	33
-2.1.3 Changement de base : matrice d'une forme bilinéaire	33
-2.2 Multiindice et liste d'indices	33
Table des matières	34
Index	65
Liste des notations	89
0 Introduction (Vol 1)	93
0.1 Auteurs, contributeurs, sources et remerciements	93
0.1.1 Ceux qui ont travaillé sur le Frido	93
0.1.2 Aide directe, mais pas volontairement sur le Frido	94
0.1.3 Des gens qui ont fait un travail qui m'a bien servi	95
0.2 Originalité	95
0.3 Les choses qui doivent vous faire tiquer	96
0.4 Quelques choix qui peuvent provoquer des quiproquos	96
0.5 Autres choix pas spécialement standards	96
0.5.1 Mathématique intéressante	97
0.6 Sage est là pour vous aider	97
0.6.1 Lancez-vous dans Sage	97
0.6.2 Exemples de ce que Sage peut faire pour vous	98
0.7 Comment contribuer et aider ?	99
0.7.1 Des preuves qui manquent	99
0.7.2 Du texte qui manque	99
0.7.3 Des exemples qui manquent	99
0.7.4 Trucs de programmation et de L ^A T _E X	99
0.8 Les politiques éditoriales	100
0.8.1 Licence libre	100
0.8.2 pdf _l atex	100
0.8.3 utf8	100
0.8.4 Notations	100
0.8.5 De la bibliographie	100
0.8.6 Faire des références à tout	100
0.8.7 Des listes de liens internes	100
0.8.8 Pas de références vers le futur	101
0.8.9 Écriture inclusive	101
1 Construction des ensembles de nombres (Vol 1)	103
1.1 Quelques éléments sur les ensembles	103
1.1.1 Petit mot d'introduction	103

1.1.2	Injection, surjection, bijection	104
1.1.3	Ensemble ordonné	104
1.1.4	Lemme de Zorn	105
1.1.5	Complémentaire	105
1.1.6	Relations d'équivalence	107
1.2	Quelques structures algébriques	108
1.3	Les naturels	109
1.3.1	Applications définies par récurrence	109
1.3.2	Addition sur les naturels	112
1.3.3	Ordre sur les naturels	114
1.3.4	Multiplication dans les naturels	119
1.3.5	Presque unicité des triplets naturels	122
1.3.6	Écriture d'un naturel dans une base	125
1.4	Les entiers	130
1.4.1	Opposé	131
1.5	Quelques résultats de cardinalité	132
1.5.1	Équipotence, surpotence, subpotence	132
1.5.2	Un peu d'infinité	133
1.5.3	Dénombrabilité et ensemble des naturels	139
1.5.4	Théorème de Cantor-Schröder-Bernstein	143
1.5.5	Comparabilité cardinale	146
1.5.6	Théorème de Cantor, ensemble des ensembles	147
1.5.7	Ajouter ou soustraire des cardinalités	148
1.6	Groupes	152
1.6.1	Définition, unicité du neutre	152
1.6.2	Classes de conjugaison	153
1.6.3	Permutations, groupe symétrique	154
1.6.4	Décomposition en cycles	155
1.7	Anneaux	157
1.7.1	Anneau intègre	160
1.7.2	Fonction puissance	161
1.8	Le groupe et anneau des entiers	161
1.8.1	Division euclidienne	162
1.8.2	PGCD, PPCM et Bézout	162
1.8.3	Sous-groupes de $(\mathbb{Z}, +)$	165
1.8.4	Résultats supplémentaires sur l'anneau des entiers	165
1.9	Corps	166
1.9.1	Définitions, morphismes	166
1.10	Anneau intègre	167
1.10.1	Élément premier	167
1.11	Symbole de sommation	169
1.11.1	Somme à valeurs dans un groupe abélien	169
1.12	Module sur un anneau	173
1.12.1	Module produit	174
1.12.2	Sous-module	175
1.13	Caractéristique d'un anneau	176
1.13.1	Caractéristique deux	178
1.14	Polynômes	178
1.14.1	Polynômes d'une variable	178
1.14.2	La notation $A[X]$	180
1.14.3	Action du groupe symétrique	181
1.14.4	Corps des fractions	182
1.14.5	Corps totalement ordonné	184

1.15	Les rationnels	186
1.15.1	Relation d'ordre	187
1.15.2	Caractéristique	187
1.16	Suite de Cauchy dans un corps totalement ordonné	188
1.16.1	Suites de Cauchy dans les rationnels	190
1.17	Insuffisance des rationnels	191
1.18	Les réels	195
1.18.1	L'ensemble	195
1.18.2	Relation d'ordre	198
1.18.3	Complétude	203
1.18.4	Intervalles	206
1.18.5	Maximum, supremum et compagnie	207
1.18.6	Racines	210
1.18.7	Corps valué	211
1.18.8	Partie entière, partie fractionnaire	212
1.19	Les complexes	212
2	Théorie des groupes (Vol 1)	215
2.1	Groupes	215
2.2	Sous-groupe normal	217
2.3	Groupe dérivé	220
2.4	Théorèmes d'isomorphismes	221
2.5	Indice d'un sous-groupe et ordre des éléments	223
2.6	Suite de composition	225
2.7	Groupes résolubles	228
2.8	Action de groupes	229
2.9	Produit semi-direct de groupes	233
2.10	Groupe de torsion	235
2.11	Famille presque nulle	235
3	Anneaux (Vol 1)	237
3.1	Inversibles et nilpotents	237
3.2	PGCD, PPCM et éléments inversibles	238
3.2.1	Calcul effectif du PGCD et de Bézout	238
3.2.2	Générateurs	240
3.2.3	Générateurs pour le groupe multiplicatif	241
3.2.4	Décomposition en facteurs premiers	241
3.2.5	Ordre d'un élément dans un groupe fini	244
3.2.6	Écriture des fractions	246
3.2.7	Équation diophantienne linéaire à deux inconnues	247
3.2.8	Quotients	248
3.3	Binôme de Newton et morphisme de Frobenius	249
3.4	Idéal dans un anneau	250
3.5	Polynômes de plusieurs variables	252
3.5.1	Divisibilité et classes d'association	253
3.5.2	PGCD et PPCM	253
3.5.3	Anneaux intègres et corps	254
3.5.4	Élément irréductible	254
3.6	Anneau factoriel	255
3.7	Anneau principal et idéal premier	256
3.7.1	Bézout	259
3.7.2	Idéal premier	260
3.7.3	Anneau noethérien	261
3.8	Anneau $\mathbb{Z}/6\mathbb{Z}$	262

3.9	Anneau euclidien	263
3.9.1	Équations diophantiennes	266
3.9.2	Triplets pythagoriciens et équation de Fermat pour $n = 4$	267
3.10	Polynômes à coefficients dans un anneau commutatif	270
3.10.1	Monômes	270
3.10.2	Évaluation	270
3.10.3	Polynômes sur un anneau intègre	271
3.10.4	Division euclidienne	272
3.10.5	Polynôme primitif	273
3.10.6	Racines des polynômes	273
3.10.7	Quelques identités	275
4	Espaces vectoriels (début) (Vol 1)	277
4.1	Parties libres, génératrices, bases et dimension	277
4.1.1	Et en dimension infinie	283
4.1.2	Espace librement engendré	284
4.2	Applications linéaires	285
4.2.1	Définition	285
4.2.2	Linéarité et bases	288
4.2.3	Rang	289
4.3	Matrices	293
4.3.1	Définitions	293
4.3.2	Identifier matrices et applications linéaires	295
4.3.3	Déterminant	299
4.3.4	Déterminant en petite dimension	299
4.3.5	Manipulations de lignes et de colonnes	299
4.3.6	Réduction de Gauss	305
4.3.7	Matrices inversibles	307
4.3.8	Inversibilité et déterminant	308
4.3.9	Quelques ensembles de matrices particuliers	309
4.3.10	Déterminant et combinaisons de lignes et colonnes	309
4.3.11	Transvections	311
4.3.12	Mineur, rang	312
4.3.13	Matrices équivalentes et semblables	313
4.3.14	Algorithme des facteurs invariants	314
4.4	Changement de base	316
4.4.1	Changement de base : vecteurs de base	316
4.4.2	Changement de base : coordonnées	316
4.4.3	Changement de base : matrice d'une application linéaire	317
4.5	Espaces de polynômes	318
4.5.1	Projection et orthogonalité	319
4.6	Dualité	321
4.6.1	Orthogonal	322
4.6.2	Transposée : pas d'approche naïve	323
4.6.3	Transposée : la bonne approche	325
4.6.4	Polynômes de Lagrange	327
4.6.5	Dual de $M(n, K)$	327
4.7	Représentation de groupe	329
4.8	Somme directe d'espaces vectoriels	329
4.8.1	Structure réelle	330
5	Classification de certains groupes (Vol 1)	333
5.1	Théorèmes de Sylow	333
5.2	Groupe monogène	337

5.3	Automorphismes du groupe $\mathbb{Z}/n\mathbb{Z}$	338
5.4	Groupes abéliens finis	339
5.5	Groupes d'ordre pq	342
5.6	Groupe symétrique, groupe alterné	345
5.6.1	Le groupe alterné	345
5.6.2	Sous-groupes normaux	351
5.6.3	Indice	352
5.7	Isométries du cube	354
6	Corps (Vol 1)	357
6.1	Généralités	357
6.1.1	Corps ordonnés	357
6.1.2	Automorphismes de $\mathbb{R}$ et $\mathbb{C}$	357
6.1.3	Corps premier	359
6.1.4	Petit théorème de Fermat	359
6.1.5	Nombres de Sophie Germain	360
6.2	Théorème des deux carrés	363
6.2.1	Un peu de structure dans $\mathbb{Z}[i]$	363
6.2.2	Résultats chinois	366
6.3	Polynômes à coefficients dans un corps	369
6.3.1	Irréductibilité	369
6.3.2	Idéaux	370
6.3.3	Bézout	372
6.3.4	Lemme et théorème de Gauss	373
6.3.5	Polynômes sur un corps et pgcd	373
6.4	Extension de corps	376
6.4.1	Extension et polynôme minimal	377
6.4.2	Extensions algébriques et éléments transcendants	378
6.4.3	Extension algébrique et polynôme minimal	381
6.4.4	Extensions et polynômes	382
6.4.5	Racines de polynômes	391
6.4.6	Corps de rupture	392
6.4.7	Pile d'extensions	395
6.4.8	Clôture algébrique	396
6.4.9	Polynômes à plusieurs variables	401
6.4.10	Corps de décomposition	402
6.4.11	Non irréductible ou pas corps ?	406
6.4.12	Clôture algébrique	406
6.4.13	Extensions séparables	408
6.5	Idéal maximum	412
6.5.1	Idéal maximum	412
6.6	Polynômes symétriques et alternés	414
6.6.1	Polynômes symétriques, alternés ou semi-symétriques	414
6.6.2	Polynôme symétrique élémentaire	414
6.6.3	Relations coefficients racines	416
6.7	Minuscule morceau sur la théorie de Galois	417
7	Topologie générale (Vol 1)	419
7.1	Éléments généraux de topologie	419
7.1.1	Définitions et propriétés de base	419
7.1.2	Base de topologie	419
7.1.3	Fermés	420
7.1.4	Quelques exemples	420
7.1.5	Topologie produit	422

7.1.6	Adhérence, fermeture, intérieur, point d'accumulation et isolé	424
7.2	Suites et convergence	426
7.2.1	Convergence dans un fermé	427
7.2.2	Pour des limites uniques : séparabilité	427
7.2.3	Fonctions équivalentes	428
7.3	Connexité	430
7.4	Compacité	431
7.4.1	Définition et notions connexes	431
7.4.2	Quelques propriétés	433
7.4.3	Compactifié d'Alexandrov	435
7.5	Limites et continuité de fonctions	437
7.5.1	Limites	437
7.5.2	Continuité	438
7.5.3	Continuité et topologie induite	442
7.5.4	Continuité et connexité	443
7.5.5	Continuité et compacité	443
7.6	Topologie, distances et normes	444
7.6.1	Distance et topologie métrique	444
7.6.2	Distance à un ensemble	448
7.6.3	Norme	449
7.6.4	Topologie et matrices	450
7.7	Produit fini d'espaces vectoriels normés	451
7.7.1	Distance et norme produit	451
7.8	Topologie réelle en dimension n	452
7.8.1	Ouverts et fermés	452
7.8.2	Intérieur, adhérence et frontière	453
7.8.3	Point d'accumulation, point isolé	454
7.8.4	Limite de suite	455
7.9	Topologie et distance	455
7.9.1	Suites et espaces métriques	457
7.9.2	Espace métrisable	459
7.10	Suites de Cauchy, métrique et espaces complets	460
7.10.1	Généralités	460
7.10.2	Espace topologique métrique	462
7.11	Espaces vectoriels topologiques	463
7.11.1	Équivalence entre Cauchy et τ -Cauchy	471
7.12	Norme, espace vectoriel normé	472
7.13	Espaces métriques	475
7.13.1	Espaces métrisables	475
7.13.2	Fonctions continues	475
7.13.3	Ensembles enchainés	482
7.13.4	Produit fini d'espaces métriques	483
7.13.5	Équicontinuité	484
7.13.6	Continuité uniforme	485
7.14	Ensembles nulle part denses	485
7.15	Topologie des seminormes	485
7.15.1	Espace dual	488
7.15.2	Espace $C^k(\mathbb{R}, E')$	488
7.16	Espaces de Baire	489
8	Espaces affines (Vol 1)	491
8.1	Vecteurs agissant sur un espace	491
8.2	Repères cartésiens affines	492
8.3	Classification affine des conique	492

8.4	Applications affines	494
8.4.1	Autres propriétés	495
8.5	Isomorphismes	496
8.6	Sous espaces affines	497
8.7	Barycentre	499
8.7.1	Sous-espaces affines	499
8.7.2	Enveloppe convexe	501
8.7.3	Applications affines et barycentre	504
8.8	Repères, coordonnées cartésiennes et barycentriques	505
8.8.1	Équation de droite	508
8.8.2	Associativité, coordonnées barycentriques dans un triangle	509
8.9	Applications affines sur $\mathbb{R}^n$	510
8.9.1	Structure de groupe pour les applications affines	511
8.10	Isométries	512
9	Espaces vectoriels (encore) (Vol 1)	513
9.1	Déterminants	513
9.1.1	Formes multilinéaires alternées	513
9.1.2	Déterminant d'une famille de vecteurs	514
9.1.3	Déterminant d'un endomorphisme	517
9.1.4	Déterminant de Vandermonde	519
9.1.5	Déterminant de Gram	521
9.1.6	Déterminant de Cauchy	522
9.1.7	Matrice de Sylvester	522
9.1.8	Théorème de Kronecker	524
9.2	Orientation	526
9.2.1	Cas vectoriel	526
9.2.2	Cas affine	528
9.3	Hermitien, orthogonal, adjoint	528
9.3.1	Opérateur orthogonal, matrice orthogonale	531
9.4	Topologie	532
9.4.1	Boules et sphères	532
9.4.2	Ouverts, fermés, intérieur et adhérence	533
9.4.3	Point isolé, point d'accumulation	540
9.4.4	Des exemples	541
9.5	Valeur propre et vecteur propre	543
9.5.1	Généralités	543
9.5.2	Dans le vif du sujet	544
9.6	Polynômes d'endomorphismes	545
9.6.1	Polynômes d'endomorphismes	545
9.6.2	Polynôme minimal et minimal ponctuel	547
9.6.3	Polynôme caractéristique	553
9.7	Diagonalisation et trigonalisation	557
9.7.1	Matrices semblables	557
9.7.2	Endomorphismes nilpotents	557
9.7.3	Endomorphismes diagonalisables	561
9.7.4	Diagonalisation : cas complexe, pas toujours	564
9.7.5	Trigonalisation : généralités	564
9.7.6	Trigonalisation : cas complexe	565
9.7.7	Diagonalisation : cas réel	567
9.8	Fonctions	571
9.9	Sous espaces caractéristiques	571
9.9.1	Théorèmes de décomposition	573
9.9.2	Diverses conséquences	575

9.9.3	Valeurs singulières	575
9.10	Extension du corps de base	576
9.10.1	Extension des applications linéaires	576
9.10.2	Projections	578
9.10.3	Rang, polynôme minimal, polynôme caractéristique	580
9.11	Frobenius et Jordan	582
9.11.1	Matrice compagnon	582
9.11.2	Réduction de Frobenius	583
9.11.3	Forme normale de Jordan	586
9.12	Commutant et endomorphismes cycliques	587
9.12.1	Endomorphisme cyclique	587
9.12.2	Commutant : cas diagonalisable	587
9.12.3	Commutant : cas général	590
9.13	Hyperplans et formes linéaires	592
9.13.1	Trouver la matrice d'une symétrie donnée	594
9.14	Théorème de Burnside	596
9.14.1	Théorème de Lie-Kolchin	598
9.15	Formes bilinéaires et quadratiques	600
9.15.1	Dégénérescence d'une forme bilinéaire	601
9.15.2	Topologie	602
9.15.3	Isotropie	603
9.16	Formes bilinéaires et quadratiques	603
9.16.1	Généralités	603
9.16.2	Matrice associée à une forme bilinéaire	604
9.16.3	Changement de base : matrice d'une forme bilinéaire	605
9.16.4	Diagonalisation	606
9.16.5	Réduction de Gauss	606
9.16.6	Orthogonalité	609
9.16.7	Diagonalisation	611
9.16.8	Isométrie, forme quadratique et bilinéaire	611
9.16.9	Isométries	612
9.17	Signature, théorème de Sylvester	614
9.17.1	Invariance de la trace	617
9.18	Produit scalaire, produit hermitien	618
9.18.1	Ellipsoïde	619
9.19	Système d'équations linéaires : méthode de Gauss	620
10	Analyse réelle : topologie et continuité (Vol 2)	623
10.1	Intervalles	623
10.2	Application réciproque	624
10.2.1	Définitions	624
10.2.2	Graphes de la fonction réciproque	625
10.3	Topologie sur l'ensemble des réels	625
10.3.1	Compacité pour les réels	626
10.3.2	Conséquence : les fermés bornés sont compacts	628
10.3.3	Suites et limites dans les réels	629
10.3.4	Opérations sur les limites	630
10.3.5	Exemples	631
10.3.6	Suites croissantes et bornées	632
10.3.7	Suites adjacentes	633
10.3.8	Limite supérieure et inférieure	634
10.3.9	Ouverts, voisinage, topologie	635
10.3.10	Intervalles et connexité	636
10.3.11	Recouvrement par des intervalles ouverts	640

10.3.12	Connexité par arcs	642
10.3.13	Un peu de connexité par arcs	642
10.3.14	Des exemples	644
10.3.15	Topologie de la droite réelle complétée	646
10.3.16	Quelques mots à propos de la droite réelle complétée	647
10.4	Continuité	647
10.4.1	Opération sur la continuité	648
10.4.2	La fonction la moins continue du monde	649
10.4.3	Approche topologique	650
10.4.4	Module sur les nombres complexes	652
10.4.5	Continuité de la racine carrée, invitation à la topologie induite	655
10.4.6	Second degré	657
11	Espaces vectoriels normés (Vol 2)	659
11.0.1	Norme, produit scalaire et Cauchy-Schwarz (cas réel)	659
11.1	Théorème spectral autoadjoint	661
11.1.1	Inégalité de Minkowski	664
11.1.2	Cauchy-Schwarz etc. cas complexe	666
11.1.3	Diagonalisation : cas complexe, ce qu'on a	667
11.1.4	Projection et orthogonalité	669
11.1.5	Théorème de Pythagore	670
11.1.6	Produit vectoriel	671
11.1.7	Produit mixte	675
11.1.8	Procédé de Gram-Schmidt	676
11.1.9	Pseudo-réduction simultanée	677
11.2	Approximations	678
11.2.1	Quelques exemples de normes sur $\mathbb{R}^n$	679
11.3	Équivalence des normes	680
11.3.1	En dimension finie	680
11.3.2	Contre-exemple en dimension infinie	682
11.4	Norme opérateur	683
11.4.1	Norme d'algèbre	685
11.4.2	Matrices, spectre et norme	686
11.4.3	Rayon spectral	687
11.4.4	Normes de matrices et d'applications linéaires	692
11.4.5	Application linéaire continue et bornée	693
11.4.6	Suites	696
11.4.7	Continuité du produit de matrices	697
11.5	Applications multilinéaires	699
11.6	Séries	700
11.6.1	Les trois types de convergence	702
11.6.2	Séries dans une algèbre normée	704
11.7	Série réelle	705
11.7.1	Critères de convergence absolue	706
11.7.2	Critères de convergence simple	707
11.7.3	Quelques séries usuelles	708
11.7.4	Séries alternées	710
11.7.5	Moyenne de Cesaro	711
11.7.6	Écriture décimale d'un réel	711
11.7.7	Théorème de Banach-Steinhaus	715
11.7.8	Convergence forte	718
11.8	Application ouverte	719
11.9	Sommes de familles infinies	722
11.9.1	Convergence commutative	722

11.9.2	Somme non dénombrables	724
11.9.3	Sommes dénombrables	725
11.9.4	Convergence en norme et par composante	728
11.10	Produit tensoriel d'espaces vectoriels	728
11.10.1	Les produits tensoriels	729
11.10.2	Le produit tensoriel	730
11.10.3	Bases	734
11.10.4	Norme	735
11.10.5	Applications bilinéaires, matrices et produit tensoriel	736
11.10.6	Application d'opérateurs	737
11.11	Calcul différentiel dans un espace vectoriel normé	737
11.11.1	Définition de la différentielle	737
11.11.2	Accroissements finis	738
11.11.3	(non ?) Différentiabilité des applications linéaires	739
11.11.4	Dérivation en chaîne et formule de Leibnitz	739
11.11.5	Différentiation de produit	744
11.11.6	Formule des accroissements finis	747
11.11.7	Applications multilinéaires	750
11.11.8	Différentielle partielle	751
11.11.9	L'inverse, sa différentielle	753
11.12	Exponentielle de matrice	755
11.13	Espace dual	756
11.13.1	Topologies	756
11.13.2	Module de continuité	758
11.14	Mini introduction aux nombres p -adiques	759
11.14.1	La flèche d'Achille	759
11.14.2	La tortue et Achille	760
11.14.3	Dans les nombres p -adiques, c'est vrai	761
12	Analyse réelle : limites et dérivation (Vol 2)	763
12.1	Limite de fonctions	763
12.1.1	Définition	763
12.1.2	Quelques règles de calcul	765
12.2	Limites pointées et époutées	768
12.2.1	Théorèmes de composition de limites	770
12.2.2	Discussion pointée Vs époutée	773
12.3	Limites en l'infini	776
12.3.1	Limite en des nombres	778
12.3.2	Limites quand tout va bien	778
12.3.3	Limites de fonctions	780
12.3.4	Limite à gauche et à droite	780
12.4	Limite en compactifié d'Alexandrov	781
12.4.1	Prolongement par continuité	782
12.4.2	Prolongement par continuité	783
12.4.3	Théorème de la bijection	784
12.5	Limite et continuité	785
12.5.1	Règles simples de calcul	787
12.5.2	Prolongement des rationnels vers les réels	788
12.6	Espace des fonctions continues	792
12.7	Uniforme continuité	796
12.8	Fonctions sur un compact	799
12.9	Polynômes, théorème de d'Alembert	799
12.9.1	Polynômes sur les réels	799
12.9.2	Polynômes sur les complexes	800

12.10 Géométrie dans l'espace	805
12.10.1 Projection orthogonale	808
12.10.2 Plan médiateur	810
12.10.3 Tétraèdre	811
12.11 Dérivée : exemples introductifs	811
12.11.1 La vitesse	811
12.11.2 La tangente à une courbe	812
12.11.3 L'aire en dessous d'une courbe	813
12.12 Dérivation de fonctions réelles	814
12.12.1 Exemples	815
12.12.2 Interprétation géométrique : tangente	816
12.12.3 Interprétation géométrique : approximation affine	817
12.12.4 Développement limité au premier ordre	818
12.13 Règles de calcul	819
12.13.1 Dérivée de la réciproque	823
12.13.2 Dérivée de fonction composée	824
12.13.3 Dérivée de fonction périodique	825
12.14 Dérivation et croissance	826
12.14.1 Théorèmes de Rolle et des accroissements finis	827
12.14.2 Règle de l'Hospital	830
12.14.3 Dérivée et primitive	831
12.15 Fonctions de plusieurs variables	832
12.15.1 Graphes de fonctions à plusieurs variables	835
12.15.2 Courbes de niveau	836
12.16 Limites à plusieurs variables	840
12.16.1 Caractérisation de la limite par les suites	843
12.16.2 Règle de l'étau	844
12.16.3 Méthode des chemins	845
12.17 Dérivée directionnelle	847
12.17.1 Dérivée partielle et directionnelles	847
12.17.2 Gradient : direction de plus grande pente	851
12.17.3 Gradient : orthogonal au plan tangent	852
12.17.4 Mise en bouche en dimension 2	852
12.17.5 Accroissements finis et dérivées partielles	854
12.18 Formes différentielles	855
12.18.1 Décomposition dans la base duale	855
12.18.2 L'isomorphisme musical	856
12.19 Différentielle	857
12.19.1 Exemples introductifs	857
12.19.2 Différentielle	858
12.19.3 Matrice de la différentielle	858
12.19.4 Quelques propriétés	859
12.19.5 Différentielle, dual et forme différentielle	860
12.19.6 Ce n'est pas la différentielle extérieure	861
12.19.7 Continuité, dérivabilité et différentiabilité	861
12.19.8 Calcul de valeurs approchées	864
12.19.9 Différentielle et tangente	866
12.19.10 Prouver qu'une fonction n'est pas différentiable	867
12.19.11 Gradient	871
12.19.12 Linéarité	871
12.20 Produit	872
12.20.1 Difficulté d'ordre supérieur	873
12.20.2 Solution : produit tensoriel	874

12.20.3	Formes bilinéaires	874
12.21	Différentielle de fonction composée	875
12.21.1	Fonctions composées	877
12.22	Autres trucs sur la différentielle	878
12.22.1	Différentielle et dérivées partielles	878
12.22.2	Plan tangent	879
12.22.3	Calcul de différentielles	879
12.22.4	Notes idéologiques quant au concept de plan tangent	880
12.22.5	Gradient et recherche du plan tangent	880
12.23	Jacobienne	882
12.23.1	Rappels et définitions	882
12.24	Fonctions de classe C^1	882
12.25	Différentielle et dérivée complexe	892
12.25.1	Quelques règles de calcul	895
12.26	Théorèmes des accroissements finis	895
12.27	Fonctions Lipschitziennes	896
12.28	Différentielles d'ordre supérieur	898
12.28.1	Différentielle et dérivées partielles	898
12.28.2	Espaces d'applications multilinéaires et identifications	902
12.28.3	Identification des espaces d'applications multilinéaires (vieux)	906
12.28.4	Fonctions différentiables plusieurs fois	907
12.28.5	Différentielle seconde, fonction de classe C^2	907
12.28.6	Ordre supérieur	910
12.29	Suites et séries : généralités	914
12.29.1	Convergence uniforme	914
12.29.2	Série de fonctions	917
12.30	Permuter limite et dérivée	920
12.31	Densité des polynômes	927
12.31.1	Théorème de Stone-Weierstrass	927
12.32	Primitive de fonction continue	931
12.33	La fonction puissance	932
12.33.1	Sur les naturels	932
12.33.2	Sur les rationnels, racines	934
12.33.3	Dérivation de la fonction puissance (première)	946
12.33.4	Équation fonctionnelle	948
12.33.5	Dérivation de la fonction puissance (seconde)	950
12.33.6	Hölder	951
12.33.7	Vers les complexes	952
12.34	Polynômes de Taylor	953
12.34.1	Fonctions « petit o »	957
12.34.2	Autres formulations	959
12.34.3	Formule et reste	959
12.34.4	Reste intégral	960
12.35	Développement limité autour de zéro	960
12.35.1	Généralités	960
12.35.2	Formule de Taylor-Young	961
12.35.3	Règles de calcul	963
12.36	Développement ailleurs qu'à l'origine	965
12.37	Développement au voisinage de l'infini	965
12.37.1	La fonction puissance : remarques pour la suite	965
12.38	Fonctions réelles de deux variables réelles	965
12.38.1	Limites de fonctions à deux variables	966
12.38.2	Dérivées partielles	967

12.38.3	Différentielle et accroissement	968
12.39	Les fonctions à valeurs vectorielles	968
12.40	Fonctions vectorielles de plusieurs variables	969
12.41	Limites à plusieurs variables	969
12.42	Champs de vecteurs	973
12.42.1	Matrice jacobienne	973
12.43	Divergence, rotationnel et l'opérateur nabla	974
12.44	Interprétation de la divergence	976
12.45	Quelques formules de Leibnitz	978
13	Analyse sur des groupes (Vol 2)	979
13.1	Action de groupe et connexité	979
13.2	Espaces de matrices	981
13.2.1	Dilatations et transvections	981
13.2.2	Connexité de certains groupes	987
13.2.3	Densité	989
13.2.4	Racine carrée d'une matrice hermitienne positive	991
13.2.5	Racine carrée d'une matrice symétrique positive	992
13.2.6	Décomposition polaires : cas réel	993
13.2.7	Enveloppe convexe	995
13.2.8	Décomposition de Bruhat	997
13.3	Sous-groupes du groupe linéaire	999
14	Tribus, théorie de la mesure, intégration (Vol 2)	1003
14.1	Tribus	1003
14.1.1	Généralités	1003
14.1.2	Tribu induite	1004
14.1.3	Tribu de Baire	1005
14.2	Théorie de la mesure	1007
14.2.1	Mesure sur un ensemble de parties	1007
14.2.2	Mesure sur une algèbre de parties	1007
14.2.3	Mesure sur une tribu, espace mesuré	1009
14.2.4	Mesure extérieure	1015
14.3	Applications mesurables	1017
14.3.1	Propriétés	1017
14.3.2	D'une tribu à l'autre	1018
14.4	Espace mesuré complet	1021
14.4.1	Partie négligeable	1021
14.4.2	Prolongement	1030
14.5	Tribu borélienne	1032
14.5.1	Mesure image	1034
14.5.2	Régularité d'une mesure	1035
14.5.3	Théorème de récurrence	1039
14.6	Mesurabilité des fonctions à valeurs réelles	1039
14.6.1	Fonctions à valeurs réelles sur un espace mesurable	1040
14.6.2	Fonction étagée	1046
14.6.3	Fonctions réelles à variables réelles	1048
14.7	Tribu produit	1049
14.7.1	Produit d'espaces mesurables	1049
14.7.2	Le cas des boréliens	1050
14.8	Mesure de Lebesgue sur $\mathbb{R}$	1052
14.8.1	Mesure et tribu de Lebesgue	1056
14.8.2	Propriétés de la mesure de Lebesgue	1057
14.8.3	Fonctions mesurables	1062

14.8.4	Ensemble de Vitali (non mesurable)	1062
14.8.5	Ensemble de Cantor	1063
14.8.6	Mesure positive sans intervalle	1065
14.9	Intégrale par rapport à une mesure	1066
14.9.1	Définition pour les fonctions à valeurs positives	1066
14.9.2	Premières propriétés	1068
14.9.3	Propriétés plus avancées	1071
14.9.4	Fonctions à valeurs réelles	1075
14.9.5	Additivité de l'intégrale	1076
14.9.6	Fonctions à valeurs vectorielles (dimension finie)	1077
14.9.7	Quelques propriétés	1079
14.9.8	Permuter limite et intégrale	1080
14.9.9	Additivité de l'intégrale de Lebesgue	1082
14.9.10	Produit d'une mesure par une fonction (mesure à densité)	1084
14.9.11	Mesure et topologie	1086
14.10	Propriétés des intégrales	1087
14.11	Mesure à densité	1089
14.11.1	Théorème de Radon-Nikodym	1089
14.11.2	Mesure complexe	1090
14.11.3	Théorème d'approximation	1090
14.12	Produit de mesures	1094
14.13	Tribu et mesure de Lebesgue sur $\mathbb{R}^d$	1099
14.13.1	Ensembles négligeables	1100
14.13.2	Parties et fonctions mesurables	1101
14.13.3	Propriétés d'unicité	1102
14.13.4	Régularité	1104
14.14	Propriétés de l'intégrale de Lebesgue	1104
14.14.1	Quelques limites dans les bornes	1105
14.14.2	Mesure de comptage et série	1106
14.14.3	Théorème de la moyenne	1107
14.14.4	Primitives et intégrales	1108
14.14.5	Exemples et applications	1109
14.14.6	Permuter limite et dérivée	1110
14.14.7	Intégrales impropres	1112
14.15	Changement de variables dans une intégrale multiple	1115
14.15.1	Des lemmes	1115
14.15.2	Déterminant et mesure de Lebesgue	1116
14.15.3	Le théorème et sa démonstration	1117
14.15.4	Exemples	1122
14.16	Changement d'espace mesuré	1122
14.17	Théorème de Fubini-Tonelli et de Fubini	1123
15	Suites et séries de fonctions (Vol 2)	1133
15.1	Séries de fonctions	1133
15.1.1	Intégration de séries de fonctions	1133
15.1.2	Différentiabilité	1134
15.2	Séries entières	1139
15.2.1	Disque de convergence	1139
15.2.2	Somme et produit de séries	1142
15.2.3	Convergence normale	1147
15.2.4	Dérivation	1150
15.2.5	Intégration	1153
15.3	Séries de Taylor	1153
15.3.1	Polynôme de Taylor d'une série entière	1153

15.3.2	Une majoration pour le reste	1154
15.3.3	Fonctions analytiques	1155
15.4	Algèbre engendrée par une matrice	1156
15.5	Exponentielle sur une algèbre normée	1157
15.5.1	Définition	1157
15.5.2	Différentielles	1159
15.5.3	Exponentielle de matrice	1162
15.6	Exponentielle et logarithme dans les réels	1165
15.6.1	L'équation différentielle	1165
15.6.2	Existence	1166
15.6.3	Le nombre de Neper e	1167
15.6.4	Application réciproque : logarithme	1167
15.6.5	Approximations numériques de e	1169
15.6.6	Résumé des propriétés de l'exponentielle	1170
15.6.7	Dérivée de la fonction puissance	1171
15.6.8	Dérivée du logarithme	1172
15.6.9	Taylor pour l'exponentielle	1172
15.6.10	Analycité	1173
15.6.11	Autres propriétés et petits calculs	1173
15.6.12	Taylor pour le logarithme	1174
15.6.13	Développements et calcul de limites	1177
15.7	Vitesses des puissances, de l'exponentielle et du logarithme	1178
15.7.1	Un peu de théorie	1178
15.7.2	Nombres premiers	1182
15.7.3	Quelques limites	1184
15.8	Trigonométrie hyperbolique	1185
15.9	Séries entières de matrices	1187
15.9.1	Différentiabilité	1187
15.10	Exponentielle de matrices	1189
15.10.1	Diagonalisabilité d'exponentielle	1190
15.11	Étude d'asymptote	1192
15.12	Développement en série	1193
15.12.1	Série génératrice d'une suite	1193
15.12.2	Développement en série et Taylor	1193
15.12.3	Resommer une série	1195
15.13	Séries entières de matrices	1200
15.13.1	Rayon de convergence	1200
15.13.2	Convergence et rayon spectral	1200
15.13.3	Exponentielle et logarithme de matrice	1202
15.13.4	Calcul effectif de l'exponentielle d'une matrice	1205
15.14	Lemme de Borel	1206
15.14.1	Fonctions plateaux, Urysohn, partition de l'unité	1206
15.14.2	Lemme de Urysohn	1208
15.14.3	Partition de l'unité	1209
15.14.4	Le lemme de Borel	1210
15.15	Nombres de Bell	1212
16	Représentations et caractères (Vol 2)	1217
16.1	Représentations et caractères	1217
16.1.1	Crochet de dualité et transformée de Fourier	1219
16.1.2	Groupes non abéliens	1220
16.1.3	Représentations linéaires des groupes finis	1220
16.1.4	Module	1221
16.1.5	Structure hermitienne	1223

16.1.6	Caractères	1224
16.2	Équivalence de représentations et caractères	1224
16.2.1	Représentation régulière	1227
16.2.2	Caractères et représentations : suite et fin	1228
16.3	Représentation produit tensoriel	1230
16.4	Exemple sur le groupe symétrique	1231
16.5	Table des caractères du groupe symétrique S_4	1231
16.5.1	Calculs à partir de rien ou presque	1231
16.5.2	À propos de la représentation ρ_s	1233
16.5.3	À propos de la représentation ρ_u	1234
17	Encore de l'analyse (et c'est pas fini) (Vol 3)	1237
17.1	Densité des polynômes	1237
17.2	Primitive et intégrale	1237
17.2.1	Théorème taubérien de Hardy-Littlewood	1238
17.2.2	Théorème de Müntz	1241
17.3	Intégrales convergeant uniformément	1244
17.3.1	Définition et propriété	1244
17.3.2	Critères de convergence uniforme	1245
17.4	Fonctions définies par une intégrale	1245
17.4.1	Continuité sous l'intégrale	1246
17.4.2	Le coup du compact	1247
17.4.3	Dérivabilité sous l'intégrale	1248
17.4.4	Absolue continuité	1250
17.4.5	Différentiabilité sous l'intégrale	1252
17.5	Deux théorèmes de point fixe	1255
17.5.1	Points fixes attractifs et répulsifs	1255
17.5.2	Picard	1256
17.6	Théorèmes de point fixes et équations différentielles	1259
17.6.1	Théorème de Cauchy-Lipschitz	1259
17.7	Théorèmes d'inversion locale et de la fonction implicite	1266
17.7.1	Mise en situation	1266
17.7.2	Théorème d'inversion locale	1267
17.7.3	Théorème de la fonction implicite	1270
17.7.4	Exemple	1272
17.8	Décomposition polaire (régularité)	1274
17.9	Théorème de Von Neumann	1276
17.10	Recherche d'extrémums	1278
17.10.1	Extrema à une variable	1278
17.10.2	Extrema libre	1279
17.10.3	Extrema et Hessienne	1281
17.10.4	Un peu de recettes de cuisine	1283
17.10.5	Extrema liés	1283
17.11	Fonctions convexes	1285
17.11.1	Inégalité des pentes	1286
17.11.2	Convexité et régularité	1287
17.11.3	Dérivées d'une fonction convexe	1287
17.11.4	Graphes d'une fonction convexe	1289
17.11.5	Convexité et hessienne	1294
17.11.6	Quelques inégalités	1300
17.12	Trucs et astuces de calcul d'intégrales	1306
17.12.1	Quelques intégrales « usuelles »	1306
17.12.2	Reformer un carré au dénominateur	1308
17.12.3	Décomposition en fractions simples	1309

17.13	Algorithme du gradient à pas optimal	1309
17.14	Formes quadratiques, signature, et lemme de Morse	1313
17.15	Ellipsoïde de John-Loewner	1317
17.16	Prolongement de fonctions	1323
17.16.1	Encore du prolongement	1325
17.17	Complétion d'un espace métrique	1327
17.17.1	Principe des zéros isolés	1329
17.18	Un petit extra	1330
18	Trigonométrie, isométries (Vol 3)	1333
18.1	Trigonométrie	1333
18.1.1	Définitions, périodicité et quelques valeurs remarquables	1333
18.1.2	Fonction puissance (pour les complexes)	1334
18.1.3	Formules de trigonométrie	1336
18.2	Très modeste approximation de π	1346
18.3	Cercle trigonométriques	1347
18.3.1	Les fonctions tangente et arc tangente	1348
18.3.2	La fonction arc sinus	1350
18.3.3	La fonction arc cosinus	1352
18.3.4	Une meilleure approximation de π	1353
18.3.5	Forme trigonométrique des nombres complexes	1354
18.3.6	Angle entre deux vecteurs	1354
18.3.7	Aire du parallélogramme	1356
18.4	Paramétrisation du cercle	1357
18.4.1	Bijection continue	1358
18.4.2	Inverse	1359
18.4.3	Cercle trigonométrique	1360
18.4.4	Du point de vue de la tribu, mesure et co.	1360
18.5	Exemples trigonométriques	1363
18.5.1	Quelques équations trigonométriques	1363
18.5.2	Développements en série	1364
18.5.3	Intégration	1366
18.5.4	Changement de variables dans une intégrale	1366
18.6	Isométries de l'espace euclidien	1367
18.6.1	Structure du groupe $\text{Isom}(\mathbb{R}^n)$	1367
18.7	Isométries dans $\mathbb{R}^n$	1369
18.8	Groupes finis d'isométries	1373
18.8.1	Groupe diédral	1375
18.8.2	Applications : du dénombrement	1383
18.8.3	Points fixés par une affinité	1384
18.9	Classification des isométries dans $\mathbb{R}^2$	1384
18.9.1	Réflexions	1384
18.9.2	Segment, plan médiateur et équidistance	1386
18.9.3	Translations et réflexions	1387
18.9.4	Rotations	1388
18.9.5	Rotation d'un angle donné	1391
18.9.6	Rotations vectorielles	1392
18.9.7	Matrice des transformations orthogonales	1395
18.9.8	Rotations, $\text{SO}(2)$ et matrice de rotation	1397
18.9.9	Rotation et application affine	1398
18.9.10	Angle entre deux droites	1399
18.9.11	Angle orienté	1399
18.9.12	Angles et nombres complexes	1402
18.9.13	Classification	1405

18.9.14	Classification des isométries de $\mathbb{R}$	1408
18.9.15	Isométries du tétraèdre régulier	1409
18.9.16	Représentation de S_4 via les isométries du tétraèdre	1410
18.10	Transformations de Lorentz	1411
18.10.1	Sous-groupe fini d'isométries du plan	1414
18.10.2	Relations trigonométriques dans un triangle rectangle	1418
18.10.3	Pavages du plan	1419
18.11	Un peu de structure de $O(n)$	1435
18.11.1	Valeurs propres dans $O(n)$	1435
18.11.2	Sous-groupes finis de $SO(3)$	1438
18.12	Systèmes de coordonnées	1447
18.12.1	Coordonnées polaires	1447
18.12.2	Coordonnées cylindriques	1454
18.12.3	Coordonnées sphériques	1455
18.13	Calcul de limites	1456
18.13.1	Méthode des coordonnées polaires	1457
18.13.2	Méthode du développement asymptotique	1460
18.14	Quelques intégrales avec de la trigonométrie	1461
18.14.1	Changement de variables	1461
18.14.2	Coordonnées polaires	1462
18.14.3	Coordonnées cylindriques	1464
18.14.4	Coordonnées sphériques	1465
18.14.5	Un autre système utile	1465
18.15	Aire d'une surface de révolution	1467
18.16	Table de caractères du groupe diédral	1468
18.16.1	Représentations de dimension un	1468
18.16.2	Représentations de dimension deux	1469
18.16.3	Le compte pour n pair	1471
18.16.4	Le compte pour n impair	1471
19	Corps finis, racines de l'unité (Vol 3)	1473
19.1	Le groupe des racines de l'unité dans les nombres complexes	1473
19.1.1	Le groupe	1473
19.1.2	Fonction indicatrice d'Euler (première partie)	1475
19.1.3	Introduction par les racines de l'unité	1475
19.1.4	Générateurs	1477
19.1.5	Fonction indicatrice d'Euler (propriétés)	1477
19.1.6	Décomposition en éléments simples	1477
19.2	Chiffrement RSA	1478
19.2.1	Mise en place par Bob	1479
19.2.2	Chiffrement	1479
19.2.3	Déchiffrement	1479
19.2.4	Une imprudence à ne pas commettre	1480
19.2.5	Problèmes calculatoires	1480
19.2.6	La solidité de RSA	1481
19.2.7	Note non mathématique pour doucher l'enthousiasme	1481
19.3	Polynômes cyclotomiques	1481
19.3.1	Définitions et propriétés	1481
19.3.2	Nombres premiers	1485
19.4	Corps finis	1487
19.4.1	Théorème de Wedderburn	1487
19.4.2	Existence, unicité	1489
19.4.3	Symboles de Legendre et carrés	1491
19.4.4	Théorème de Chevalley-Waring	1497

19.4.5	Contenu d'un polynôme	1499
19.4.6	Théorème de l'élément primitif	1500
19.4.7	Construction de $\mathbb{F}_q$	1504
19.4.8	Exemple : étude de $\mathbb{F}_{16}$	1507
19.4.9	Polynômes irréductibles sur $\mathbb{F}_q$	1509
19.4.10	Matrices	1511
19.5	Constructions à la règle et au compas	1513
19.5.1	Quelques constructions	1513
19.5.2	Nombres constructibles	1515
19.5.3	Polygones constructibles	1517
20	Intégration sur des variétés (Vol 3)	1523
20.1	Variétés	1523
20.1.1	Introduction	1523
20.1.2	Définition, carte	1523
20.1.3	Ancienne définition	1524
20.1.4	Espace tangent	1526
20.2	Intégration	1526
20.2.1	Le problème pour une intégration globale	1526
20.2.2	Intégrale sur une carte	1526
20.2.3	Quelques expressions pour l'élément de volume	1529
20.3	Intégrale sur une variété	1530
20.3.1	Mesure sur une carte	1530
20.3.2	Intégrale sur une carte	1531
20.3.3	Exemples	1532
20.3.4	Orientation	1532
20.3.5	Formes différentielles	1534
20.3.6	Intégrale d'une fonction sur une sous-variété	1535
20.4	Longueur, aire, volumes etc.	1536
20.4.1	Quelques aires faciles	1536
20.5	Autres théorèmes de points fixes	1538
20.5.1	Brouwer	1538
20.5.2	Théorème de Schauder	1540
20.5.3	Théorème de Cauchy-Arzella	1541
20.5.4	Théorème de Markov-Kakutani et mesure de Haar	1542
20.6	Intégrales curvilignes	1543
20.6.1	Chemins de classe C^1	1543
20.6.2	Intégrer une fonction	1544
20.6.3	Intégrer un champ de vecteurs	1545
20.6.4	Intégrer une forme différentielle sur un chemin	1546
20.6.5	Intégration d'une forme différentielle sur un chemin	1546
20.6.6	Interprétation physique : travail	1548
20.6.7	Intégrer un champ de vecteurs sur un bord en $2D$	1549
20.6.8	Intégrer une forme différentielle sur un bord en $2D$	1549
20.6.9	Intégrer une forme différentielle sur un bord en $3D$	1549
20.6.10	Intégrer un champ de vecteurs sur un bord en $3D$	1549
20.6.11	Dérivées croisées et forme différentielle exacte	1550
20.7	Surfaces paramétrées	1551
20.7.1	Graphe d'une fonction	1552
20.7.2	Intégrale sur une partie de $\mathbb{R}^m$	1553
20.8	Intégrales de surface	1554
20.8.1	Intégrale d'un champ de vecteurs	1554
20.9	Intégrales de surface	1554
20.9.1	Aire d'une surface paramétrée	1554

20.9.2	Intégrale d'une fonction sur une surface	1556
20.9.3	Intégrale d'une 2-forme	1556
20.10	Flux d'un champ de vecteurs à travers une surface	1557
20.11	Divergence, Green, Stokes	1559
20.11.1	Théorème de la divergence	1560
20.11.2	Formule de Green	1561
20.11.3	Formule de Stokes	1562
20.12	Résumé des intégrales vues	1563
20.12.1	L'intégrale d'une fonction sur les réels	1563
20.12.2	Intégrale d'une fonction sur un chemin	1564
20.12.3	Intégrale d'une fonction sur une surface	1564
20.12.4	Intégrale d'une fonction sur un volume	1564
20.12.5	Conclusion pour les fonctions	1565
20.12.6	Circulation d'un champ de vecteurs	1565
20.12.7	Flux d'un champ de vecteurs	1565
20.12.8	Conclusion pour les champs de vecteurs	1566
20.12.9	Attention pour les surfaces fermées !	1566
20.13	Formes différentielles exactes et fermées	1568
20.14	Théorème d'Abel angulaire	1570
20.14.1	Passage à la limite sous le signe intégral	1573
20.14.2	Intégrale en dimension un	1573
20.14.3	Intégrales convergentes	1574
20.14.4	La méthode de Rothstein-Trager	1574
20.15	Rappel sur les intégrales usuelles	1580
20.16	Intégrales le long de chemins	1580
20.16.1	Circulation d'un champ de vecteur	1580
20.17	Circulation d'un champ conservatif	1582
20.18	Intégration de fonction à deux variables	1584
20.18.1	Intégration sur un domaine rectangulaire	1584
20.18.2	Intégration sur un domaine non rectangulaire	1585
20.18.3	Changement de variables	1587
20.19	Les intégrales triples	1587
20.19.1	Volume	1589
20.20	Un petit peu plus formel	1590
20.20.1	Intégration sur un domaine non rectangulaire	1590
20.21	Aire et primitive	1592
20.21.1	Longueur d'arc de courbe	1592
20.21.2	Aire de révolution	1593
20.22	L'aire en dessous d'une courbe	1593
20.23	Propriétés des intégrales	1594
20.24	Techniques d'intégration	1595
20.24.1	Intégration par parties	1596
20.24.2	Changement de variables – pour trouver des primitives	1597
20.24.3	Changement de variables – pour calculer des intégrales	1599
20.24.4	Intégrations des fractions rationnelles réduites	1601
20.24.5	Quelques formules à connaître	1601
20.24.6	Approximation de $\ln(2)$	1602
20.25	Constructions plus naïves de l'intégrale dans le cas réel	1605
20.25.1	Mesure de Lebesgue, version rapide	1605
20.25.2	Pavés et subdivisions	1606
20.25.3	Intégrale d'une fonction en escalier	1609
20.25.4	Intégrales partielles	1609
20.25.5	Réduction d'une intégrale multiple	1610

20.25.6	Propriétés de l'intégrale	1611
20.25.7	Intégrales multiples, cas général	1612
20.25.8	Réduction d'une intégrale multiple	1613
20.25.9	Intégrales sur des parties de $\mathbb{R}^2$	1614
20.25.10	Intégrales sur des parties de $\mathbb{R}^3$	1617
20.25.11	Fonctions et ensembles non bornés	1619
20.25.12	Lemme de Morse	1620
20.26	Autres intégrales sympathiques	1622
20.26.1	Intégrale de Wallis	1622
20.26.2	Formule de Stirling	1626
20.26.3	La fonction sinus cardinal, intégrale de Dirichlet	1629
21	Arcs paramétrés (Vol 3)	1639
21.1	Définitions	1639
21.2	Longueur d'arc	1639
21.3	Abscisse curviligne	1642
21.3.1	Formule intégrale de la longueur	1643
21.4	Suite du chapitre	1648
21.5	Autres exemples	1649
21.6	Élément de longueur	1650
21.6.1	Élément de longueur : cartésiennes	1650
21.6.2	Élément de longueur : polaires (1)	1651
21.6.3	Élément de longueur : polaires (2)	1651
21.6.4	Approximation de la longueur par des cordes	1653
21.7	Arc géométrique	1655
21.7.1	Abscisse curviligne et paramétrage normal	1656
21.7.2	Tangente à une courbe paramétrée	1661
21.8	Un peu de topologie	1662
21.9	Repère de Frenet	1665
21.9.1	Torsion	1667
21.10	Hors des coordonnées normales	1668
21.11	Tracer des courbes paramétriques dans $\mathbb{R}^2$	1671
21.12	Courbes planes	1672
21.12.1	Angle	1672
21.12.2	Courbure signée	1673
21.12.3	Degré, indice et homotopie	1676
21.13	Courbes fermées planes	1682
21.13.1	Cercle circonscrit	1682
21.13.2	Description locale	1684
21.13.3	Enveloppe convexe	1685
21.13.4	Courbure et convexité	1688
21.13.5	Théorème des quatre sommets	1689
21.13.6	Le théorème de Jordan	1691
22	Géométrie hyperbolique (Vol 3)	1693
22.1	Inversion	1693
22.1.1	Cercles perpendiculaires	1693
22.1.2	Inversion	1694
23	Espaces projectifs (Vol 3)	1699
23.1	Sous espaces projectifs	1699
23.2	Espace projectifs comme « complétés » d'espaces affines	1701
23.3	Théorème de Pappus	1704
23.4	Homographies	1705

23.4.1	Homographies	1705
23.4.2	Le groupe projectif	1706
23.4.3	Repères projectifs	1707
23.4.4	Identifications $P(\mathbb{K}^2)$ vers $\mathbb{K} \cup \{\infty\}$	1711
23.4.5	Birapport	1712
23.5	Coordonnées homogènes	1718
23.5.1	Curiosité : matrice de translation	1718
23.5.2	Dualité	1719
23.5.3	Polynômes	1720
23.6	La sphère de Riemann $P_1(\mathbb{C})$	1722
23.6.1	Éléments de géométrie dans $P_1(\mathbb{C})$	1723
23.6.2	Homographies	1726
23.6.3	Birapport	1732
23.6.4	Division harmonique	1735
23.6.5	Groupe circulaire	1739
23.6.6	Action du groupe modulaire	1741
24	Analyse vectorielle (Vol 3)	1747
24.1	Le théorème de Green	1747
24.2	Théorème de la divergence dans le plan	1751
24.2.1	La convention de sens de parcours	1751
24.2.2	Théorème de la divergence	1752
24.3	Théorème de Stokes	1752
24.4	Théorème de Gauss	1754
24.5	Coordonnées curvilignes	1756
24.5.1	Base locale	1756
24.5.2	Importance de l'orthogonalité	1756
24.5.3	Coordonnées polaires	1758
24.5.4	Coordonnées cylindriques	1758
24.5.5	Coordonnées sphériques	1759
24.5.6	Gradient en coordonnées curvilignes	1759
24.5.7	Divergence en coordonnées curvilignes	1760
24.5.8	Laplacien en coordonnées curvilignes orthogonales	1763
24.5.9	Rotationnel en coordonnées curvilignes orthogonales	1763
24.6	Les formules	1764
24.6.1	Coordonnées polaires	1764
24.6.2	Coordonnées cylindriques	1764
24.6.3	Coordonnées sphériques	1765
25	Espaces de Hilbert (Vol 3)	1767
25.1	Espaces de Hilbert	1767
25.1.1	Sous-espace vectoriel fermé ???	1768
25.2	Théorème de la projection	1769
25.3	Systèmes orthogonaux et bases	1772
25.3.1	Orthogonal d'une partie	1772
25.3.2	Dual, théorème de représentation de Riesz	1773
25.3.3	Séparabilité	1775
25.3.4	Base hilbertienne	1777
25.3.5	Décomposition dans une base hilbertienne	1781
25.3.6	Digression sur les normes opérateurs	1786
25.3.7	Applications linéaires et continuité	1787
25.4	Théorème de Kochen-Specker	1789
25.5	Théorème de Lax-Milgram	1790

26 Analyse complexe (Vol 3)	1795
26.1 Fonctions holomorphes	1795
26.1.1 Équations de Cauchy-Riemann	1795
26.1.2 Intégrales sur des chemins fermés	1797
26.1.3 Lacets, indice et homotopie	1799
26.1.4 Théorème de Cauchy et analytité	1800
26.1.5 Théorème de Brouwer en dimension 2	1803
26.1.6 Principe des zéros isolés	1804
26.1.7 Prolongement de fonctions holomorphes	1806
26.1.8 Théorème de Runge	1807
26.2 Intégrales de fonctions holomorphes	1809
26.2.1 Mesure de Radon	1813
26.3 Conditions équivalentes à l'holomorphicité	1814
26.4 Singularités, pôles et méromorphe	1815
26.5 Dénombrement des solutions d'une équation diophantienne	1818
26.6 Fonctions d'Euler	1824
26.6.1 Euler et factorielle	1827
26.7 Exponentielle et logarithme complexe	1828
26.7.1 Propriétés de l'exponentielle	1828
26.7.2 Intégrale de Fresnel	1829
26.7.3 Logarithme complexe	1831
26.8 Théorème de Weierstrass	1840
27 Analyse fonctionnelle (Vol 4)	1843
27.1 Théorème d'isomorphisme de Banach	1843
27.2 Théorème d'Ascoli	1843
27.3 Espaces de Lebesgue L^p	1845
27.3.1 Généralités	1845
27.3.2 Un peu de convergence de suites	1848
27.3.3 L'espace L^∞	1850
27.3.4 Quelques identifications	1851
27.3.5 Inégalité de Young, Jensen, Hölder et de Minkowski	1852
27.3.6 Ni inclusions ni inégalités	1859
27.3.7 Complétude	1861
27.3.8 Théorèmes d'approximation	1866
27.3.9 Densité des fonctions infiniment dérivables à support compact	1867
27.3.10 Approximation	1870
27.4 Convolution	1871
27.4.1 Approximation de l'unité	1874
27.4.2 Densité des polynômes trigonométriques	1877
27.5 Espaces L^2 , généralités	1878
27.6 L'espace $L^2(\mathbb{R}^d)$	1880
27.7 L'espace $L^2(S^1)$	1880
27.7.1 Espace mesuré	1881
27.7.2 Topologie	1882
27.7.3 Système trigonométrique	1887
27.7.4 Convolution	1888
27.7.5 Approximation de l'unité	1891
27.7.6 Base hilbertienne (suite des polynômes trigonométriques)	1895
27.7.7 Convolution, bis	1896
27.8 L'espace $L^2([a, b])$	1896
27.9 Sur $[0, 2\pi[$	1900
27.10 Sur $[-T, T[$	1900
27.10.1 Le cas dans $[0, 2\pi]$	1900

27.11	Théorème de la projection normale	1902
27.11.1	Espace uniformément convexe	1902
27.11.2	Des inégalités	1905
27.11.3	Inégalités de Clarkson	1911
27.11.4	Uniforme convexité des espaces de Lebesgue	1913
27.11.5	Théorème de la projection normale	1914
27.12	Théorèmes de Hahn-Banach	1915
27.12.1	Applications $\mathbb{R}$ -linéaires et $\mathbb{C}$ -linéaires	1915
27.12.2	Hahn-Banach	1918
27.12.3	Prolongement de fonctionnelles (cas fini)	1920
27.13	Théorème de Tietze	1924
27.14	Dualité, réflexivité et théorème de représentation de Riesz	1927
27.15	Espace de Schwartz	1938
27.15.1	Topologie	1939
27.15.2	Produit de convolution	1942
27.16	Théorème de Montel	1942
27.17	Espaces de Bergman	1943
28	Séries de Fourier (Vol 4)	1947
28.1	Densité des polynômes trigonométriques	1947
28.1.1	Convergence pour les fonctions continues (via Weierstrass)	1947
28.1.2	Convergence pour les fonctions continues (via Fejér)	1947
28.1.3	Densité dans L^p	1950
28.1.4	Suite équirépartie, critère de Weyl	1951
28.2	Fonctions de Dirichlet	1953
28.3	Coefficients et série de Fourier	1954
28.3.1	Le contre-exemple que nous attendions tous	1957
28.3.2	Inégalité isopérimétrique	1959
28.3.3	À propos des coefficients	1960
29	Transformation de Fourier (Vol 4)	1961
29.1	Transformée de Fourier sur $L^1(\mathbb{R}^d)$	1962
29.1.1	Formule sommatoire de Poisson	1965
29.2	Suite régularisante	1968
29.3	Transformée de Fourier dans l'espace de Schwartz	1969
29.3.1	Quelques transformées de Fourier	1972
29.3.2	Formule d'inversion	1974
29.4	Transformée de Fourier sur $L^2(\mathbb{R}^d)$	1978
29.4.1	Le problème	1978
29.4.2	Extension de $L^1 \cap L^2$ vers L^2	1979
30	Distributions (Vol 4)	1983
30.1	Dérivée faible	1984
30.1.1	Dérivée partielle au sens faible	1984
30.1.2	Dérivée faible partielle	1986
30.2	Topologie et convergence sur des espaces de fonctions	1987
30.3	Distributions	1990
30.3.1	Multiplication d'une distribution par une fonction	1991
30.3.2	Dérivée de distribution	1991
30.3.3	Ordre et support d'une distribution	1993
30.4	L'espace $C^\infty(\mathbb{R}, \mathcal{D}'(\mathbb{R}^d))$	1995
30.4.1	Dérivation	1998
30.5	Une équation de distribution	1998
30.6	Localisation, principe de recollement	1999

30.7	Permuter distributions, dérivées et intégrales	2004
30.8	Distributions tempérées	2009
30.8.1	Topologie	2010
30.8.2	Distributions associées à des fonctions	2011
30.8.3	Composition avec une fonction	2011
30.8.4	Transformée de Fourier d'une distribution tempérée	2011
30.8.5	Convolution d'une distribution par une fonction	2012
30.8.6	Approximation de la distribution de Dirac	2012
30.8.7	Peigne de Dirac	2015
30.9	L'espace $C^\infty(\mathbb{R}, \mathcal{S}'(\mathbb{R}^d))$	2016
30.9.1	Propriétés générales	2017
30.9.2	Dérivation	2019
31	Espaces de Sobolev, équations elliptiques (Vol 4)	2023
31.1	Espaces de Sobolev	2023
31.1.1	Sur un intervalle de $\mathbb{R}$	2023
31.1.2	Sur un ouvert de $\mathbb{R}^n$	2028
31.1.3	Espace de Sobolev fractionnaire	2030
31.2	Trace	2032
31.3	Théorème de plongement	2035
32	Équations différentielles ordinaires (Vol 4)	2039
32.1	Équation homogène, solution particulière	2040
32.2	Que faire avec $f(z)dz = g(t)dt$?	2040
32.3	Équations linéaires du premier ordre	2041
32.3.1	Pourquoi la variation des constantes fonctionne toujours ?	2043
32.4	Équations à variables séparées	2044
32.4.1	La méthode rapide	2044
32.4.2	La méthode plus propre	2045
32.4.3	Les théorèmes	2045
32.5	Équations linéaires d'ordre supérieur	2047
32.5.1	Équations et systèmes linéaires à coefficients constants	2047
32.5.2	Si les coefficients ne sont pas constants ?	2047
32.6	Système d'équations linéaires	2048
32.6.1	La magie de l'exponentielle.	2048
32.6.2	... mais la difficulté	2048
32.6.3	La recette	2048
32.6.4	Système d'équations linéaires avec matrice constante	2049
32.6.5	Système d'équations linéaires avec matrice non constante	2050
32.7	Réduction de l'ordre	2050
32.8	Autour de Cauchy-Lipschitz	2052
32.8.1	Fuite des compacts et explosion en temps fini	2052
32.8.2	Écart entre deux conditions initiales	2054
32.8.3	Flot d'un champ de vecteurs	2055
32.8.4	Stabilité de Lyapunov	2068
32.8.5	Système proies-prédateurs de Lotka-Volterra	2072
32.9	Équation du second ordre	2075
32.9.1	Wronskien	2075
32.9.2	Avec second membre	2076
32.9.3	Équation $y'' + q(t)y = 0$	2076
32.9.4	Équation de Hill	2078
32.10	Différents types d'équations différentielles	2081
32.10.1	Équation homogène	2081
32.10.2	Équation de Bernoulli	2081

32.10.3	Équation de Riccati	2082
32.10.4	Équation différentielle exacte	2082
32.11	Distributions pour les équations différentielles	2083
32.11.1	Équation de Schrödinger	2083
32.12	Équations différentielles du premier ordre	2087
32.13	Premier ordre, variables séparables	2089
32.14	Équations différentielles linéaires du premier ordre	2091
32.14.1	Méthode de variation de la constante	2093
32.15	Équations différentielles linéaires du second ordre	2094
32.15.1	Équations différentielles linéaires du second ordre homogènes à coefficients constants	2095
32.15.2	Linéaires du second ordre à coefficients constants, non homogènes	2096
32.16	Fonction de Green	2098
33	Équations aux dérivées partielles (Vol 4)	2101
33.1	Symbole principal, équation des caractéristiques	2101
33.2	Méthode des caractéristiques pour l'ordre 1	2101
33.2.1	Un exemple complet un peu minimal	2102
33.2.2	Un théorème d'existence et d'unicité	2104
33.3	Méthode des caractéristiques pour l'ordre 2	2107
33.3.1	Principe général	2107
33.3.2	Exemple : l'équation d'onde	2108
33.4	Classification des équations du second ordre	2110
33.4.1	Problème au limite	2111
33.5	Principe du maximum	2112
33.6	Quelques exemples	2115
33.6.1	Un changement de variables	2115
34	Numérique (Vol 4)	2119
34.1	Introduction	2119
34.2	Représentations numériques	2119
34.2.1	Entier relatif en complément à deux (binaire)	2119
34.2.2	Représentation en virgule flottante	2121
34.2.3	Simple précision, IEEE-754	2121
34.3	Problèmes pour écrire des nombres	2124
34.3.1	Troncature : la base	2124
34.3.2	Troncature : le drift	2125
34.3.3	Quelques bonnes règles	2126
34.3.4	Erreur de "cancellation"	2126
34.3.5	Calcul d'une dérivée	2128
34.3.6	Erreur d'absorption	2128
34.4	Conditionnement et stabilité	2129
34.4.1	Comment choisir et penser le K ?	2132
34.5	Un peu de points fixes	2133
34.5.1	Choix de la fonction à point fixe	2133
34.5.2	Convergence quadratique	2134
34.5.3	Convergence	2136
34.6	Méthode de Newton	2137
34.6.1	« Justification » par la formule par Taylor	2137
34.6.2	« Justification » par points fixes	2138
34.6.3	Convergence de la méthode de Newton	2138
34.6.4	Racine carré par la méthode de Newton	2140
34.6.5	Formalisation de l'algorithme	2140
34.6.6	Caractéristiques	2141

34.6.7	Exemple de la racine carrée	2142
34.6.8	Si multiplicité	2143
34.6.9	Et la dérivée ?	2143
34.6.10	Méthode de Newton : le cas général	2143
34.7	Estimation de l'ordre de convergence	2145
34.8	Autres méthodes	2146
34.8.1	Méthode de Schröder	2146
34.8.2	Halley	2146
34.9	Méthode des sécantes variables	2146
34.9.1	Aitken	2147
34.10	Équations algébrique	2148
34.10.1	Résoudre un système linéaire	2148
34.10.2	Caractéristiques	2148
34.10.3	Définitions	2149
34.11	Équations non linéaires	2149
34.11.1	Méthode de bisection	2151
34.12	Efficacité	2153
34.13	Exemples sous forme d'exercices	2153
34.14	Approximations de fonctions	2157
34.14.1	Critère d'interpolation	2157
34.14.2	Base de Newton	2158
34.14.3	Méthode des minimums quadratiques	2159
34.14.4	Notre espace de Hilbert	2160
34.14.5	Droite de régression	2161
34.15	Conditionnement d'une matrice	2162
34.15.1	Perturbation du vecteur	2164
34.15.2	Perturbation de la matrice	2166
34.16	Système linéaires (généralités)	2167
34.16.1	Les méthodes directes	2167
34.16.2	Méthodes itératives	2168
34.17	Système linéaires (méthodes directes)	2168
34.17.1	Inversion de matrice triangulaire	2168
34.17.2	Transformation gaussienne	2169
34.17.3	Méthode de Gauss pour résoudre des systèmes d'équations linéaires	2170
34.17.4	Méthode de Gauss sans pivot (décomposition LU)	2171
34.17.5	Matrice de permutation élémentaire	2175
34.18	Méthode de Gauss avec pivot partiel (décomposition PLU)	2176
34.18.1	L'idée	2176
34.18.2	Le théorème	2177
34.18.3	D'un point de vue algorithmique	2180
34.18.4	Exemples	2182
34.19	Résolution de systèmes linéaires (suite)	2185
34.19.1	Déterminant	2185
34.19.2	Plusieurs termes indépendants	2185
34.19.3	Cholesky	2186
34.20	Système linéaire (méthodes itératives)	2189
34.20.1	La méthode générale	2190
34.20.2	Jacobi	2190
34.20.3	Gauss-Seidel	2190
34.20.4	Autres	2190
34.21	Indices connectés, matrice irréductible	2190
34.22	Localisation des valeurs propres	2192
34.22.1	Matrices à diagonale dominante	2194

34.22.2	M-matrice	2197
35	Méthode des différences finies (Vol 4)	2201
35.1	Problèmes de dimension un	2201
35.1.1	Un schéma à cinq points	2202
35.1.2	Exemple	2206
35.2	Problèmes de dimension deux	2207
35.2.1	Discrétisation en croix	2207
35.2.2	Discrétisation en carré	2208
35.2.3	Résolution de la discrétisation en croix	2209
35.3	Consistance, convergence	2211
35.3.1	Définitions, mise en place	2211
35.3.2	Exemple	2213
35.3.3	Consistance, stabilité et convergence	2214
35.3.4	Exemple : schéma à cinq points, laplacien en croix	2215
35.4	Autres laplaciens	2216
35.4.1	Travail avec le laplacien à 9 points	2219
36	Variables aléatoires et théorie des probabilités (Vol 4)	2221
36.1	Espace de probabilité	2221
36.2	Variables aléatoires	2222
36.2.1	Indépendance	2222
36.2.2	Lois conjointes et indépendance	2225
36.2.3	Somme et produit de variables aléatoires indépendantes	2226
36.2.4	Espérance	2228
36.2.5	Variance	2229
36.2.6	Covariance	2230
36.2.7	Probabilité conditionnelle : événements	2231
36.2.8	Espérance conditionnelle	2233
36.2.9	Probabilité conditionnelle : tribu	2240
36.2.10	Variables de Rademacher indépendantes	2243
36.2.11	Un petit paradoxe	2244
36.2.12	Inégalité de Jensen	2251
36.2.13	Fonction de répartition	2251
36.2.14	Fonction caractéristique	2252
36.2.15	Fonction génératrice des moments, transformée de Laplace	2253
36.2.16	Loi d'une variable aléatoire	2254
36.2.17	Changement de variables	2255
36.3	Convergence	2255
36.4	Loi des grands nombres, théorème central limite	2261
36.4.1	Loi des grands nombres	2261
36.4.2	Théorème central limite	2263
36.4.3	Marche aléatoire	2266
36.5	Les lois usuelles	2267
36.5.1	Loi de Bernoulli	2267
36.5.2	Loi binomiale	2267
36.5.3	Loi multinomiale	2268
36.5.4	Loi géométrique	2269
36.5.5	Loi de Poisson	2269
36.5.6	Loi exponentielle	2270
36.5.7	Approximation de la binomiale par une Poisson	2272
36.5.8	Loi de Poisson et loi exponentielle	2273
36.5.9	Loi normale	2275
36.5.10	Vecteurs gaussiens	2276

36.5.11	Variable aléatoire de Rademacher	2280
36.5.12	Loi de Student	2282
36.5.13	Indépendance, covariance et variance de somme	2283
36.6	Estimation des grands écarts	2283
36.7	Simulations de réalisations de variables aléatoires	2287
36.7.1	Générateur uniforme	2287
36.7.2	Simulation par inversion	2287
36.7.3	Algorithme de Box-Muller	2288
36.7.4	Méthode du rejet	2289
36.7.5	Simuler une loi géométrique à l'ordinateur	2291
36.7.6	Simuler une loi exponentielle à l'ordinateur	2291
36.7.7	Simuler une loi de Poisson à l'ordinateur	2291
36.8	Sage	2292
36.8.1	Loi exponentielle	2292
36.8.2	Inverser des lois	2292
36.9	Monte-Carlo	2293
36.9.1	Intervalle de confiance	2294
36.10	Résultats qui se démontrent avec des variables aléatoires	2296
36.10.1	Nombres normaux	2296
36.10.2	Théorème de Bernstein	2298
37	Statistiques (Vol 4)	2303
37.1	Notations et hypothèses	2303
37.2	Modèle statistique	2303
37.3	Modèles d'échantillonnages	2306
37.4	Estimation ponctuelle	2309
37.5	Statistiques et estimateurs	2311
37.5.1	Qualité des estimateurs	2311
37.5.2	Méthode des moments	2312
37.5.3	Méthode de substitution	2314
37.5.4	Méthode du maximum de vraisemblance	2314
37.5.5	Exemples sous forme d'exercices	2314
37.5.6	Estimation d'une fonction de répartition	2316
37.5.7	Exemples sous forme d'exercices	2317
37.5.8	Espérance et variance d'un estimateur	2319
37.6	Estimation par intervalle de confiance	2319
37.6.1	Région de confiance	2322
37.6.2	Fonction pivotale	2322
37.6.3	Sondage de proportion	2326
37.7	Estimer une densité lorsqu'on ne sait rien	2327
37.7.1	Distance entre des mesures	2327
37.7.2	Estimateur par fenêtres glissantes	2328
37.8	Test d'hypothèses, prise de décision	2330
37.8.1	Exemple : qualité des pièces d'usine	2330
37.8.2	Exemple : la résistance d'un fil	2330
37.8.3	Vocabulaire et théorie	2331
37.8.4	Risque de première et seconde espèce	2332
37.8.5	Modèle paramétrique de loi gaussienne	2333
37.9	Tests paramétriques	2334
37.10	Tests d'adéquation	2335
38	Chaînes de Markov à temps discret (Vol 4)	2341
38.1	Généralités	2341
38.2	Chaînes de Markov sur un ensemble fini	2344

38.3	Marche aléatoire sur $\mathbb{Z}$	2346
38.3.1	Chaînes de Markov homogènes	2348
38.3.2	Graphe de transition	2349
38.3.3	Chaîne de Markov définie par récurrence	2350
38.4	Classification des états	2352
38.4.1	Chaînes irréductibles	2354
38.4.2	Nombre de visites	2356
38.5	Mesure invariante	2360
38.6	Convergence vers l'équilibre	2362
38.7	Processus de Galton-Watson	2365
39	Martingales (Vol 4)	2369
39.1	Convergence de martingales	2369
39.2	Temps d'arrêt et martingale terminée	2372
39.3	Décomposition de martingales	2374
39.4	Problème de la ruine du joueur	2376
39.4.1	Le cas où la pièce est truquée	2377
39.4.2	Le cas où la pièce est non truquée	2380
39.4.3	Un petit complément	2382
40	Processus de Poisson (Vol 4)	2385
40.1	Processus de Poisson	2385
40.2	Quelques trucs sur la simulation	2388
40.2.1	Le théorème central limite pour Markov	2389
40.2.2	Feuille 5	2389
40.2.3	Feuille 6	2389
40.2.4	Feuille 7	2390
40.2.5	Simuler des lois conditionnelles	2390
41	Langages (Vol 4)	2391
41.1	Langages	2391
41.1.1	Alphabets et mots	2391
41.1.2	Langage	2392
42	Utilisation dans les autres sciences (Vol 4)	2395
42.1	Démystification du MRUA	2395
42.1.1	Preuve de la formule	2395
42.1.2	Interprétation graphique	2396
42.2	Relativité en mécanique newtonienne	2396
42.2.1	Relativité du mouvement	2396
42.2.2	Bob et Alice	2396
42.3	Invariance de la vitesse de la lumière	2397
42.3.1	Champ de gravitation et électrique	2397
42.3.2	Support du champ : pas d'éther	2398
42.3.3	Le problème	2398
42.4	Conséquences	2398
42.4.1	Ligne d'univers	2398
42.4.2	Transformations de Lorentz	2399
42.4.3	Conditions d'existence	2402
42.4.4	La notion d'intervalle	2403
42.4.5	Le cône de lumière d'un point	2403
42.4.6	Contraction des longueurs	2404
42.4.7	Dilatation des intervalles de temps	2404
42.4.8	Invariance de l'intervalle	2405

42.4.9	Vitesse limite	2410
42.5	Applications	2410
42.5.1	Le GPS	2410
42.5.2	Les ondes électromagnétiques	2410
42.6	Mécanique relativiste	2410
42.6.1	Des problèmes, toujours des problèmes	2411
42.6.2	Loi d'addition des vitesses	2411
42.6.3	L'action d'une force	2412
42.6.4	Équivalence entre la masse et l'énergie	2413
42.7	Principe de correspondance	2413
43	Exemples avec Sage (Vol 4)	2415
43.1	Graphiques	2415
43.1.1	Autres	2415
44	Épilogue : la constante de Weiner (Vol 4)	2435
45	Développements possibles (Vol 4)	2437
45.1	Algèbre et géométrie	2437
45.2	Analyse	2441
45.3	Anciennes leçons	2444
46	GNU Free Documentation License (Vol 4)	2453
	Bibliographie	2461

Index

- λ -système, 1013
- p -Sylow, 333
- p -groupe, 333
- q -orthogonal, 604
- Abel
 - angulaire, 1570
 - convergence radiale, 1148
- abscisse
 - curviligne, 1656
- absolument continue, 1250
- absorbant, 2352
- abélianisé, 221
- abélien
 - groupe, 153
- accroissement, 968
- accroissements finie
 - dérivée partielle, 850
- accélération d'un chemin, 1639
- action, 181
 - adjointe, 230
 - de groupe
 - Wedderburn, 1487
 - domaine fondamental, 232
 - fidèle, 229
 - libre, 233
 - transitive, 233
- action de groupe, 520
 - sur des matrices, 1620
- adhérence, 536
- adjoint, 528
- affine
 - application, 494
 - espace, 491
 - sous-espace, 497
- aire, 1616
- aire dans $\mathbb{R}^2$, 1536
- algorithme, 2149
 - consistant, 2149
 - convergeant, 2149
 - facteurs invariants, 314
 - fortement consistant, 2149
 - stable, 2149
- algèbre, 176
 - de parties, 1007
 - engendrée, 176
- algèbre de Banach, 460
- algèbre engendrée, 1156
- algébrique, 379
- algébriquement
 - indépendant, 418
- alignement
 - dans un espace projectif, 1700
- alphabet, 2391
- alterné
 - groupe, 345
 - polynôme, 414
- alternée
 - forme linéaire, 513
- analytique
 - au sens complexe, 953
- angle
 - d'une courbe, 1675
 - entre deux droites, 1403
 - orienté de vecteurs, 1399
- angle entre deux vecteurs, 1354
- Anneau
 - $\mathbb{Z}/n\mathbb{Z}$
 - polynôme cyclotomique, 1483
- anneau, 109
 - $\mathbb{Z}/n\mathbb{Z}$, 343, 1478, 1486, 1490
 - de séries formelles, 1212
 - euclidien
 - facteurs invariants, 314
 - factoriel, 255
 - noethérien, 261
 - principal, 259, 364, 551
 - utilisation, 365
 - quotient par un idéal, 159
 - à division, 357
- anneau commutatif, 109
- anneau intègre, 161
- application
 - de classe C^k , 738
 - différentiable, 737, 738, 862, 895, 1269, 1620
 - extrémums lié, 1283
 - définie positive, 603
 - en escalier, 1608

- linéaire
 - théorème de Banach-Steinhaus, 717
- mesurable, 1011
- multilinéaire, 699
- ouverte, 695
- semi-définie positive, 603
- tangente, 866
- application affine, 805
- application bilinéaire, 600
- application ouverte, 719
- application réciproque, 441
- approximation
 - de fonctions
 - par des polynômes, 2298
 - de l'unité, 1874
 - par polynômes, 1239
 - polynomiale, 1807
- apériodique
 - chaîne de Markov, 2364
 - état d'une chaîne de Markov, 2363
- arc
 - géométriques, 1655
 - paramétré, 1639
- arc cosinus, 1352
- arc sinus, 1350
- arc tangente, 1349
- archimédien, 119
- associée
 - subdivision, 1608
- associés
 - éléments d'un anneau, 253
- asymptotiquement pivotale, 2322
- attractif
 - point fixe, 1255
- automorphisme
 - d'espace vectoriel, 286
- automorphisme de groupes, 109
- axiome
 - du choix, 104
- Baire
 - espace, 489
 - théorème, 485, 490
 - tribu, 1005
- Banach
 - espace, 460
- barycentre
 - cas affine, 499
 - cas vectoriel, 1373
 - enveloppe convexe, 503
- base, 278
 - d'un module, 175
 - de Newton, 2158
 - de topologie
 - dénombrable, 445
 - espace métrique, 445
 - duale, 321
 - espace préhilbertien, 1777
 - hilbertienne, 1777
 - utilisation, 1959
 - locale, 1756
- base associée à un repère cartésien, 492
- base canonique de $\mathbb{R}^m$, 282
- base de topologie, 419
- base de voisinages, 420
- base préduale, 322
- Bergman (espace), 1943
- Bernoulli, 2267
 - somme, 2284
- Berry-Esséen (borne), 2265
- Bessel
 - inégalité, 1776
- biais
 - d'estimateur, 2312
- bien
 - conditionné, 2130
 - enchaîné, 482
- bijection, 104, 441
- bilinéaire, 699
- binormale, 1666
- birapport, 1713
- birapport dans $\mathbb{C} \cup \{\infty\}$, 1732
- birégulier
 - point sur une courbe, 1653
- Bolzano-Weierstrass
 - espaces métriques, 446
- bon
 - ordre, 105
- bord, 453
- borné, 445
 - partie de V , 532
 - temps d'arrêt, 2372
- bornée
 - différentielle, 883
 - partie de $\mathbb{R}^m$, 796
 - suite, 632
- borélienne
 - fonction, 1017
 - tribu, 1032
- boréliens, 1032
- boule
 - avec seminormes, 486
 - fermée, 532
 - ouverte, 444, 532
- boule dans un corps, 184
- Bruhat (décomposition), 997
- Burnside

- formule, 232
- Bézout
 - anneau principal, 259
 - calcul effectif, 240
 - nombres entiers, 163
 - polynômes, 372
- canonique
 - base, 282
 - décomposition, 108
 - espace affine, 492
- Cantor
 - ensemble, 1063
- caractère, 1224
 - abélien, 1217
 - de S_4 , 1231
 - groupe diédral, 1468
 - irréductible, 1224
- caractéristique
 - d'un anneau, 177
 - d'une équation différentielle, 2101
 - polynôme, 553
 - sous-groupe, 215
- cardinal, 136
- cardioïde, 1653
- carré
 - dans un corps fini, 1491
- carrée
 - matrice, 293
- carte, 1524
- catégorie
 - ensemble de première, 485
- Cauchy
 - critère
 - uniforme, 914
 - déterminant, 522
 - formule, 1800
 - suite, 471
 - théorème, 333
- Cauchy-continue, 789
- Cauchy-Riemann, 1795
- Cauchy-Schwarz, 659, 1767
- Cayley
 - théorème, 333
- cellule d'un pavage, 1608
- centrale (application), 1224
- centralisateur, 159, 215
- centre
 - d'un anneau, 159
 - d'un groupe, 215
 - d'une rotation, 1388
- cercle
 - circonsrit à une courbe, 1682
 - dans la sphère de Riemann, 1723
- cercle-droite, 1724
- cercles
 - perpendiculaires, 1693
- Cesaro
 - moyenne, 711
- chaîne, 482
 - de Markov, 2341
 - apériodique, 2364
 - convergence, 2364
 - finie, 2344
 - homogène, 2341
 - irréductible, 2349
 - récurrente positive, 2359
 - régulière, 2344
- champ
 - conservatif, 1582
 - de vecteurs, 1545
- champ de vecteur conservatif, 1548
- champ dérivant d'un potentiel, 1582
- changement de variable, 1655
- Chasles, 491
- Chemin
 - classe C^2 , 1543
- chemin, 1543, 1639
 - dans $\mathbb{R}^p$, 1639
- circulation, 1580
- classe
 - d'association, 253
 - de conjugaison, 153
- classe d'association, 253
- classe de conjugaison
 - dans S_4 , 156
- clôture algébrique, 380
- codimension, 282
- coefficients
 - de Fourier, 1877
- coefficients binomiaux, 249
- coefficients de Fourier, 1888
- coercion, 1790
- coercive, 1309
- colinéarité, 1699
- combinaison
 - convexe, 499
- combinatoire, 1383
- commutant, 587
- commutateur
 - dans un groupe, 220
- commutatif
 - groupe, 153
- compacité, 446, 478, 483, 1811, 1840
 - sous-groupes du groupe linéaire, 1000
 - théorème de Dini, 916
 - utilisation, 1319

- théorème de Montel, 1942
- compact, 431, 534
 - arc paramétré, 1639
 - boule unité, 629
 - et fonction continue, 447, 639
 - fermé et borné, 628
 - intervalle $[a, b]$, 628
 - le coup du, 1247
 - localement, 432
 - opérateur, 1843
 - produit dénombrable, 484
 - produit fini, 483
 - quasi, 431
 - relatif, 1843
 - relativement, 432
 - suite exhaustive, 480
 - séquentiellement, 432
- compacts et fermés, 433
- complet
 - $\mathbb{R}$
 - corps, 206
 - espace métrique, 472
 - corps, 184
 - espace mesuré, 1021
 - espace topologique, 460
 - métrique, 460
- complexe conjugué, 213
- complète
 - famille de projecteurs, 175
- complément
 - à deux, 2120
- complémentaire, 106
- complétion
 - projective, 1702
- complétude, 1325, 1327, 1861
 - espaces L^p , 1862
- complété
 - d'un espace métrique, 1327
- composante, 968
- composante connexe, 430
- composition
 - suite de, 225
- concaténation
 - de langages, 2392
 - de mots, 2391
- concave, 1285
 - log-concave, 1292
- condition initiale, 2088
- conditionnement
 - absolu, 2129
 - d'une matrice inversible, 2163
 - relatif asymptotique, 2149
- conjugués
 - éléments d'une extension, 378
- connectés
 - indices d'une matrice, 2190, 2191
- connexe par arc, 642
- connexité, 483
 - définition, 430
 - et intervalles, 636
 - fonction holomorphe, 1330
 - indice d'une courbe, 1799
 - le groupe $GL^+(n, \mathbb{R})$, 988
 - par arc
 - fonction différentiable, 896
 - points d'accumulation, 478
 - prolongement analytique, 1330
 - signature d'une forme quadratique, 1314
 - théorème de Runge, 1807
 - théorème des valeurs intermédiaires, 651
 - utilisation
 - Brouwer, 1803
- consistance
 - estimateur, 2311
 - ordre, 2212
- constructible
 - angle, 1517
 - point, 1513
 - réel, 1513
- construction
 - des réels, 196
- contenu, 273
- continue
 - fonction entre espaces métriques, 476
 - fonction entre espaces topologiques, 438
 - forme différentielle, 856
 - sur espace métrique, 656
 - uniformément, 797
- continue sur $\mathbb{R}$, 647
- continuité
 - fonction définie par une intégrale, 1246
 - séquentielle, 440
- contraction, 1256
- convergeant
 - schéma discret, 2213
- convergence
 - commutative, 722
 - dans un espace vectoriel normé, 630
 - de martingales, 2373
 - de suite, 422
 - en loi, 2256
 - en probabilité, 2256
 - ordre, 2145
 - presque sûrement, 2255
 - quadratique, 2134
 - rapidité, 1183, 1966, 1967, 2144, 2284

- suite
 - dans un corps, 184
 - suite dans $\mathbb{R}^m$, 455
 - suite numérique, 629, 1239, 1951
 - Abel angulaire, 1570
 - uniforme, 914
 - intégrale, 1244
 - théorème de Dini, 916
- convergence absolue, 702
- convergence forte, 718
- convergence normale, 702
- convergence uniforme
 - série de fonctions, 702
- convergent
 - estimateur, 2311
- convexe
 - courbe plane, 1684
 - fonction sur $\mathbb{R}^n$, 1294
- convexité
 - barycentre, 501
 - enveloppe de $O(n)$, 996
 - fonction, 1285
 - inégalité de Jensen, 1300
 - locale, 1919
 - méthode de Newton, 2140
 - utilisation, 1319
- convolution, 2227, 2367
- convolution sur S^1 , 1889
- coordonnées
 - cartésiennes
 - dans un espace affine, 506
 - curvilignes, 1756
 - cylindrique, 1454
 - dans un espace affine, 492
 - homogène, 1718
 - sphériques, 1455
- coordonnées barycentrique, 507
- coordonnées polaires, 1449
- corps, 166
 - complet, 184
 - de décomposition, 402
 - de rupture, 392
 - polynôme cyclotomique, 1483
 - des fractions, 182, 184
 - extension, 409, 415
 - fini, 1490, 1494, 1498
 - Wedderburn, 1487
 - formellement réel, 357
 - ordonné, 184
 - premier, 359
- corps algébriquement clos, 379
- corps valué, 211
- cosinus, 1333
 - hyperbolique, 1185
- courbe, 1639
 - de Jordan, 1691
 - efficacité, 2332
 - fermée, 1672
 - simple, 1672
 - étude métrique, 1959
- courbe de niveau, 834, 836
- courbure, 1666
 - signée, 1673
 - totale, 1674
- covariance, 2230
- critique
 - Galton-Watson, 2367
 - point, 1279
 - point d'un arc, 1653
 - région, 2331
 - valeur, 2332
- critère
 - Abel, 1140
 - Abel pour intégrales, 1245
 - Cauchy
 - uniforme, 914
 - de Cauchy, 206, 472
 - Weierstrass, 1245
 - série de fonctions, 919
- critère du quotient, 707
- cyclique
 - endomorphisme, 549
 - matrice, 549
- cycloïde
 - coordonnées normales, 1658
 - longueur, 1652
- Cône de lumière, 2403
- d, 848
- degré
 - application $S^1 \rightarrow S^1$, 1676
 - d'un polynôme, 178
 - d'une représentation, 329
 - extension de corps, 376
- dense, 426
 - nulle part, 485
- densité, 1327
 - conjointe, 2226
 - d'une variable aléatoire, 2222
 - dans un espace de fonction
 - critère de Weyl, 1951
 - de $\mathbb{Q}$ dans $\mathbb{R}$, 626
 - utilisation, 1291
 - de $GL(n, \mathbb{R})$ dans $M(n, \mathbb{R})$, 989
 - de $\mathcal{D}(\mathbb{R}^n)$ dans $L^1(\mathbb{R}^n)$, 1940
 - de $C_c^\infty(\mathbb{R}^d)$ dans $L^p(\mathbb{R}^d)$, 1867
 - de $L^2([0, 1])$ dans $L^p([0, 1])$, 1869

- de $S^+(n, \mathbb{R})$ dans $S^{++}(n, \mathbb{R})$, 993
- des fonctions étagées dans L^p , 1867
- des polynômes
 - dans $C_c^0[0, 1]$, 2298
- matrices diagonalisables dans $M(n, \mathbb{C})$, 989
- mesure, 1084
- points extrémaux dans $\mathcal{L}$, 995
- prolongement, 1325
- densité d'une mesure, 1084
- diagonale
 - dominante, 2194
 - fortement dominante, 2195
 - strictement dominante, 2195
- diagonalisable, 561
 - et polynôme minimum scindé, 561
 - exponentielle, 1190
- diagonalisation
 - cas complexe, 668
 - cas réel, 568
 - endomorphisme autoadjoint, 661
 - simultanée, 563
- diamètre, 796
- difféomorphisme, 738
 - de classe C^k , 907
- différence
 - centrée, 2201
 - divisée, 2158
 - progressive, 2201
 - régressive, 2201
- différentiabilité, 896
- différentielle, 737
 - de $u \mapsto u^{-1}$, 753
 - partielle, 751
 - totale, 968
- dilatation, 982
- dilatation (matrice), 311
- dimension, 282
 - n -formes multilinéaires alternées, 513
 - définition, 282
 - sous espace affine, 497
 - utilisation, 503
- direction, 848, 1661
 - sous-espace affine, 497
- Dirichlet
 - noyau, 1947
 - théorème, 1948
 - théorème (sur les nombres premiers), 1486
- disque de convergence, 1139, 1141
- distance, 444
 - associée à une norme, 450
 - compatible, 466
 - entre deux mesures de probabilités, 2327
 - invariante, 466
 - point et ensemble, 457
- distance discrète, 456
- distance produit, 451
- distingué
 - sous-groupe, 215
- distribution, 1990
 - de Dirac, 2009
 - produit par une fonction, 1991
 - tempérée, 2009
 - équation de Schrödinger, 2083
- divergence, 974
- diviseur
 - dans un anneau, 160
 - de zéro, 160
 - de zéro à droite, 160
 - polynôme, 272
- diviseur de zéro, 160
- divisible, 125
- division
 - euclidienne, 162, 272
 - harmonique, 1735
- diédral, 1383
- domaine, 623
 - fondamental d'une action, 232
- dominé
 - modèle statistique, 2310
- dominée
 - convergence (Lebesgue), 1081
 - mesure, 1089
- droite
 - dans la sphère de Riemann, 1723
 - projective, 1699
- droite affine, 805
- droite réelle complétée, 647
- droite vectorielle, 805
- droites parallèles, 806
- droites perpendiculaires, 806
- dual
 - d'un espace de Hilbert, 1773
 - de L^p , 1931
 - de $L^p(\Omega)$, 1936
 - de $M(n, \mathbb{K})$, 327
- dual algébrique, 321
- dual topologique, 694, 756
- Dunford
 - décomposition, 574
- dyadique, 1100
 - développement, 203
- décalage, 2121
- décomposition
 - Bruhat, 997
 - canonique, 108
 - corps, 402

- Dunford, 574
 - application, 1190
 - exponentielle de matrice, 575
- Jordan
 - et exponentielle de matrice, 1189
- polaire, 994
- primaire, 573
- sous-espaces caractéristiques, 573
- spectrale, 573
- décomposition décimale, 714
- décomposition polaire, 1359
- dénombrable, 138
 - à l'infini, 432
- dénombrement, 1383
 - partitions de $\{1, \dots, n\}$, 1212
- déplacement, 1419
- dérivabilité
 - fonction définie par une intégrale, 1248
 - lemme de Borel, 1210
- dérivable, 814
 - au sens complexe, 892
 - fonction, 2039
- dérivation
 - au sens des distribution
 - Sobolev, 2026
- dérivé
 - groupe, 221
- dérivée
 - dans Sobolev $H^1(I)$, 2023
 - directionnelle, 848, 851
 - distributionnelle, 1991
 - faible, 1986
 - fonction à valeurs dans E' , 489
 - partielle, 847, 967
 - seconde, 815
- dérivée faible, 1984
- dérivée partielle, 848
- déterminant, 513
 - Cauchy, 1242
 - d'un endomorphisme, 517
 - d'une famille de vecteurs, 514
 - de Cauchy, 522
 - et inversibilité, 517
 - forme linéaire alternée, 513
 - Gram, 521, 1242
 - interprétation géométrique, 1116
 - matrice, 299
 - résultant, 523, 1575
 - utilisation, 1319
 - Vandermonde, 519
- détermination
 - logarithme, 1837
 - principale, 1837
- développable
 - en série entière, 1193
- développement
 - asymptotique, 965
 - limité
 - en zéro, 960
 - fonction holomorphe, 1795
 - premier ordre, 818
 - Taylor, 1620
- écart-type, 2230
- échantillon, 2304, 2306
- effectif
 - empirique, 2336
- efficacité
 - courbe, 2332
 - d'une méthode itérative, 2153
- élément
 - de surface, 1556
 - de torsion, 235
- élément de surface, 1530
- ellipsoïde, 619
- elliptique
 - équation aux dérivées partielles, 2110
- endomorphisme, 286
 - cyclique, 549
 - diagonalisable, 596, 991, 2079
 - Dunford, 574
 - diagonalisation, 568
 - décomposition
 - polaire, 994
 - nilpotent
 - Dunford, 574
 - préservant une forme quadratique, 1002
 - sous-espace stable, 574, 2079
- endomorphisme direct, 527
- endomorphisme préserve l'orientation, 527
- engendré, 250
 - λ -système, 1013
 - corps, extension, 390
 - idéal dans un anneau, 250
 - sous-espace affine, 497
 - sous-groupe, 216
 - tribu, 1004
 - par une variable aléatoire, 2223
- ensemble
 - archimédien, 119
 - de Cantor, 1063
 - différence symétrique, 106
 - infini, 133
- ensemble connexe, 430
- ensemble des mots, 2391
- ensemble fini, 133
- ensemble quotient, 107

- ensembles
 - disjoints, 103
- entier, 130
- entrelacement, 1224
- enveloppe
 - convexe, 501
- équation
 - différentielle
 - linéaire, 2041
 - ordinaire d'ordre 1, 2039
 - variables séparées, 2044
 - générale de degré n , 418
- équi-intégrable, 2373
- équivalence
 - arcs paramétrés, 1655
 - chemin, 1647
 - classe de fonctions, 1845
 - de représentations, 1224
 - de suites, 632
 - homotopie, 1799
 - norme, 680
 - suite de composition, 227
- erreur, 2159, 2189
 - assignation, 2124
 - de consistance, 2212
 - discrétisation, 2212
 - quadratique, 2162
 - troncature, 2124
- erreur relative, 2124
- escalier, 1046
- Espace
 - de Sobolev, 2028
- espace
 - L^2
 - Sobolev, 2026
 - L^p , 1848
 - Banach, 460
 - de Baire, 489
 - de Bergman, 1943
 - de fonctions
 - L^p , 1862
 - Sobolev H^1 , 2026
 - de Hilbert
 - espace de Sobolev H^1 , 2026
 - de probabilité, 2221
 - de Schwartz, 1938, 2009
 - de Sobolev, 2023, 2030
 - euclidien, 676
 - mesurable, 1003
 - mesuré, 1009
 - complété, 1024
 - métrique, 444
 - base de topologie, 445
 - projectif, 1699
 - propre, 544
 - séparé, 427
 - tangent, 1526
 - topologique
 - métrisable, 475
 - vectériel, 173
 - dimension, 513
 - vectériel topologique
 - métrisable, 459
- espace topologique, 419
- espace vectériel
 - topologique, 463
- espace vectériel normé, 449
- espérance, 2228
 - conditionnelle, 2233, 2235
 - variable aléatoire, 2239
 - événement, 2235
- estimateur, 2311
 - biais, 2312
 - consistant, 2311
 - convergent, 2311
 - de fonction de répartition, 2317
 - maximum de vraisemblance, 2314
- estimation
 - des grands écarts, 2284
- étrangers
 - polynômes, 272
- Euclide
 - algorithme étendu, 238
 - lemme, 241
- euclidien
 - anneau, 263
 - espace, 618
- Euler
 - indicatrice, 1475
- événement, 2221
- exact
 - intervalle de confiance, 2320
- excès
 - intervalle de confiance, 2320
- exhaustive (suite de compacts), 480
- exponentielle, 1170
 - convergence, 709
 - de matrice, 755, 1189, 1190, 1202
 - utilisation, 1277
 - existence, 1166
 - rapide, 1480
 - unicité, 947
- exposant, 339, 596
 - d'un groupe, 220
- extension
 - corps de base, 576

- de corps, 376, 415
 - algébrique, 387
 - finie, 1500
 - simple, 390
 - utilisation, 1517
- isométrie, 1326
- séparable, 410
- extension algébrique, 379
- extension algébriquement clos, 379
- extrapolation, 2158
- extrémal
 - point dans un convexe, 995
- extrémité
 - d'un intervalle, 636
- extrémum, 1620
 - lié, 1283
 - local
 - relatif, 1283
- extrémum local, 1278
- extrémums, 1281
 - volume d'un ellipsoïde, 1319
- facteur
 - intégrant, 2083
- factoriel
 - anneau, 255
- factorisation
 - de polynôme, 274, 391
- faisceau de droites, 1720
- famille
 - sommable, 723
- famille trigonométrique
 - sur S^1 , 1887
- famille équicontinue, 484
- Fatou, 1072
- Fejér
 - noyau, 1947
- fermeture, 536
- fermeture séquentielle, 458
- fermé, 420, 453, 534
- fidèle (action), 229
- filtration, 2369
- fine
 - subdivision, 1640
- fixateur, 229
- flot, 2055, 2101
- flux
 - d'un champ de vecteur, 1560
- flux d'un champ de vecteurs, 1558
- fonction, 623
 - Γ d'Euler, 1824
 - borélienne, 1017
 - caractéristique, 1610
 - d'une variable aléatoire, 2252
 - continue
 - par morceaux, 1049
 - égales, 459
 - convexe, 1285, 1291
 - croissante, 623
 - de Dirichlet, 1953
 - de Möbius, 1509
 - de répartition, 2251
 - décroissante, 623
 - définie par une intégrale, 1207, 1245, 1251, 1252, 1840
 - Γ d'Euler, 1824
 - utilisation, 2271
 - en escalier intégrable, 1609
 - génératrice, 2253
 - holomorphe, 892, 1840
 - théorème de Montel, 1942
 - image, 623
 - monotone, 624
 - par morceaux, 1049
 - méromorphe
 - Γ d'Euler, 1824
 - valeurs vectorielles, 968
 - à décroissance rapide, 1938
 - étagée, 1867
- fonction continue en un point, 438
- fonction de classe C^1 , 883
- fonction dérivée, 814
- fonction périodique, 825
- fonctionnelle
 - énergie, 1793
- fonctions équivalentes, 428
- fondamental
 - domaine d'une action, 232
- forme
 - bilinéaire, 600
 - non dégénérée, 601
 - différentielle, 855
 - exacte, 1568
 - fermée, 1568
 - linéaire
 - différentielle, 1283
 - quadratique, 603, 617, 1314, 1316, 1620
 - groupe orthogonal, 1002
- forme bilinéaire symétrique, 600
- forme canonique
 - fonction simple, 1046
- forme linéaire, 321
 - alternée, 513
- formule
 - Bayes, 2232
 - Burnside, 232
 - d'expulsion (produit vectoriel), 674

- de Cauchy, 1800
- Hadamard, 1141
- inversion Möbius, 1509
- probabilité totales, 2232
- sommatore de Poisson, 1966
- Taylor
 - reste intégral, 1604
 - utilisation, 2144
- Formule de Leibnitz, 1986
- formule de Stirling, 1627
- Fourier, 1966
 - série
 - utilisation, 1959
 - transformée
 - groupe abélien fini, 1219
- fraction
 - rationnelle
 - intégration, 1575
- fraction rationnelle, 1601
- fractions
 - rationnelles, 182
- fractions (corps), 184
- Fredholm
 - équation, 1258
- Frenet
 - formules, 1667
- Fresnel
 - intégrale, 1829
- Frobenius
 - morphisme, 177
- Frobénius
 - réduction, 583
- frontière, 426, 453, 539
- fréquence
 - empirique, 2336, 2356
- Fubini
 - théorème
 - dans $\mathbb{R}^n$, 1131
- Galton-Watson
 - sous-critique, 2367
 - sur-critique, 2367
- Gauss
 - lemme
 - polynômes, 373
 - somme de, 1492
- Gershgorin
 - disque, 2192
- gradient, 863, 871, 882
- Gram (déterminant), 521
- Gram-Schmidt, 676
- graphe, 623, 816
 - de transition (chaîne de Markov), 2349
 - fonction, 833
 - fonction de deux variables, 835
- groupe, 108
 - p -groupe, 333
 - $GL(n, \mathbb{R})$, 1316
 - action, 1741
 - utilisation, 1002
 - agissant sur un ensemble
 - diédral, 1375
 - alterné, 345
 - circulaire, 1739
 - de Galois, 417
 - de permutation, 1468
 - de permutations, 1383
 - caractères de S_4 , 1231
 - de torsion, 235
 - des isométries
 - espace métrique, 456
 - des symétries, 1416
 - diédral, 1375, 1383
 - générateurs (preuve), 1376
 - générateurs (utilisation), 1468
 - dérivé, 221
 - de $GL(n, \mathbb{K})$, 987
 - de $SL(n, \mathbb{K})$, 987
 - du groupe alterné, 348
 - du groupe symétrique, 346
 - en géométrie, 1375
 - et géométrie, 513, 1383, 1741
 - isométries du cube, 354
 - fini, 335, 343, 1383, 1478, 1487, 1490
 - alterné, 347
 - diédral, 1375
 - Wedderburn, 1487
 - linéaire, 997
 - décomposition polaire, 994
 - enveloppe convexe de $\Omega(n)$, 996
 - hyperplan, 328
 - sous-groupes compacts, 1000
 - modulaire, 1741
 - orthogonal, 531
 - d'une forme quadratique, 1002
 - partie génératrice, 347, 1478, 1741
 - permutation, 513, 520, 997, 1478
 - diédral, 1375
 - projectif, 1706
 - quotient, 225
 - résoluble, 228
 - spécial orthogonal, 531
 - symétrique, 154
 - action sur un triangle, 1221
- groupe cyclique, 217
- groupe de pavage, 1420
- groupe dérivé

- de $GL(n, \mathbb{C})$, 981
- Grönwall (lemme), 2039, 2040
- générateur, 217
- génératrice
 - partie d'un module, 175
- géométrie
 - avec des groupes, 1376, 1741
 - avec nombres complexes, 1376, 1741
- géométrique
 - avec des nombres complexes, 1959
- Hadamard
 - conditions, 2112
 - formule, 1141
- Hardy-Littlewood (théorème), 1239
- Hausdorff, 427
- Heine (théorème), 797
- hermitienne, 618
- hessienne, 908
- Hilbert
 - espace, 1767
- holomorphe, 892
 - sur un compact, 892
- homographie, 1705, 1741
 - sur $\mathbb{C} \cup \{\infty\}$, 1727
- homogène
 - chaîne de Markov, 2341
- homotopie, 1678
- homéomorphisme, 442
- hyperbolique
 - équation aux dérivées partielles, 2110
- hyperplan, 592, 1369
 - de $M(n, \mathbb{K})$, 329
 - sépare
 - au sens strict, 1920
 - séparer
 - au sens large, 1920
- hypothèse
 - alternative, 2331
 - composite, 2331
 - multiple, 2331
 - nulle, 2331
 - simple, 2331
- identifiable, 2310
- identité de polarisation, 603
- idéal
 - bilatère, 159
 - dans un anneau, 159
 - maximal, 252
 - principal
 - à droite, 256
 - à gauche, 256
- image, 623
- incompressible
 - champ de vecteur, 976
- indicatrice d'Euler, 1475
- indice, 224
 - d'une courbe dans $\mathbb{C}$, 1799
 - de rotation, 1677
- indice d'inertie, 614
- inductif, 105
- induite
 - topologie, 536
 - tribu, 1004
- indécomposable
 - module, 176
- indépendance, 2225
 - affine, 505
 - algébrique, 418
 - projective, 1707
 - sous tribus, 2222
 - variables aléatoires, 2223
 - événements, 2222
 - utilisation, 2296, 2376
- infimum, 207
- inférence statistique, 2303
- injection, 104, 441
- interpolation, 2158
- Intervalle, 2403
- intervalle, 105, 623, 641
 - fermé, 623
 - longueur, 1052
 - ouvert, 623
- intervalle de confiance
 - asymptotique, 2324
- intégrable, 1075
 - fonction non en escalier, 1615
 - fonction positive, 1619
 - fonction à valeurs vectorielles, 1078
- intégrale
 - calcul, 1951
 - convergente, 1113, 1574
 - d'une fonction sur une carte, 1531
 - d'une fonction sur une variété, 1535
 - d'une forme différentielle, 1546
 - fonction en escalier, 1609
 - Fresnel, 1829
 - impropre, 1112, 1113
 - sur un chemin, 1544
- intégrale d'une fonction, 1066
- intégrale d'une forme différentielle, 1546
- intégrale de Dirichlet, 1637
- intégrale sur une carte, 1527
- intégration
 - fraction rationnelle, 1575
- intéressante, 97

- intérieur, 424
 - d'un ensemble, 533
 - point, 533
- invariance cyclique
 - trace, 295
- invariant
 - de similitude, 583
- invariante
 - mesure
 - pour une chaine de Markov, 2360
- inverse
 - dans un groupe, 153
- inverse généralisé, 2288
- inversion, 1694
 - dans le groupe symétrique, 155
- inversion dans $\mathbb{C} \cup \{\infty\}$, 1726
- involution, 563
- inégalité
 - arithmético-géométrique, 1301
 - Bessel, 1776
 - Cauchy-Schwarz, 659, 1767
 - de Khintchine, 2281
 - de la moyenne, 895
 - des pentes, 1286
 - Hölder, 1853
 - utilisation, 2229, 2299
 - isopérimétrique, 1959
 - Jensen, 1300
 - espérance conditionnelle, 2251
 - pour une somme, 1300
 - version intégrale, 1852
 - Kantorovitch, 1301
 - Markov, 2261
 - Minkowski, 1856
 - triangulaire, 444, 449
- irrationalité
 - $\sqrt{2}$, 192
- irréductible
 - chaîne de Markov, 2349
 - dans un anneau, 254
 - module, 176
 - représentation, 1222
- isobarycentre, 499
- isomorphisme, 729
 - $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$, 1490
 - d'anneaux, 157
 - d'espaces topologiques, 442
 - de corps, 166
 - espace affine, 496
 - espace vectoriel normé, 691
 - espaces vectoriels, 287
- isométrie
 - de forme quadratique, 611
 - de l'espace euclidien $\mathbb{R}^2$, 1376
 - espace euclidien
 - isométries du cube, 354
 - groupe, 456
 - isométrie (forme bilinéaire), 612
 - isométrie d'espaces métriques, 456
- isotrope
 - cône, 603
 - totalement, 603
- isotrope (vecteur), 603
- jacobien, 882, 973
- Jordan
 - chemin, 1561
 - courbe, 1691
 - réduction, 586
- Jordan-Hölder, 225
- Kronecker, 282
- lacet, 1799
- Lagrange
 - multiplicateur, 1283
 - polynôme, 327
 - théorème, 224
- lagrangien, 1283
- langage, 2392
 - itéré, 2393
 - itéré strict, 2393
 - unité, 2392
 - vide, 2392
- Laplace
 - transformée, 2253
- laplacien, 1763
- Legendre
 - symbole, 1491
- Leibnitz, 819
 - applications entre espaces vectoriels normés, 751
- lemme
 - Borel, 1210
 - d'Euclide, 241
 - de Borel-Cantelli, 2259
 - de Gauss
 - contenu de polynôme, 1499
 - pour des entiers, 241
 - de Morse, 1620
 - de Schreider, 227
 - de Slutsky, 2258
 - de transport, 1019
 - de Zorn, 105
 - des noyaux, 546
 - Fatou, 1072
 - Gauss

- dans un anneau principal, 260
 - polynômes, 373
- Grönwall, 2039, 2040
- Hadamard, 1254
- regroupement, 2225
- Schur complexe, 565
- Schur réel, 567
- lettres, 2391
- Levi-Civita, 1757
- libre
 - action, 233
 - partie, 277
 - partie d'un module, 175
- librement engendré, 284
- Ligne d'univers, 2399
- limite, 571
 - d'ensembles, 1011
 - d'une fonction, 437
 - de fonctions holomorphes, 1840
 - de suite
 - espace topologique, 422
 - inférieure, 634
 - inversion, 1212, 1239, 1840, 1848
 - permutation
 - utilisation, 2253
 - suite dans $\mathbb{R}^m$, 455
 - suite numérique, 629
 - supérieure, 634
 - unicité, 438
- limite pointée, 768
- limite à droite, 780
- limite épointée, 768
- linéaire
 - application, 285
- linéairement indépendant
 - module, 173
- Lipschitz, 1256
 - localement, 897
- Lipschitzienne, 896
- liste d'indices, 33
- localement
 - intégrable, 1112
- log-concave, 1292
- logarithme
 - complexe, 1834
 - dans $\mathbb{C}$, 1831
 - de matrice, 1203
 - sur les réels positifs, 1167
- loi
 - χ^2 , 2282
 - binomiale
 - comportement asymptotique, 2284
 - conjointe, 2225
 - d'une variable aléatoire, 2254
 - de Poisson, 2269
 - des grands nombres
 - forte, 2261
 - pour les chaînes de Markov, 2362
 - processus de Poisson, 2386
 - utilisation, 2284, 2296
 - marginale, 2225
 - normale
 - vecteur gaussien, 2276
 - parente, 2303, 2304
 - parente d'un échantillon, 2306
 - réciprocité quadratique, 1494
 - sans mémoire, 2271
 - Student, 2282
- longueur
 - arc géométrique, 1656
 - d'un arc paramétré compact, 1640
 - d'un intervalle, 1052
 - d'une arrête, 1606
 - élément de, 1650
- longueur d'arc, 1642
- Lotka-Volterra, 2072
- M-matrice, 2197
- maigre, 1005
- maigre (ensemble), 485
- majorant, 105, 207
 - essentiel, 1850
- Markov
 - inégalité, 2261, 2309
- martingale, 2369
 - bornée dans $L^2(\Omega)$, 2370
- matrice, 293, 997, 1741
 - compagnon, 582
 - creuse, 2167
 - cyclique, 549
 - de dilatation, 311
 - de permutation, 311
 - de similitude, 892
 - de Sylvester, 522
 - de transvection, 311
 - dense, 2167
 - hermitienne
 - racine carrée, 991
 - jacobienne, 871, 882
 - normale, 668
 - orthogonale, 309, 531
 - permutation
 - élémentaire, 2175
 - racine carrée, 991
 - réductible, 2191
 - semblable, 991
 - semblables, 617, 1316

- stochastique, 2343
- symétrique, 1316
 - réelle, 1314
- trigonalisable, 564
- équivalence, 313
 - dans le groupe linéaire, 1002
- matrice d'une application linéaire, 296
- matrice d'une forme bilinéaire, 604
- matrice de transition, 2342
- matrice-colonne, 294
- matrice-ligne, 294
- matrices
 - similitude, 313
- maximale
 - partie orthonormale, 1778
- maximum, 105
 - global, 1278
 - local, 1278
- maximum local, 1278
- mesurable
 - application, 1011
 - au sens de m^* , 1016
 - ensemble, 1009
 - fonction, 1017
 - Lebesgue, 1605
- mesure
 - σ -finie, 1009
 - absolument continue, 1089
 - angle entre vecteurs, 1400
 - complexe, 1090
 - dans une carte, 1530
 - de Borel, 1037
 - de comptage, 1106, 1130
 - de Haar, 1542, 1543
 - de Lebesgue, 1056
 - de Radon, 1037, 1813
 - externe, 1605
 - extérieure, 1007
 - finie, 1009
 - image, 1034
 - positive, 1009
 - probabilité, 2221
 - produit, 1097
 - régulière, 1037
 - extérieure, 1037
 - intérieure, 1037
 - sur un ensemble de parties, 1007
- mesure σ -finie, 1007
- mesure finie, 1007
- mesure à densité, 1084
- minimum
 - ensemble ordonné, 105
- minimum local, 1278
- minorant, 105, 207
- modulaire (groupe), 1741
- module
 - de continuité, 758
 - indécomposable, 176
 - irréductible, 176
 - simple, 176
 - à gauche, 173
- module d'un nombre complexe, 652
- module produit, 174
- modèle
 - paramétrique, 2304
 - statistique, 2303
 - échantillonnage, 2304, 2306
- moment, 2228
 - fonction génératrice, 2253
- monogène, 217
 - extension de corps, 390
- monotonie, 2077
- monoïde, 363
- monôme, 270
- morceau
 - fonction continue ou monotone, 1049
- morphisme
 - d'algèbres, 176
 - d'anneaux, 109
 - de corps, 166
 - espace vectoriel normé, 691
 - Frobenius, 177
- morphisme de groupes, 109
- morphisme de produits tensoriels, 729
- mot, 2391
 - longueur d'un mot, 2391
 - mot vide, 2391
 - nombre d'occurrences, 2391
- mot non vide, 2391
- moyenne
 - de Cesaro, 711
 - empirique, 2230
 - empirique d'un échantillon, 2306
 - quadratique, 2230
- multiindice, 33
- multiplicateur
 - de Lagrange, 1283
- multiplication, 119
- multiplicité
 - racine d'un polynôme, 274
 - racine de $f(x) = 0$, 2137
 - valeur propre
 - algébrique, 804
 - géométrique, 804
- méromorphe, 1817
- Méthode

- de Newton, 2138
- méthode
 - des chemins, 845
 - Newton, 2144
 - cas convexe, 2140
- métrisable
 - espace vectoriel topologique, 459
- nabla, 880
- neutre
 - dans un groupe, 153
- Newton
 - méthode, 2144
- nilpotent, 160
- niveau de confiance, 2320
- nombre
 - complexe
 - norme 1, 1487
 - de Fermat, 1517
 - dénormalisé, 2122
 - normal, 2296
 - normalisée, 2122
 - premier, 343, 364, 1183, 1478, 1486, 1490
 - dans leur ensemble, 163
 - deux nombres entre eux, 163
 - théorème des deux carrés, 365
 - tours d'une courbe plane, 1676
- nombre premier
 - polynôme cyclotomique, 1483
- nombres complexes, 212
- non dénombrable, 138
- normal
 - arc paramétré, 1656
 - endomorphisme, 668
 - nombre, 2296
 - sous-groupe, 215
- normal extérieur
 - vecteur, 1560
- normale
 - loi réduite, 2275
 - principale, 1666
- normalisateur, 215
- norme, 449
 - d'algèbre, 685
 - d'application linéaire, 683
 - d'une application linéaire, 683
 - euclidienne, 679
 - dans $\mathbb{R}^m$, 664
 - supremum, 679
 - sur $\mathbb{Z}[i\sqrt{5}]$, 261
 - vecteur, 320
 - équivalence, 680
- norme maximum, 450
- normé
 - espace vectoriel, 450
- noyau
 - application vers un groupe, 221
 - d'une forme bilinéaire, 603
 - Dirichlet, 1947
 - Fejér, 1947
 - vers un espace vectoriel, 287
- nulle part dense, 485
- négatif, 200
- négligeable
 - partie d'un espace mesuré, 1021
- observation, 2221
- opposés
 - chemins, 1647
- opérateur
 - autoadjoint, 530
 - définit positif, 569
 - hermitien, 530
- opérateurs
 - compatibles, 1789
- orbite
 - d'un point sous une action, 229
- ordre, 104
 - bon ordre, 105
 - d'un groupe, 219
 - d'un polynôme, 273
 - d'une matrice carrée, 293
 - dans un corps, 184
 - de convergence d'un schéma, 2213
 - distribution, 1993
 - partiel, 104
 - sur un anneau factoriel, 255
 - total, 104
 - élément, 219
- orientation, 526, 1532, 1554
- orientation affine, 528
- origine
 - abscisse curviligne, 1656
 - repère affine, 506
- orthogonal, 664, 1772
 - coordonnées curviligne, 1756
 - famille de projecteurs, 175
 - matrice, 531
 - opérateur, 531
 - sous-espace, 322
 - vecteur, 320
- orthonormé, 664
 - système, 1775
- oscillation
 - d'une fonction, 792
 - d'une fonction en un point, 792
- osculateur (cercle), 1671
- ouvert, 419, 453, 534

- parabolique
 - équation aux dérivées partielles, 2110
- parallèle
 - sous-espaces affines, 497
- parallélogramme, 1537
- paramétrage, 1647
 - normale, 1656
- paramétrages
 - admissible, 1655
- Parseval, 1782
- partie
 - génératrice, 277
 - régulière, 960
 - totale, 1775
- partie convexe, 498
- partie entière, 212
- partie fractionnaire, 212
- partie génératrice, 217
- partie libre
 - module, 173
- partie linéaire, 494
- partie symétrique, 463
- partie équilibrée, 463
- partition
 - dénombrable mesurable, 1042
- partition de l'unité, 1209
- pavable, 1606
- pavage du plan, 1419
- pavé, 1605, 1606
- Pearson
 - théorème, 2336
- peigne de Dirac, 2015
- permutation, 154
 - matrice, 311
- permutation paire, 156
- permuter
 - différentielle et intégrale
 - $\mathbb{R}^n$, 1253
 - dérivée et intégrale
 - $\mathbb{R}^n$, 1252
 - dans $\mathbb{R}$, 1248
 - dans $\mathbb{R}$ avec les bornes, 1251
 - dérivée et limite, 923
 - intégrale
 - et série, 1130
 - limite et intégrale
 - convergence dominée, 1081
 - convergence monotone, 1071
 - espace mesuré, 1246, 1247
 - somme et intégrale, 1072, 1133
 - série entière et dérivation, 1151
 - série entière et intégration, 1153
- permuter limite et intégrale, 1245
- petit théorème de Fermat, 360
- pgcd
 - calcul effectif, 239
 - dans un anneau intègre, 160
 - polynômes, 375
- pivotal, 2322
- plan
 - projectif, 1699
 - tangent, 881, 968
- plan affín, 805
- plan médiateur, 810
- plan vectoriel, 805
- Plancherel, 1782
- plongement, 1325
- Poincaré (demi-plan), 1741
- point
 - d'équilibre
 - stable, 2068
 - pondéré, 499
- point adhérent, 425
- point critique
 - définition, 1622
- point d'accumulation, 426
- point fixe, 2367
 - attractif, 1255
 - Brouwer, 1538
 - Picard, 1256
 - Schauder, 1540
- point intérieur, 424
- point isolé, 426
- Poisson
 - formule sommatoire, 1966
 - processus, 2385
- polynôme
 - alterné, 414
 - annulateur, 545, 548
 - caractéristique, 553, 566
 - contenu, 273
 - cyclotomique, 1481
 - irréductibilité, 1483
 - propriétés, 1482
- d'endomorphisme, 991
 - décomposition de Dunford, 574
- de Bernstein, 2298
- irréductible
 - sur $\mathbb{F}_q$, 1510
 - séparable, 408
- Lagrange, 327
- minimal, 381
 - d'un élément d'une extension, 377
 - ponctuel, 548
- racines, 415
- scindé, 369

- semi-symétrique, 414
- symétrique, 414, 415, 520, 525, 1498
 - élémentaire, 414, 416
- séparable, 408
- trigonométrique, 1877
 - à plusieurs indéterminées, 525, 1498
- polynôme de plusieurs variables, 252
- polynôme de Taylor, 953
- polynôme scindé, 369
- polynôme trigonométrique, 1887
- polynômes, 178
- portée
 - mesure, 1089
- positif, 200
- potentiel, 1551, 1582
- ppcm
 - dans un anneau intègre, 160
- premier
 - corps, 359
 - deux polynômes entre eux, 272
 - deux éléments d'un anneau principal, 259
 - idéal, 256
 - sous corps, 359
- premier temps d'atteinte, 2352
- premier type
 - région solide, 1617
- presque
 - nulle, 235
 - partout, 1011
 - surjective, 1924
- primitif
 - polynôme, 273
 - au sens du pgcd, 273
 - racine, 1503
 - triplet pythagoricien, 267
 - élément d'un corps, 1491
 - élément d'une extension de corps, 390
- primitive, 814, 1580
 - de fonction continue, 931
 - et intégrale, 1114
 - fonction, 832
- primitive et intégrale, 1108
- principal
 - anneau, 256
 - idéal, 256
- principe
 - prolongement analytique, 1330
 - zéros isolés, 1329
- Principe de correspondance, 2414
- probabilité
 - conditionnelle, 2231
- problème
 - aux limites d'évolution, 2111
 - aux limites stationnaires, 2111
 - bien posé, 2111
 - limite de Dirichlet, 2111
 - limite de Von Neumann, 2111
- problème de Cauchy, 2088
- processus
 - adapté à une filtration, 2369
 - arrêté, 2374
 - croissant prévisible, 2374
 - Galton-Watson, 2365
 - Poisson, 2385
 - sans mémoire, 2271
- produit, 119
 - d'une mesure par une fonction, 1084
 - de convolution, 1871
 - et Fourier, 1963
 - de langages, 2392
 - de mots, 2391
 - distribution et fonction, 1991
 - espaces mesurés, 1099
 - espaces topologiques, 422
 - mixte, 672, 675
 - scalaire
 - en général, 618
 - sur $M(n, \mathbb{R})$, 692
 - sur $\mathbb{R}^n$, 663
 - semi-direct, 234
 - tensoriel
 - de représentations, 1230
 - vectorel, 671
- produit de Cauchy, 1144, 1146
- produit hermitien, 618
- produit pseudo-scalaire, 618
- produit remarquable, 1808
- produit scalaire sur $\mathbb{R}^n$, 319
- produit tensoriel, 729, 730
- projecteur
 - dans un module, 175
- projectif
 - complétion, 1702
 - droite, 1699, 1700
 - espace, 1699
 - groupe, 1706
 - hyperplan, 1700
 - plan, 1699
 - repère, 1707
 - sous-espace, 1699
- projection
 - orthogonale, 1770
- projection normale, 1903
- prolongement
 - analytique, 1330
 - utilisation, 1943

- de fonctions, 1325
 - lemme de Borel, 1210
- méromorphe de la fonction Γ , 1824
- par continuité, 783
 - dans $H^1(I)$, 2026
- par densité, 1325
- théorème de Hahn, 1030
- propriété d'intersection non vide, 432
- propriété universelle, 729
- prébase, 421
- précision
 - simple, 2121, 2122
- préhilbertien, 1767
- préserve l'orientation, 528
- puissance
 - d'un langage, 2393
 - d'un mot, 2392
 - d'un point, 1693
 - d'un test, 2332
 - d'une inversion, 1726
- période, 825
- pôle, 1439, 1815
- quasi-compact, 431
- quaternion, 412
- queue de liste d'indices, 33
- quotient, 162, 272
 - dans une suite de composition, 225
 - de groupe, 225
 - de groupes, 342
- quotient d'un espace vectoriel, 728
- racine
 - carré
 - de matrice hermitienne, 991
 - carré de matrice
 - hermitienne positive, 991
 - d'un polynôme, 273
 - de l'unité, 596, 1376, 1483, 1486, 1741
 - primitive, 1475
 - utilisation, 1482
 - de polynôme, 391
 - multiple, 2137
 - primitive, 1503
 - simple, 2137
- racine carrée, 651
- racine de l'unité, 1473
- raffinement, 1640
 - subdivision d'un pavé, 1607
- rang, 289, 513, 616
 - classe d'équivalence, 313
 - diagonalisation, 568
 - différentielle, 1283
 - utilisation, 1774
- rang d'une forme quadratique, 614
- rang d'une matrice, 312
- rare, 1005
- rationnels, 186
- rayon
 - de convergence, 1139
 - de courbure, 1666
 - de torsion, 1667
 - spectral, 575, 685
- recouvrement, 431
- rectangle
 - produit de tribus, 1049
- rectifiable, 1640
 - arc géométrique, 1656
- rejet
 - région dans une prise de décision, 2331
- relation d'équivalence, 107
- relations
 - coefficient-racines, 416
 - de Chasles, 491, 1594
- relativement
 - compact, 432, 1843
- relèvement, 1676
- Représentation
 - virgule flottante normalisée, 2121
- représentation, 329
 - de groupe fini
 - caractères de S_4 , 1231
 - fidèle, 329
 - groupe diédral, 1468
 - irréductible, 1222
 - produit tensoriel, 1230
 - régulière gauche, 1227
 - virgule fixe, 2121
- repère
 - affine, 506
 - cartésien
 - espace affine, 492
 - de Frenet, 1666
 - projectif, 1707
- reste, 162, 272
 - d'un développement limité, 960
- restriction d'une distribution, 2000
- Riemann
 - fonction, 1180
- risque
 - première espèce, 2332
 - quadratique, 2311
 - seconde espèce, 2332
- rotation
 - en dimension 2, 1388
- rotation d'angle θ , 1391
- rotation-homothétie, 1725

- rupture
 - corps, 392
- règle du produit nul, 161
- réci-proque
 - continuité, 441
 - dérivabilité, 823
- récurrent
 - nul, 2353
 - point d'un système dynamique, 1039
 - positif, 2353
 - état, 2353
- réduction
 - d'endomorphisme, 574
 - Frobénius, 583
 - Jordan, 586
- réel, 196
- réflexif, 1928
- réflexion, 1408
 - dans $\mathbb{R}^2$, 1384
 - glissée, 1406
 - par rapport à un hyperplan, 1369
- région
 - critique, 2331
 - de confiance exact, 2322
 - de rejet, 2331
- régularité
 - d'une mesure, 1037
 - extérieure de la mesure de Lebesgue, 1059
 - intérieure de la mesure de Lebesgue, 1061
- régulier
 - arc, 1653
 - chemin, 1561
 - point d'un arc, 1653
- régulier à droite, 160
- régulière
 - surface, 1552
- répulsif
 - point fixe, 1255
- résidu
 - méthode itérative, 2189
- résolvante, 2049
- résultant, 522
 - utilisation, 525, 1575
- Schrödinger, 2083
- Schur (théorème), 1224
- schéma
 - consistant, 2212
- schéma numérique, 2212
- section, 848
 - de graphe, 834
 - propriété des, 1094
- segment
 - dans $\mathbb{R}^p$, 636
 - dans un espace affine, 499
- semblables
 - matrices, 557
- semi-définie positive, 569
- semi-simple
 - endomorphisme, 551
- semi-symétrique
 - polynôme, 414
- seminorme, 485
- sesquilinéaire, 618
- signature
 - d'une permutation, 155
 - forme quadratique, 614
- similitude, 892
- simple
 - extension de corps, 390
 - fonction, 1046
 - groupe, 216
 - module, 176
- singularité, 1815
- singularité effaçable, 1815
- singularité isolée, 1815
- sinus, 1333
 - hyperbolique, 1185
- sinus cardinal, 1308, 1629
- solfège, 1474
- solution
 - générale, 2087
 - particulière, 2087
- somme
 - inférieure, 1612
 - partielle, 700
 - supérieure, 1612
- somme directe, 329
- somme directe (de représentations), 1221
- somme partielles
 - Abel angulaire, 1570
- sommet, 1690
- Sophie Germain, 360
- sous anneau, 250
- sous arc, 1639
- sous-additivité
 - sur algèbre de parties, 1008
- sous-espace
 - affine engendré par une partie, 497
 - caractéristique, 572
- sous-groupe
 - caractéristique, 215
 - distingué, 343
 - dans le groupe alterné, 347
 - engendré, 216
 - normal, 225, 342
- sous-martingale, 2369

- sous-module, 175
- sous-module engendré, 173
- sous-suite, 796
- spectre
 - matrice hermitienne, 667
 - matrice symétrique réelle, 568
- spectre d'un endomorphisme, 544
- sphère, 532
 - de Riemann, 1722
- stabilisateur, 229
- stabilité
 - d'un point d'équilibre, 2068
 - Lyapunov, 2068
- stable, 2129
 - schéma numérique, 2215
- stathme
 - sur $\mathbb{Z}[i]$, 363
- stathme euclidien, 263
- stationnaire
 - chaîne de Markov, 2361
- statistique, 2311
- statistiques
 - descriptives, 2303
- strictement
 - convexe
 - sur $\mathbb{R}^n$, 1294
- strictement convexe, 1285
- structure
 - complexe, 1673
- structure d'anneau canonique, 158
- structure réelle, 330
- Student, 2282, 2324
- subdivision, 1607
 - associée à une fonction, 1608
 - d'un intervalle, 1640
- subordonnée
 - norme, 683
- subpotent, 133
- suite, 235
 - arithmético-géométrique, 709
 - de Cauchy, 460
 - dans un corps, 184
 - de fonctions, 1848
 - théorème de Montel, 1942
 - de fonctions intégrables, 1245, 1840
 - de Jordan-Hölder, 225
 - définie par itération, 2144
 - exacte, 233
 - régularisante, 1968
 - équirépartie, 1951
 - critère de Weyl, 1951
- suite de composition, 225
- suite de variables aléatoires de Bernoulli, 2365
- suites adjacentes, 633
- support, 1609
 - d'une permutation, 155
 - distribution, 1993
 - famille d'éléments, 235
- supremum, 207
 - d'une suite d'ensembles, 1003
- sur-martingale, 2369
- surface paramétrée, 1551
- surjection, 104, 441
- surpotent, 133
- Sylow
 - p -Sylow, 333
- Sylvester (matrice), 522
- symbole
 - de Legendre, 1491
- symbole principal, 2101
- symétrique
 - polynôme, 414
- système
 - fondamental, 2047
 - orthonormé, 1775
 - trigonométrique, 1775, 1877
- système trigonométrique, 1899
- séparable, 1775
 - espace topologique, 427
 - extension de corps, 410
 - polynôme irréductible, 408
 - polynôme non constant, 408
 - élément d'une extension, 410
- sépare
 - les points, 927
- séquentiellement fermé, 458
- série
 - dans un espace vectoriel normé, 700
 - de Fourier, 1954, 1966
 - utilisation, 1959
 - de Laurent, 1818
 - de puissance, 1139
 - donnant $(1 - A)^{-1}$, 753
 - entière, 1139, 1212, 1966
 - Abel angulaire, 1570
 - processus de Markov, 2367
 - utilisation, 2253
 - fonctions, 1239, 1966
 - génératrice d'une suite, 1193
 - géométrique, 708
 - harmonique, 708
 - nombres, 1239
 - numérique, 1183, 1212
 - Riemann, 709
 - Taylor, 1194
- série convergente, 701

- série de Taylor, 953
- série divergente, 701
- série entière
 - fonctions holomorphes, 1801
- tangent
 - vecteur unitaire, 1666
- tangente, 1348, 1661
- Tangente hyperbolique, 2408
- tangente hyperbolique, 1187
- tangente à un chemin, 1526
- taubérien, 1238
- taux d'accroissement, 1286
- Taylor
 - série entière, 1193
- Taylor avec reste intégral, 1604
- temps d'arrêt, 2372
- temps de retour, 2352
- terminée
 - martingale, 2373
- test, 2331
 - bilatéral, 2332
 - unilatéral, 2332
- théorème
 - accroissements finis, 748
 - dans $\mathbb{R}$, 829
 - forme générale, 895
 - Ascoli, 1843
 - Baire, 485
 - Banach-Steinhaus, 717
 - avec seminormes, 1844
 - base incomplète, 281
 - Beppo-Levi, 1071
 - Bolzano-Weierstrass, 446
 - Borel-Cantelli, 2221
 - Borel-Lebesgue, 628
 - Brouwer, 1539
 - dimension 2, 1803
 - Bézout
 - polynômes, 372
 - utilisation, 523
 - Carathéodory, 503
 - Cauchy
 - groupe, 245
 - Cauchy-Arzela, 1542
 - Cauchy-Lipschitz, 1259
 - Cayley-Hamilton, 556, 990
 - central limite, 2263
 - processus de Poisson, 2387
 - Chevalley-Warning, 1498
 - chinois, 368
 - anneau des polynômes, 369
 - anneau principal, 259
 - Cochran, 2308
 - Cochrane, 2309
 - convergence
 - dominée de Lebesgue, 1081
 - monotone, 1071
 - de Baire, 490
 - de Jordan, 1691
 - de représentation de Riesz, 1774
 - des deux carrés, 365
 - version faible, 364
 - Dini, 916
 - Dirichlet, 1948
 - forme faible, 1486
 - Doob, 2373
 - du rang, 289
 - décomposition des noyaux
 - et exponentielle de matrice, 1205
 - extension d'isométrie, 1326
 - Fejér, 1949
 - fonction implicite dans $\mathbb{R}^n$, 1272
 - fonction implicite dans Banach, 1271
 - Fubini
 - dans $\mathbb{R}^n$, 1131
 - espace mesuré, 1126
 - version compacte dans $\mathbb{R}^2$, 1584
 - Fubini-Tonelli, 1124
 - fuite des compacts, 2052
 - Gauss
 - polynômes, 373
 - Gauss-Wantzel, 1517
 - Glivenko-Cantelli, 2317
 - Hahn-Banach, 1918
 - Hardy-Littlewood, 1239
 - Heine, 797
 - incidence, 1700
 - inversion locale, 1269
 - utilisation, 1283, 1620
 - isomorphisme
 - second, 222
 - troisième, 223
 - isomorphisme de Banach, 1843
 - Kronecker, 525
 - Lagrange, 224
 - Lie-Kolchin, 599
 - Lotka-Volterra, 2073
 - Markov-Takutani, 1542
 - Montel, 1942
 - Pappus
 - affine, 1704
 - projectif, 1704
 - Pearson, 2336
 - petit de Fermat, 360
 - Picard, 1256
 - point fixe

- Brouwer, 1803
- projection
 - cas vectoriel, 1770
 - partie fermée convexe, 1769
- prolongement de Hahn, 1030
- prolongement de Riemann, 1816
- Radon-Nikodym, 1089
 - complexe, 1090
- Rolle, 827
- Rothstein-Trager, 1575
- Runge, 1807
- Schauder, 1540
- Schur, 1224
- spectral, 573
 - autoadjoint, 661
 - matrice symétrique, 568
 - matrices normales, 668
- stabilité de Lyapunov, 2068
- Stone-Weierstrass, 928, 930
- Sylvester, 616
- taubérien, 1238
- taubérien faible, 1572
- transfert, 2254
- Tykhonov, 482
 - dénombrable, 484
 - fini, 483
- valeurs intermédiaires, 651
- Von Neumann, 1277
- Wedderburn, 1487
- Weierstrass, 447
 - élément primitif, 411, 1500, 1501
- théorème des extrémums liés, 1283
- théorème fondamental du calcul intégral, 1108
- topologie, 419, 536
 - *-faible, 488, 1990
 - p -adique, 761
 - discrète, 421
 - engendrée par une famille, 421
 - et seminormes, 486
 - faible, 684
 - forte, 684
 - grossière, 420
 - induite, 423
 - métrique, 444
 - produit, 422
 - sur $\mathcal{D}(\Omega)$, 1987
 - sur $\mathcal{D}(K)$, 1987
 - sur $C^\infty(\Omega)$, 1987
 - sur dual topologique, 488
 - usuelle sur $\mathbb{R}^n$, 536
- topologique
 - somme directe, 1772
- torsion, 1667
 - d'un groupe, 235
- totale, 1775
- trace, 2032
 - dual de $M(n, \mathbb{K})$, 327
 - endomorphisme, 558
 - matrice, 557
 - produit scalaire sur $M(n, \mathbb{R})$, 692
 - unicité pour la propriété de trace, 328
- transcendant, 379
- transformation
 - Fourier, 1966
 - gaussienne, 2169
- transformée
 - de Cauchy, 1813
 - de Fourier, 1961, 2252
 - continuité, 1964
 - groupe abélien fini, 1219
 - Fourier
 - distribution tempérée, 2011
 - Laplace, 2253
- transient
 - état, 2353
- transition
 - probabilité, 2341
- transitive, 233
- transitoire
 - état, 2353
- transposition, 154
- transposé, 529
- transposée, 325
- transvection, 982
- transvection (matrice), 311
- transversale, 232
- tribu, 1003
 - borélienne, 1032
 - de Baire, 1005
 - de Lebesgue, 1056
 - engendrée, 1004
 - par un événement, 2223
 - par une application, 1019
 - par une variable aléatoire, 2223
 - induite, 1004
 - produit, 1049
- tribu de Lebesgue sur S^1 , 1362
- trigonalisation
 - et polynôme caractéristique, 564
 - simultanée, 598, 599
- triplet
 - pythagoricien, 267
- triplet naturel, 109
- type
 - fini
 - en algèbre, 412

- espace vectoriel, 280
- tétraèdre régulier, 811
- unicité
 - des mesures, 1014
- uniformément continue, 485
- uniformément convexe, 1902
- unipotent, 160
- unitaire
 - normale principale, 1666
- valeur
 - principale (distribution), 2009
 - propre, 544
 - singulière, 575
- valeur absolue, 211
 - p -adique, 761
- valeur principale, 1831
- valeur propre
 - d'une forme quadratique, 606
 - forme quadratique, 606
- valuation
 - p -adique, 761
 - d'un polynôme, 271
- Vandermonde (déterminant), 519
- variable
 - de décision, 2332
- variable aléatoire, 2222
 - absolument continue, 2222
 - Bernoulli
 - marche aléatoire, 2346
 - utilisation, 2298
 - binomiale
 - utilisation, 2376
 - centrée, 2229
 - de Bernoulli
 - utilisation, 2376
 - de Rademacher, 2280
- variance, 2229
 - empirique, 2230, 2307
 - empirique corrigée, 2307
 - vecteur gaussien, 2276
- variation des constantes, 2043, 2047
- variété, 1283, 1523
- variété
 - orientée, 1533
- variété orientable, 1533
- vecteur
 - cyclique, 549
 - gaussien, 2276
 - propre, 544
 - unitaire normal, 1666
 - unitaire tangent, 1661
- Vitali (ensemble), 1062
- vitesse d'un chemin, 1639
- voisinage, 420, 536
- volume
 - d'une région solide, 1618
 - région bornée dans $\mathbb{R}^3$, 1616
- volume dans $\mathbb{R}^3$, 1536
- vraisemblance, 2314
- Weiner
 - constante, 2435
- Wronskien, 2075
- Éther, 2398
- Événement, 2403
- élément
 - inversible
 - dans un anneau, 160
- élément premier, 167
- élément régulier, 112
- élément régulier à gauche, 112
- élémentaire
 - polynôme symétrique, 414
- équation
 - aux variations, 2061
 - de Riccati, 2082
 - des classes, 232
 - des orbites, 231
 - différentielle
 - Hill, 2078
 - homogène, 2081
 - système, 2079
 - étude qualitative, 2079
 - diophantienne, 247, 266, 269
 - Fredholm, 1258
 - orbite-stabilisateur, 231
- équation de droite, 807
- équation différentielle
 - linéaire du premier ordre, 2092
 - linéaire du premier ordre, homogène, 2092
 - linéaire du second ordre, 2094
 - linéaire du second ordre, homogène, 2095
 - premier ordre, 2087
 - second ordre, 2087
 - variables séparables, 2089
- équation exponentielle, 947
- équation fonctionnelle, 947
- équation homogène associée, 2092
- équilibre
 - point point une équation différentielle, 2068
- équipotent, 133
- équivalence
 - de norme, 680
- équivalence de forme quadratiques, 617
- étagée

- fonction, 1046
- état
 - apériodique, 2363
 - récurrent, 2353
 - récurrent positif, 2353
 - transitoire, 2353
- étoile de Kleene, 2393
- étranger
 - dans leur ensemble, 272
- évaluation
 - polynôme plusieurs variables, 252

Liste des notations

$N \triangleleft G$ Le sous-groupe N est normal dans G , page 215

Algèbre

$[\mathbb{L} : \mathbb{K}]$ degré d'une extension de corps, page 376

$\mathcal{L}(E, F)$ Ensemble des applications linéaires de E dans F , page 286

$\mathbb{K}(A)$ corps contenant $\mathbb{K}$ et A , page 390

$\mathbb{K}[A]$ anneau contenant $\mathbb{K}$ et A , page 390

$\mathbb{N}_0$ les naturels non nuls : $\mathbb{N}_0 = \mathbb{N} \setminus \{0\}$, page 136

$\mathcal{M}_{n \times m}$ l'ensemble des matrices $n \times m$, page 286

∇f gradient de la fonction f , page 871

proj_V projection de $V \times W$ sur V , page 695

$\text{Span}(A)$ l'ensemble des combinaisons linéaires finies d'éléments de A , page 277

$df_a(u)$ Application de la différentielle de f sur le vecteur u , page 858

$f^{(n)}$ La n -ième dérivée de la fonction f , page 955

$o(x)$ fonction tendant rapidement vers zéro, page 957

(p) idéal engendré par p , page 250

$\mathbb{F}_p$ lorsque p est premier, page 359

$\mathbb{F}_{p^n}$ corps fini à p^n éléments, page 1489

$\text{Frac}(\mathbb{A})$ Le corps des fractions de l'anneau $\mathbb{A}$, page 184

$\text{Fun}(X, Y)$ les applications de X vers Y , page 158

$S(E)$ Les opérateurs autoadjoints de E , page 530

U_n Le groupe des racines n °de l'unité., page 1473

$\text{res}(P, Q)$ résultat des polynômes P et Q , page 522

$\sqrt{A}$ racine d'une matrice hermitienne positive, page 991

$\theta_\alpha(P)$ la multiplicité de α par rapport à P , page 274

$A[X]$ tous les polynômes de degré fini à coefficients dans A , page 180

$A_n[X]$ les polynômes à coefficients dans A et de degré inférieur à n , page 270

$C(P)$ matrice compagnon, page 582

$D \mid P$ D divise P , page 272

$E_\lambda(u)$ Espace propre de u , page 544

$\text{mat}_{\mathcal{B}}(q)$ matrice de q dans la base $\mathcal{B}$, page 1317

$U(A)$ ensemble des inversibles, page 160

Ensembles de matrices

$S^+(n, \mathbb{R})$ matrices symétriques définies positives, page 569

$S^{++}(n, \mathbb{R})$ matrices symétriques strictement définies positives, page 569

$\text{Aut}(E)$ automorphisme de l'espace vectoriel E , page 286

$\text{End}(E)$ les endomorphismes de E , page 286

$L(E, F)$ applications linéaires bornées (continues), page 691

$O(n, \mathbb{R})$ le groupe des matrices orthogonales, page 531

$\Omega(E)$ formes quadratiques non dégénérées, page 1313

$Q(E)$ formes quadratiques réelles sur E , page 603

$Q^+(E)$ formes quadratiques positives, page 1313

$Q^{++}(E)$ formes quadratiques strictement définies positives, page 1313

$S_n^{p,q}(\mathbb{R})$ matrices symétriques réelles de signature (p, q) , page 1314

$\beta(s)$ Vecteur unitaire de la binormale, page 1666

$\gamma \sim g$ Équivalence d'arcs paramétrés, page 1655

$\nu(s)$ Vecteur unitaire de la normale principale, page 1666

$c(s)$ rayon de courbure, page 1666

$t(s)$ Torsion, page 1667

Géométrie

$P(E)$ l'espace projectif de E , page 1699

$(x_0 : \dots : x_n)$ coordonnées homogènes dans un espace projectif, page 1718

$\text{Conv}(A)$ enveloppe convexe, page 501

$\mathbb{C}[G]$ combinaisons d'éléments de G à coefficients dans $\mathbb{C}$, page 1221

$\text{PGL}(E)$ groupe projectif, page 1706

B^o orthogonal dans le dual, page 323

$P_1(\mathbb{C})$ sphère de Riemann, page 1722

Chaînes de Markov

$\pi(x)$ lié au temps de retour, page 2355

Probabilités et statistique

$\sigma(X)$ La tribu engendrée par la variable aléatoire X , page 2223

$a \wedge b$ $\min(a, b)$, page 2373

K_X matrice de covariance d'un vecteur gaussien, page 2276

$m(\mathcal{A})$ Ensemble des fonctions $\mathcal{A}$ -mesurables, page 1018

Théorie des groupes

$(G/H)_g$ classes à gauche, page 230

$[a]_p$ ensemble des $a + kp$, page 248

$[G, G]$ groupe dérivé, page 221

- $[g, h]$ commutateur dans un groupe, page 220
 $\text{Aff}(\mathbb{R}^n)$ Le groupe des applications affines bijectives de $\mathbb{R}^n$, page 511
 gr_G groupe engendré, page 216
 $\hat{G}$ groupe des caractères de G , page 1217
 σ_x réflexion par rapport à x , page 1408
 A_n groupe alterné, page 345
 $D(G)$ groupe dérivé, page 221
 D_n groupe diédral, page 1375
 G^{ab} groupe abélianisé de G , page 221
 $N \times_\phi H$ produit semi-direct, page 234
 S_n le groupe symétrique, page 154

Topologie et théorie des ensembles

- $\text{Adh}(A)$ adhérence de A , page 425
 $\complement A$ Le complémentaire de l'ensemble A , page 106
 $\text{Diam}(A)$ Diamètre de la partie A , page 796
 ∂A La frontière de l'ensemble A , page 539
 $A \Delta B$ différence symétrique, page 106
 A^c complémentaire de A , page 106

Analyse

- $\text{Isom}(X)$ Le groupe des isométries de X , page 456
 $\mu \ll \nu$ La mesure μ est absolument continue par rapport à la mesure ν , page 1089
 $C^\infty(\mathbb{R}, \mathcal{S}'(\mathbb{R}^d))$ Fonctions à valeurs dans les distributions., page 2083
 $C^\infty(I, \mathcal{D}'(\mathbb{R}^d))$ fonctions à valeurs dans les distributions, page 1996
 $(S, \hat{\mathcal{F}}, \hat{\mu})$ complété de l'espace mesuré $(S, \hat{\mathcal{F}}, \hat{\mu})$, page 1024
 $\mathcal{L}(E, F)$ Les applications linéaires de E vers F , page 739
 $\mathcal{L}^{(n)}(V, W)$ L'espace des applications n -linéaires $V^n \rightarrow W$, page 906
 $\arg(z)$ La valeur principale de l'argument de $z \in \mathbb{C}$, page 1831
 L Les applications linéaires continues de E vers F , page 739
 $\mathbb{D}_b$ l'ensemble de écritures décimales en base b , page 711
 $\mathbb{R}$ l'ensemble des réels, page 196
 $\mathbb{R}^+$ les réels positifs ou nuls, page 200
 $\exp$ exponentielle, page 1170
 $\mathcal{H}'$ dual, page 1773
 $\liminf a_n$ limite inférieure, page 634
 $\limsup a_n$ limite supérieure, page 634
 $\mathcal{L}^p$ espace de Lebesgue, sans les classes, page 1845
 $\mu \perp \nu$ mesures perpendiculaires, page 1089

- μ^* La mesure extérieure associée à la mesure μ , page 1015
- $\partial_z, \partial_{\bar{z}}$ dérivées partielles d'une fonction complexe, page 1795
- $\text{proj}_K(x)$ projection orthogonale de x sur y , page 1770
- $\sigma(\mathcal{A})$ tribu engendrée par $\mathcal{D}$, page 1004
- $\mathcal{D}(\Omega)$ Les fonctions C^∞ à support compact sur Ω , page 1990
- $\mathcal{S}'(\mathbb{R}^d)$ espace des distributions tempérées, page 2009
- $A^2(\Omega)$ espace de Bergman, page 1943
- $A^\perp$ orthogonal d'une partie., page 1772
- $C_c(I)$ fonctions continues à support compact dans I , page 1870
- $f \sim g$ fonctions ayant des limites équivalentes, page 845
- $H^1(\Omega)$ espace de Sobolev sur Ω , page 2028
- $H^1(I)$ espace de Sobolev, page 2023
- $H^m(M)$ espace de Sobolev, page 2030
- $L^1_{loc}(I)$ fonctions intégrables sur les compacts de I , page 2023
- L^p espace de Lebesgue avec les classes, page 1847
- $M_i\varphi$ La fonction $x \mapsto x_i\varphi(x)$, page 1938
- S_nf somme partielle de série de Fourier, page 1901

Chapitre 0

Introduction

0.1 Auteurs, contributeurs, sources et remerciements

Les remerciements, dans chaque catégorie, sont mis dans l'ordre chronologique approximatif. Les noms en couvertures sont ceux qui ont fourni du code L^AT_EX (typiquement : un patch via github), par ordre chronologique approximatif d'entrée dans le projet.

0.1.1 Ceux qui ont travaillé sur le Frido

- (1) Carlotta Donadello pour l'ensemble du cours de CTU de géométrie analytique 2010-2011. Une grosse partie de « analyse réelle » vient de là.
- (2) Les étudiants de géométrie analytique en CTU 2010-2011 ont détecté d'innombrables coquilles. Les étudiants du cours présentiel de géométrie analytique 2011-2012 ont signalé un certain nombre d'incorrections dans les exercices et les corrigés. Les agrégatifs de Besançon 2011-2012 pour leurs plans et leurs développements.
- (3) Lilian Besson pour m'avoir signalé un paquet de fautes, et quelques points pas clairs en statistiques.
- (4) Plouf qui m'a signalé une coquille dans le fil [la-selection-scientifique-de-la-semaine-numero-106](#).
- (5) Benjamin de Block pour des coquilles et une mise au point sur les conventions à propos de $\mathbb{R}^+$ et $(\mathbb{R}^+)^*$.
- (6) Olivier Garet pour avoir répondu à plein de questions de probabilités.
- (7) François Gannaz pour de la relecture et une version plus claire de la preuve (et de l'énoncé) de la proposition [19.8](#).
- (8) Danarmk pour des réponses à des questions dans les commentaires (allongement pour éviter un Overfull hbox) <http://linuxfr.org/nodes/110155/comments/1675589>. Et aussi pour [une discussion](#) à propos de la topologie sur $\mathcal{D}(\Omega)$.
- (9) Cédric Boutilier pour des réponses à des questions de probabilité statistique. <https://github.com/LaurentClaessens/mazhe/issues/16>
- (10) Remsirems pour des réponses à des questions d'analyse¹
- (11) Bertrand Desmons pour plusieurs patches rendant plus clairs de nombreux passages sur les suites de Cauchy dans $\mathbb{Q}$.
- (12) Anthony Ollivier pour m'avoir fait remarquer qu'il n'est pas vrai que $A[X]$ est euclidien lorsque A est intègre (contre-exemple : $A = \mathbb{Z}$). Ça fait une faute de moins dans le Frido.
- (13) ybailly pour avoir détecté un bon nombre de coquilles dans la partie sur les ensembles de nombres.
- (14) Éric Guirbal pour le remplacement de `frenchb` par `french`.

1. <http://linuxfr.org/nodes/110155/comments/1675813>

- (15) cdrcprds pour une réponse à une question d'algèbre, démonstration à l'appui à propos de [pgcd](#). Également pour sa relecture sans pitié de la partie sur la cardinalité (en particulier $A \approx A \setminus B$) et pour avoir pointé l'utilisé du théorème de comparabilité cardinale.
- (16) Antoine Bensalah pour avoir répondu à une question sur Lax-Milgram tout en même temps que pointé une erreur dans la démonstration et fourni l'exemple [25.60](#) sur l'optimalité de l'inégalité.
- (17) Guillaume Deschamps pour ses remarques à propos du fait que le chapitre « constructions des ensembles » est très ardu.
- (18) Guillaume Barriere pour sa relecture attentive jusqu'aux corps.
- (19) Samy Clementz pour avoir découvert une faute dans la définition de mesure positive sur un espace mesurable.
- (20) Sylvain Rousseau pour avoir clarifié une construction dans le théorème de Bower version C^∞ .
- (21) Maxmax pour des typos dans l'index thématique.
- (22) Laurent Choulette pour une typo dans les propriétés du neutre d'un groupe.
- (23) Pierre Lairez pour la démonstration du théorème d'inversion de limite et de dérivée [12.328](#) sans passer par les intégrales (et les lemmes correspondants à propos du module de continuité).
- (24) Gregory Berhuy pour des réponses d'algèbres dans les catégories facile, moyen et difficile.
- (25) Benoît Tran pour avoir signalé un paquet de typos dans la démonstration de l'ellipsoïde de John-Loewner et ses dépendances.
- (26) Provatisus pour avoir signalé un paquet de choses pas claires, et surtout pour avoir trouvé une faute dans la démonstration du fait qu'une fonction continue sur $\mathbb{Q}$ se prolonge en une fonction continue sur $\mathbb{R}$. Et pour cause : cet énoncé est faux. <https://github.com/LaurentClaessens/mazhe/issues/124>
- (27) William pour l'environnement `example` qui gère correctement le triangle.
- (28) Colin Pitrat pour de nombreuses remarques, typos et relecture de théorèmes.
- (29) Bruno Turgeon pour une très belle moisson de fautes de frappe (euphémisme pour dire « mon ignorance crasse de l'orthographe »).
- (30) Sacha Dhénin pour une belle quantité de fautes de frappes et pour avoir soulevé quelques points pas clairs (par exemple la définition du sous-groupe engendré dans le cas de la partie vide).
- (31) Patrice Goyer pour m'avoir signalé quelques fautes et pas mal de points pas clairs dans les polynômes et la théorie généraliste des ensembles.

0.1.2 Aide directe, mais pas volontairement sur le Frido

- (1) Plein de monde pour diverses contributions à des énoncés d'exercices. Pierre Bieliavsky pour les énoncés d'analyse numérique (MAT1151 à Louvain la Neuve 2009-2010). Jonathan Di Cosmo pour certaines corrections de MAT1151. François Lemeux, exercices sur les normes de matrices et correction de coquilles. Martin Meyer et Mustapha Mokhtar-Kharroubi pour certains exercices du cours *Outils mathématiques* (surtout ceux des DS et examens).
- (2) Nicolas Richard et Ivik Swan pour les parties des exercices et rappels de calcul différentiel et intégral (Université libre de Bruxelles, 2003-2004) qui leurs reviennent.
- (3) Carlotta Donadello pour la partie géométrie analytique : topologie dans $\mathbb{R}^n$, courbes, intégrales, limites. (Université de Franche-Comté 2010-2012)
- (4) Le forum usenet de math, en particulier pour la construction des corps fini dans la fil « Vérifier qu'un polynôme est primitif » initié le 20 décembre 2011.
- (5) Mihai Bostan nous a donné ses notes manuscrites de son cours présentiel de géométrie analytique 2009-2010. (Presque) Toute la structure du cours de géométrie analytique lui est due (qui est maintenant fondue un peu partout dans les chapitres d'analyse).

0.1.3 Des gens qui ont fait un travail qui m'a bien servi

- (1) Arnaud Girand pour avoir mis ses développements bien faits en ligne. Une bonne vingtaine de résultats un peu partout dans ces notes viennent de lui.
- (2) Le site <http://www.les-mathematiques.net> m'a donné les preuves de nombreux résultats.
- (3) Pierre Monmarché pour son document en ligne tout plein de développements, et des réponses à des questions.
- (4) Tous les contributeurs du Wikipédia francophone (et aussi un peu l'anglophone) doivent être remerciés. J'en ai pompé des quantités astronomiques ; des articles utilisés sont cités à divers endroits du texte, mais ce n'est absolument pas exhaustif. Il n'y a à peu près pas un résultat important de ces notes dont je n'aie pas lu la page Wikipédia, et souvent plusieurs pages connexes.
- (5) Les intervenants du fil « [Antisymétrisation, alterné, déterminant et caractéristique](#) » sur [les-mathematiques.net](#) m'ont bien aidé pour la section sur les déterminants 9.1 (bien qu'ils ne le savent pas).
- (6) Xavier Mauquoy pour l'énoncé et la preuve du théorème 3.35.
- (7) David Revoy pour les dessins de Pepper&Carrot [de la couverture](#).

J'ai souvent donné entre parenthèses à côté des mots « théorème », « lemme » ou « proposition » une ou plusieurs références vers les sources de la preuve que je donne. Ce sont parfois des liens vers la bibliographie ; parfois aussi des liens hypertextes vers des sites, des blogs, etc. Tous ces gens ont fait du bon boulot. Sans toute cette « communauté », l'internet serait mort ².

0.2 Originalité

Ces notes ne sont pas originales par leur contenu : ce sont toutes des choses qu'on trouve facilement sur internet ; je crois que la bibliographie est éloquent à ce sujet. Ce cours se distingue des autres sur les points suivants.

La longueur J'ai décidé de ne pas me soucier de la taille du fichier. Il fera cinq mille pages s'il le faut, mais il restera en un bloc. Étant donné qu'il n'existe qu'une seule mathématique, il ne m'a pas semblé intéressant de produire une division artificielle entre l'analyse, la géométrie ou l'algèbre. Tous les résultats d'une branche peuvent (et sont) être utilisés dans toutes les autres branches.

Dans cette optique, je me suis évertué à ne créer que des références « vers le haut ». À moins d'oubli de ma part ³, il n'y a aucun endroit du texte qui dépend d'un lemme démontré plus bas. Le fait qu'un théorème B soit plus bas qu'un théorème A signifie qu'on peut démontrer A sans savoir B .

La licence Ce document est publié sous une licence libre. Elle vous donne explicitement le droit de copier, modifier et redistribuer.

Les mises à jour Ce document est régulièrement mis à jour. Des fautes d'orthographe sont corrigées (presque) chaque jour. Si vous me signalez une faute de mathématique, elle sera corrigée.

Transparence Je ne fais pas semblant que ces notes soient parfaites. Les points sur lesquels je ne suis pas sûr, les preuves que j'ai inventées moi-même sont clairement indiqués pour inciter le lecteur à redoubler de prudence. Une liste de questions à résoudre est incluse en la section 0.7. Voir 0.3 pour plus de détails.

2. Cette dernière phrase doit être comprise comme un appel à ne pas utiliser Moodle et autres iCampus pour diffuser vos cours de math, ou en tout cas pas comme moyen exclusif.

3. Par exemple pour les théorèmes pour lesquels je n'ai pas lu ni a fortiori écrit de preuves.

0.3 Les choses qui doivent vous faire tiquer

Un cours de math doit toujours être lu attentivement, surtout si vous avez l'intention de resservir à un jury le fruit de vos lectures. Dans ce livre, trois éléments doivent vous faire redoubler de prudence.

La référence [1] D'abord les références à [1] indiquent qu'une bonne partie de ce qui suit est de l'invention personnelle de l'auteur. Cela ne veut évidemment pas dire que c'est moi qui ait découvert le résultat. Ça veut dire que je n'ai pas trouvé le résultat ou certaines parties de la preuve.

Les notes en bas de page Certaines notes en bas de page sont écrites dans une fonte spéciale⁴. Elles indiquent des points sur lesquels je doute ou des étapes de calculs que je ne parviens pas à reproduire en suivant mes sources. Lorsque vous voyez une telle note, redoublez de prudence, allez voir la source, et écrivez-moi si vous pouvez résoudre le problème.

Les environnements dédiés Et enfin certains problèmes sont indiqués plus longuement dans un environnement dédié en petits caractères comme ceci :

⚠ Avertissement/question au lecteur !! 0.1

Les choses écrites comme ceci sont des questions ou des éléments sur lesquels j'ai un doute. Lisez-les attentivement. Ces notes mentionnent des points que personnellement je n'oserais pas affirmer plein d'aplomb à un jury d'agrégation.

0.4 Quelques choix qui peuvent provoquer des quiproquos

Comme tout cours de mathématique, ce cours fait des choix qui sont parfois discutables. Voici quelques points sur lesquels les choix faits ici ne sont peut-être pas ceux fait par tout le monde. Ce sont donc des points sur lesquels vous devez faire attention pour éviter les quiproquos lors par exemple d'un oral dans un concours.

- (1) Nous utilisons la définition « épointée » de limite d'une fonction en un point. Elle diffère de celle donnée par le ministère de l'enseignement en France. Si votre but est de passer un concours d'enseignement en France, vous devriez lire 12.2; dans tous les autres cas, la définition prise ici est celle qu'il vous faut.
- (2) Un compact est une partie d'un espace topologique pour lequel tout recouvrement par des ouverts admet un sous-recouvrement fini. Le fait d'être séparable n'est pas inclus dans la définition de compact. De nombreux textes français incluent la séparabilité dans la compacité.
- (3) Le logarithme sur $\mathbb{C}$ est une application $\ln: \mathbb{C}^* \rightarrow \mathbb{C}$ définie partout sauf en zéro. Elle n'est donc pas continue sur la fameuse demi-droite. À ne pas confondre avec une *détermination* du logarithme qui est par définition continue et donc non définie sur la demi-droite. Cela est un choix très discuté. La raison de donner à la notation « $\ln$ » cette signification est simplement de suivre l'usage de Sage. Pour Sage, $\ln(-1)$ existe et vaut $i\pi$. Voir les remarques 26.75.
- (4) Le mot « corps » n'implique pas la commutativité, et nous n'utilisons pas la terminologie « anneau à division ». Voir la remarque 1.191 et la discussion 6.1.

0.5 Autres choix pas spécialement standards

Nous listons ici quelques choix qui n'induisent pas de différences ou d'incompatibilité avec les autres cours, mais qui doivent être compris et justifiés.

- (1) Nous n'utilisons pas les notations $o(x)$ ou autres $O(N^2)$. D'abord parce que je n'ai jamais très bien compris comment elles fonctionnent, et ensuite (surtout) parce que ces notations

4. Les notes comme celle-ci signifient qu'il y a certaines chose dont je ne suis pas sûr.

induisent en erreur. Ce sont des notations qui cachent, sous des notations à peu près intuitive, l'utilisation de théorèmes pas simples.

Écrire

$$f(x) = P(x) + o(x^2), \quad (0.1)$$

c'est un peu comme quand on écrit (horreur !)

$$F(x) = \int f(x)dx + C. \quad (0.2)$$

Où est le x à droite ? Quel est le statut de C ?

Même chose pour la notation $f(x) = P(x) + o(x^2)$. Le x de $o(x^2)$ est-il le x qu'on a à gauche ? Si $g(x) = Q(x) + o(x^2)$, est-ce le même o que celui de f ?

- (2) Nous allons être plus calme avec la notation $A[X]$ pour les polynômes sur l'anneau A , et encore moins $A[X_1, \dots, X_n]$ pour les polynômes de n variables. Au lieu de cela nous utilisons $\mathcal{P}(A)$ et $\mathcal{P}_n(A)$.

Est-ce que vous diriez que $A[X] = A[Y]$? Quelle est exactement la nature de X dans $P = X^2 + 1$ ou dans $P(X) = X^2 + 1$? Si $P \in A[X]$ vaut $P(X) = X^2$ et si $Q \in A[Y]$ vaut $Q(Y) = Y^2$, est-ce que vous oseriez écrire $P = Q$?

0.5.1 Mathématique intéressante

Définition 0.2.

Une notion mathématique est **intéressante** si elle permet de répondre à une question que l'on peut se poser sans connaître la notion.

Exemple 0.3.

Étant donné un segment dans le plan, quels sont les triangles rectangles dont ce segment est l'hypoténuse ?

Nous n'avons pas besoin de cercles pour poser cette question. Mais nous avons besoin de connaissances sur les cercles pour y répondre. Donc l'étude des cercles est intéressante. $\triangle$

Exemple 0.4.

Comment fonctionne la gravitation ?

Cette question peut être posée sans connaître de calcul tensoriel, d'équations différentielles ou d'intégrales. Et pourtant, tous ces concepts sont utiles pour y répondre. $\triangle$

0.6 Sage est là pour vous aider

Il existe de nombreux logiciels de mathématique. Notre préféré est **Sage** pour une raison très précise : Sage est (en simplifiant) un module pour python. Donc quand on travaille en Sage, on dispose de tout Python. La syntaxe et la structure de Sage ne sont pas *ad hoc* pour faire des maths, et ce qu'on apprend en Sage peut être recyclé pour faire n'importe quoi : navigateur web, script de manipulation de texte, traitement d'image, réseau neuronaux, ...

Sage est un logiciel disponible pour l'épreuve de modélisation de l'agrégation de mathématique ; il y a donc de bonnes chances que vous en ayez l'usage.

0.6.1 Lancez-vous dans Sage

- (1) Aller sur <http://www.sagemath.org>,
- (2) créer un compte,
- (3) créer des feuilles de calcul et s'amuser!!

Il y a beaucoup de [documentation](#) sur le [site officiel](#)⁵, et nous vous conseillons particulièrement le livre [3].

Si vous comptez utiliser régulièrement ce logiciel, je vous recommande *chaudement* de [l'installer](#) sur votre ordinateur.

0.6.2 Exemples de ce que Sage peut faire pour vous

Ce livre est émaillé de petits bouts de code en Sage montrant ses différentes fonctionnalités là où nous en avons besoin⁶. Voici une liste (non exhaustive) de ce que Sage peut faire pour vous.

- (1) Calculer des limites de fonctions, exemples [43.1](#) et [43.2](#).
- (2) Tracer des graphes de fonctions, exemple [43.2](#).
- (3) Tracer des courbes en trois dimensions, voir exemple [12.160](#). Notez que pour cela vous devez installer aussi le logiciel Jmol. Pour Ubuntu, c'est dans le paquet `icedtea6-plugin`.
- (4) Calculer des dérivées partielles de fonctions à plusieurs variables, voir exemple [43.3](#).
- (5) Résoudre des systèmes d'équations linéaires. Voir les exemples [43.4](#) et [43.5](#). Lire aussi [la documentation](#).
- (6) Tout savoir d'une forme quadratique, voir exemple [43.6](#).
- (7) Calculer la matrice hessienne de fonctions de deux variables, déterminer les points critiques, déterminer le genre de la matrice hessienne aux points critiques et écrire les extrémums de la fonctions (sous réserve d'être capable de résoudre certaines équations), voir les exemples [43.7](#) et [43.8](#).
- (8) Indiquer une infinité de solutions à une équation en utilisant des paramètres. L'exemple [43.9](#) montre ça avec une équation algébrique. Un exemple concernant des fonctions trigonométriques :

```
sage: solve(sin(x)/cos(x)==1,x,to_poly_solve=True)
[x == 1/4*pi + pi*z1]
sage: solve(sin(x)**2==cos(x)**2,x,to_poly_solve=True)
[sin(x) == cos(x), x == -1/4*pi + 2*pi*z86, x == 3/4*pi + 2*pi*z84]
```

Notez l'option `to_poly_solve=true` dans `solve`.

- (9) Calculer des dérivées symboliquement, voir exemple [43.10](#).
- (10) Calculer des approximations numériques comme dans l'exemple [43.11](#).
- (11) Calculer dans un corps de polynômes modulo comme $\mathbb{F}_p[X]/P$ où P est un polynôme à coefficients dans $\mathbb{F}_p$. Voir l'exemple [19.68](#).

Sage peut en général faire tout ce que vous êtes capable de faire à l'entrée en master et probablement bien plus, à la notable exception des limites à deux variables.

Remarque 0.5.

Sage peut toutefois vous induire en erreur si vous n'y prenez pas garde parce qu'il sait des choses en mathématique que vous ne savez pas. Par conséquent il peut parfois vous donner des réponses (mathématiquement exactes) auxquelles vous ne vous attendez pas. Voir par exemple [15.129](#) pour le logarithme de nombres négatifs. Et aussi ceci :

```
1 SageMath version 7.3, Release Date: 2016-08-04
2
3 Type "notebook()" for the browser-based notebook interface.
4 Type "help()" for help.
```

5. <http://www.sagemath.org>

6. Soit un vrai besoin comme tracer un graphique en 3D, soit de la paresse comme calculer une grosse dérivée.

```

5
6 sage: limit(1/x,x=0)
7 Infinity
8 sage: limit(1/x**2,x=0)
9 +Infinity

```

tex/sage/sageSnip017.sage

Sage fait une différence entre `Infinity` et `+Infinity` et donne

$$\lim_{x \rightarrow 0} \frac{1}{x} = \infty \quad (0.3)$$

ainsi que

$$\lim_{x \rightarrow 0} \frac{1}{x^2} = +\infty. \quad (0.4)$$

Voir aussi la compactification en un point d'Alexandroff 7.68.

0.7 Comment contribuer et aider ?

0.7.1 Des preuves qui manquent

Vous trouverez un peu partout des énoncés sans preuves. Certaines sont sûrement très faciles, et d'autres probablement assez compliquées. N'hésitez pas à rédiger une preuve et me l'envoyer.

Vous pouvez m'envoyer vos preuves sous forme de « c'est bien fait dans tel cours », avec une URL.

Ne me dites juste pas « c'est bien fait dans tel *livre* ». Je ne travaille pas à l'université, et je n'ai pas accès à une bibliothèque universitaire ; je n'ai donc pas réellement accès à ces fameux « livres » dont tout le monde parle.

0.7.2 Du texte qui manque

Vous remarquerez que de nombreuses pages du Frido sont des enchainements de théorèmes et démonstrations sans articulations. Autrement dit, il manque ce qu'à l'agrégation on dirait à l'oral quand on présente le plan. Si vous avez des idées de choses à ajouter ici où là, faites le moi savoir.

0.7.3 Des exemples qui manquent

Si vous connaissez de bons exemples, faites-le moi savoir.

0.7.4 Trucs de programmation et de L^AT_EX

- (1) Comment faire en sorte que les mots commençant par « é » soient avec les « e » dans l'index, et non avant les « a » ? Il me faudrait un mécanisme plus automatique que faire `machin@truc`.
- (2) Il y a des problèmes dans la table des matières. « Table des matières », « Index », et « Liste des notations » ne pointent pas vers la bonne page.
- (3) Si vous savez comment faire `pdf -> epub` pour créer un eBook, faites le moi savoir. Cahier des charges :

— libre, disponible sur Ubuntu

— en ligne de commande (en tout cas : exécutable depuis un script en python ou C++)

Attention : le Frido étant un truc assez compliqué, avant de répondre la première chose qui vous passe par la tête, assurez-vous que votre solution fait avancer les choses sur le Frido et non sur un petit document de test.

Nous en avons déjà un peu discuté sur <https://github.com/LaurentClaessens/mazhe/issues/13>. Il faudra entre autres faire un script qui remplace tous les environnements

tizk des fichiers `*.pstricks` (désolé pour la convention de nommage historique) par un simple `\includegraphics` du fichier `pdf` correspondant que l'on trouvera dans le répertoire `auto/pictures_tikz`.

- (4) Écrire un script (en python ou autre) qui prend en argument deux numéros ou noms de chapitres et qui retourne l'ensemble des lignes du premier qui contient des `ref` ou `eqref` dont le label correspondant est dans le second.

Attention : il faut tenir compte de `input` de façon récursive.

Bonus : calculer le hash sha1 de chaque ligne du résultat et ne pas l'afficher si il se trouve dans la liste du fichier `commons.py`.

0.8 Les politiques éditoriales

Certaines parties de ce texte ne respectent pas les politiques éditoriales. Ce sont des erreurs de jeunesse, et j'en suis le premier triste.

0.8.1 Licence libre

Je crois que c'est clair.

0.8.2 pdf_{flat}tex

Tout est compilable avec pdf_LAT_EX. Pas de `pstricks`, de `psfrag` ou de `ps<quoiquecesoit>`.

0.8.3 utf8

Je crois que c'est clair.

0.8.4 Notations

On essaie d'être cohérent dans les notations et les conventions. Pour la transformée de Fourier par exemple, je crois que la définition du produit scalaire dans L^2 , des coefficients de Fourier, de la transformation et de la transformation inverse sont cohérents. Cela demande, lorsqu'on suit un livre qui ne suit pas les conventions utilisées ici, de convertir parfois massivement.

0.8.5 De la bibliographie

On évite d'écrire en haut de chapitre « les références pour ce chapitre sont ... ». Il est mieux d'écrire au niveau des théorèmes, entre parenthèses, les références.

Lorsqu'on écrit l'énoncé d'un théorème sans retranscrire la démonstration, il faut mettre une référence vers un document *en ligne* qui en contient la preuve. Il est vraiment fastidieux de chercher une preuve sur internet et de tomber sur des dizaines de documents qui donnent l'énoncé mais pas la preuve.

0.8.6 Faire des références à tout

Lorsqu'un utilise le théorème des accroissements finis, il ne faut pas écrire « d'après le théorème des accroissements finis, blabla ». Il faut écrire un `\ref` explicite vers le résultat. Cela alourdit un peu le texte, mais lorsqu'on joue avec un texte de plus de 2000 pages, il est parfois laborieux de trouver le résultat qu'on cherche (surtout s'il existe plusieurs versions d'un résultat et que l'on veut faire référence à une version particulière).

0.8.7 Des listes de liens internes

Le début du Frido contient une espèce d'index thématique. Il serait bon de l'étoffer.

0.8.8 Pas de références vers le futur

Dans le Frido, *aucune* preuve ne peut faire une référence vers un résultat prouvé plus bas. On n'utilise pas le théorème 10 dans la démonstration du théorème 7. Cela est une contrainte forte sur le découpage en chapitres et sur l'ordre de présentation des matières.

Il est bien entendu accepté et même encouragé de mettre des notes du type « Nous verrons plus loin un théorème qui ... ». Tant que ce théorème n'est pas *utilisé*, ça va.

0.8.9 Écriture inclusive

Je suis triste de devoir le préciser, mais le Frido est écrit en français. Nous n'utiliserons donc pas de féminisation abusives, et accepterons comme correcte des tournures comme, en parlant d'une fonction, « *elle* est *un* contre-exemple », ou en parlant d'un lemme que « *il* est *une* conséquence ».

Parfois le genre d'un objet n'est pas bien défini. Par exemple $3/4$ est *la* classe d'équivalence de $(3, 4)$ dans $\mathbb{Z} \times \mathbb{Z} \setminus 0$; mais en même temps c'est *un* élément de $\mathbb{Q}$. Nous utiliserons alors, prudemment, un neutre en disant « *il* est plus petit que 1 ».

Chapitre 1

Construction des ensembles de nombres

1.1 Quelques éléments sur les ensembles

1.1.1 Petit mot d'introduction

Le Frido n'est pas supposé être lu dans l'ordre de la première à la dernière page ; les matières y sont présentées dans l'ordre logique mathématique, et non dans l'ordre logique pédagogique, et encore moins par ordre de difficulté croissante.

1.1 (On saute la théorie des ensembles).

En mathématique, si on lit une démonstration et que l'on veut vraiment tout justifier, et justifier toutes les étapes de tous les résultats utilisés, on tombe forcément un jour sur les axiomes.

Or l'axiomatique est un sujet particulièrement difficile. Nous n'allons donc pas « tout justifier » jusque là. Nous n'allons même pas préciser quel système d'axiome est utilisé. En particulier nous n'allons pas donner l'axiomatique des ensembles : nous allons supposer connus les ensembles et leurs principales propriétés.

Bref. Nous supposons avoir une théorie des ensembles qui tient la route. En particulier nous supposons connues les notions suivantes :

- (1) ensemble vide,
- (2) ensemble, appartenance, intersection, union,
- (3) application entre deux ensembles, notation $f(x)$ pour désigner l'image de x par f ,
- (4) produit cartésien de plusieurs ensembles.

Ce sont toutes des choses dont la construction à partir des axiomes n'est en aucun cas évidente. En particulier, des « définitions » comme « l'intersection de deux ensembles est l'ensemble contenant exactement les éléments communs aux deux ensembles » ne sont pas correctes parce qu'elles passent à côté de l'existence et de l'unicité d'un tel ensemble.

1.2 (On saute la grammaire).

Nous n'allons pas non plus formaliser la grammaire des expressions mathématiques¹. Nous supposons que vous êtes capables de lire des expressions comme

$$x \in \mathbb{N} \Rightarrow \{a \geq x\} \text{ est infini.} \quad (1.1)$$

Tout cela pour dire que le Frido ne traitera que de la partie facile de la mathématique.

Définition 1.3.

Deux ensembles A et B sont **disjoints** si leur intersection est vide² ; en d'autres termes, s'il n'existe aucun élément commun à A et B .

1. J'utilise ici des mots que je ne comprends pas, juste pour me donner l'air malin.

2. Remarquez que les mots « intersection » et « vide » sont de ceux que nous avons décidé de ne pas définir.

1.4.

Remarquez par exemple que la première phrase de l'article de Wikipédia sur la construction de $\mathbb{N}$ est « Partant de la théorie des ensembles, on identifie 0 à l'ensemble vide, puis on construit ... ». Il est bien précisé que l'on part d'une théorie des ensembles.

1.5.

La suite de ce chapitre sera essentiellement sans exemples parce qu'avant d'avoir construit les ensembles de nombres, je ne sais pas très bien quels exemples on peut donner de quoi que ce soit.

1.1.2 Injection, surjection, bijection**Définition 1.6.**

Soient deux ensembles E et F . Une application $f: E \rightarrow F$ est

- (1) **surjective** si pour tout $y \in F$, il existe $x \in E$ tel que $y = f(x)$;
- (2) **injective** si pour tout $y \in F$, il existe au plus un $x \in E$ tel que $y = f(x)$;
- (3) **bijection** si elle est à la fois injective et surjective.

La méthode la plus courante pour démontrer qu'une application $f: E \rightarrow F$ est injective est de considérer $x, y \in E$ tels que $f(x) = f(y)$, et de prouver à partir de là que $x = y$. Ou alors de supposer $x \neq y$ et obtenir une contradiction.

La technique de la contradiction est évidemment la plus courante lorsque l'égalité $f(x) = g(x)$ implique une équation faisant intervenir $1/(x - y)$.

Lemme 1.7.

Soient deux ensembles A et B ainsi qu'une application $f: A \rightarrow B$. Nous supposons qu'il existe une application $g: B \rightarrow A$ telle que $f \circ g = \text{Id}_B$ et $g \circ f = \text{Id}_A$.

Alors f est une bijection.

Démonstration. En deux parties.

Injection Supposons que $f(a) = f(b)$. Alors en appliquant g est deux côtés, et en utilisant le fait que $g \circ f = \text{Id}_A$, nous trouvons $a = b$.

Surjection Soit $x \in B$. Posons $a = g(x)$. Alors, en utilisant le fait que $f \circ g = \text{Id}_B$ nous avons

$$f(a) = (f \circ g)(x) = x. \quad (1.2)$$

Donc x est dans l'image de f et f est surjective.

□

1.1.3 Ensemble ordonné**1.8.**

L'**axiome du choix** que nous acceptons peut s'énoncer comme ceci[4] : Étant donné un ensemble X d'ensembles non vides, il existe une fonction définie sur X , appelée fonction de choix, qui à chacun d'entre eux associe un de ses éléments.

Définition 1.9.

Une **relation d'ordre** sur un ensemble E est une relation binaire (notée $\leq$) sur E telle que pour tous $x, y, z \in E$,

réflexivité : $x \leq x$

antisymétrie : $x \leq y$ et $y \leq x$ implique $x = y$

transitivité : $x \leq y$ et $y \leq z$ implique $x \leq z$.

Définition 1.10.

Un ensemble ordonné est **totalelement ordonné** si deux éléments sont toujours comparables : si $x, y \in E$ alors nous avons soit $x \leq y$ soit $y \leq x$. Si les éléments ne sont pas tous comparables, nous disons que l'ordre est **partiel**.

Définition 1.11.

Soit un ensemble ordonné $(E, \leq)$ et une partie A de E . Nous disons que $m \in A$ est un **minimum** de A si pour tout $x \in A$, l'élément m est comparable à x et $m \leq x$.

Un élément $p \in E$ est un **minorant** de A si pour tout $a \in A$, l'élément p et a sont comparables et $p \leq a$.

Les notions de **maximum** et de **majorant** sont définies de façon analogue.

Lorsqu'une partie possède un minimum, ce dernier est nommé le « plus petit élément » de la partie. Attention : il n'en existe pas toujours. D'innombrables exemples pourront être vus lorsque nous aurons construits $\mathbb{Q}$ et $\mathbb{R}$. Typiquement les intervalles du type $]a, b[$.

Définition 1.12.

Un ensemble ordonné est **bien ordonné** si toute partie non vide possède un plus petit élément.

Autrement dit, l'ensemble ordonné E est bien ordonné si pour toute partie non vide A , il existe $x \in A$ tel que $x \leq y$ pour tout $y \in A$.

1.13.

Quelques remarques.

- (1) L'inégalité stricte (définie par : $x < y$ si et seulement si $x \leq y$ et $x \neq y$) n'est pas une relation d'ordre parce qu'elle n'est pas réflexive.
- (2) Nous verrons dans la remarque 1.308 que l'intervalle $[-1, 1]$ dans $\mathbb{R}$ n'est pas bien ordonné.
- (3) Un ensemble bien ordonné est forcément totalement ordonné parce que toutes les parties de la forme $\{x, y\}$ possèdent un minimum. Par conséquent x et y doivent être comparables : $x \leq y$ ou $y \leq x$.

Exemple 1.14.

Si E est un ensemble, l'inclusion est un ordre sur l'ensemble des parties de E , mais pas un ordre total parce que si X, Y sont des parties de E , alors nous n'avons pas automatiquement soit $X \subset Y$ ou $Y \subset X$. $\triangle$

La notion d'ordre permet d'introduire la notion d'intervalle.

Définition 1.15.

Soit un ensemble totalement ordonné $(E, \leq)$. Un **intervalle** de E est une partie I telle que tout élément compris entre deux éléments de I soit dans I . En formule, la partie I de E est un intervalle si

$$\forall a, b \in I, (a \leq x \leq b) \Rightarrow x \in I.$$

1.1.4 Lemme de Zorn

Nous admettons l'axiome du choix[5] qui s'énonce de la façon suivante[6] :

Pour tout ensemble X d'ensembles non vides, il existe une fonction définie sur X , appelée fonction de choix, qui à chaque ensemble A appartenant à X associe un élément de cet ensemble A .

Définition 1.16 (Ensemble inductif[7]).

Un ensemble est **inductif** si tout sous-ensemble totalement ordonné admet un majorant.

Lemme 1.17 (Lemme de Zorn[8]).

Tout ensemble ordonné inductif non vide admet au moins un élément maximal.

1.1.5 Complémentaire**Définition 1.18.**

Soit E , un ensemble et A , une partie de E (c'est-à-dire un sous-ensemble de E). Le **complément**

taire de l'ensemble A , dans E , noté $\complement A$ est l'ensemble des éléments de E qui ne font pas partie de A :

$$\complement A = E \setminus A = \{x \in E \text{ tel que } x \notin A\}. \quad (1.3)$$

Nous allons aussi régulièrement noter le complémentaire de A par A^c .

Lemme 1.19 (Quelque relations ensemblistes).

Soient $A, B, C \subset X$. Nous avons

- (1) $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$.
- (2) $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$.
- (3) $A \cap (B \setminus C) = (A \cap B) \setminus C$.

Lemme 1.20.

Quelques propriétés à propos des complémentaires. Si E est un ensemble et si A et B sont des sous-ensembles de E , nous avons

- (1) $\complement \complement A = A$, en d'autres termes, $E \setminus (E \setminus A) = A$,
- (2) $A \setminus B = A \cap \complement B$.
- (3) $(A \setminus B)^c = A^c \cup B$.
- (4) $A^c \setminus B^c = B \setminus A$.

Démonstration. Plusieurs points.

Pour (2)

Pour (3) Il faut le faire en deux inclusions.

$(A \setminus B)^c \subset A^c \cup B$ Supposons que $x \in (A \setminus B)^c$. Si $x \in A^c$ on est bon. Sinon, si $x \in A$ alors nous devons montrer que $x \in B$. Si x n'est pas dans B , alors $x \in A \setminus B$, et n'est donc pas dans $(A \setminus B)^c$. Donc oui, $x \in B$.

$A^c \cup B \subset (A \setminus B)^c$ Supposons d'abord que $x \in A^c$. Vu que $A \setminus B \subset A$, si $x \in A^c$, alors $x \in (A \setminus B)^c$.

Si $x \in B$, alors x n'est pas dans $A \setminus B$ et donc x est dans $(A \setminus B)^c$.

Pour (4) Pour cette égalité, nous faisons les cas suivant que x est dans A ou B ou non. Bref, nous écrivons la table de vérité :

A	1	1	0	0
B	1	0	1	0
$A^c \setminus B^c$	0	0	1	0
$B \setminus A$	0	0	1	0

(1.4)

Les deux dernières lignes étant égales, nous avons l'égalité d'ensembles annoncée.

□

Définition 1.21 (différence symétrique).

Si A et B sont des ensembles, l'ensemble $A \Delta B$ est la **différence symétrique** d'ensembles :

$$A \Delta B = (A \cup B) \setminus (A \cap B). \quad (1.5)$$

C'est l'ensemble des éléments étant soit dans A soit dans B mais pas dans les deux, ni dans aucun des deux. La table de vérité de $A \Delta B$ est intéressante :

A	1	1	0	0
B	1	0	1	0
$A \Delta B$	0	1	1	0

(1.6)

La deuxième colonne signifie que si $x \in A$ et $x \in B^c$, alors $x \in A \Delta B$.

Lemme 1.22 ([9]).

Si A et B sont des parties d'un ensemble, nous avons

- (1) $A^c \Delta B^c = A \Delta B$.
- (2) $(A \Delta B) \Delta B = A$.
- (3) $(A \Delta B)^c = (A^c \cap B^c) \cup (A \cap B)$.
- (4) Associativité : $A \Delta (B \Delta C) = (A \Delta B) \Delta C$.

Démonstration. Nous rappelons l'égalité $X^c \setminus Y^c = Y \setminus X$ du lemme 1.20(4). De là nous prouvons.

Pour (1) De là nous avons la première assertion :

$$A^c \Delta B^c = (A^c \cup B^c) \setminus (A^c \cap B^c) = (A \cap B)^c \setminus (A \cup B)^c = (A \cup B) \setminus (A \cap B) = A \Delta B. \quad (1.7)$$

Pour (2) Pour la seconde assertion, il faut remarquer que $(A \Delta B) \cup B = A \cup B$ et que $(A \Delta B) \cap B = B \setminus A$, donc

$$(A \Delta B) \Delta B = (A \cup B) \setminus (B \setminus A) = A. \quad (1.8)$$

Pour (3) Il s'agit d'utiliser le lemme 1.20(3) :

$$(A \Delta B)^c = \left((A \cup B) \setminus (A \cap B) \right)^c \quad (1.9a)$$

$$= (A \cup B)^c \cup (A \cap B) \quad (1.9b)$$

$$= (A^c \cap B^c) \cup (A \cap B). \quad (1.9c)$$

Pour l'associativité (4) Nous écrivons les tables de vérités selon que x est dans A , B , C ou non.

D'abord

A	1	1	1	1	0	0	0	0
B	1	1	0	0	1	1	0	0
C	1	0	1	0	1	0	1	0
$B \Delta C$	0	1	1	0	0	1	1	0
$A \Delta (B \Delta C)$	1	0	0	1	0	1	1	0

(1.10)

La quatrième ligne s'écrit sur le modèle de (1.6) en regardant les deuxièmes et troisièmes lignes. La dernière ligne se fait avec la première et la quatrième.

L'autre table de vérité se fait de la même manière :

A	1	1	1	1	0	0	0	0
B	1	1	0	0	1	1	0	0
C	1	0	1	0	1	0	1	0
$A \Delta B$	0	0	1	1	1	1	0	0
$(A \Delta B) \Delta C$	1	0	0	1	0	1	1	0

(1.11)

Vu que les lignes pour $A \Delta (B \Delta C)$ et pour $(A \Delta B) \Delta C$ sont identiques, nous avons égalité.

□

1.1.6 Relations d'équivalence

Définition 1.23.

Si E est un ensemble, une **relation d'équivalence** sur E est une relation $\sim$ qui est à la fois **réflexive** $x \sim x$ pour tout $x \in E$,

symétrique $x \sim y$ si et seulement si $y \sim x$;

transitive si $x \sim y$ et $y \sim z$, alors $x \sim z$.

Définition 1.24.

Si E est un ensemble et si $\sim$ est une relation d'équivalence sur E , alors nous notons $E / \sim$ l'**ensemble quotient**, c'est-à-dire l'ensemble des classes d'équivalence dans E . Un élément de $E / \sim$ est de la forme

$$[a] = \{x \in E \text{ tel que } x \sim a\}. \quad (1.12)$$

Lemme 1.25.

Soit un ensemble E et une relation d'équivalence $\sim$. Pour $a, b \in E$, nous avons $[a] = [b]$ si et seulement si $a \sim b$.

Démonstration. En deux parties.

$\Rightarrow$ Nous supposons que $[a] = [b]$. Vu que $a \sim a$, nous avons $a \in [a] = [b]$. Mais $a \in [b]$ signifie $a \sim b$, ce qu'il fallait.

$\Leftarrow$ Nous supposons que $a \sim b$, et nous démontrons que $[a] \subset [b]$ (pour l'inclusion inverse, vous devriez vous en sortir par tout seul). Si $x \in [a]$, alors $x \sim a$. Mais $a \sim b$. Donc $x \sim a \sim b$, ce qui implique $x \sim b$ par transitivité. Or dire $x \sim b$ implique $x \in [b]$.

□

Exemple 1.26.

Sur l'ensemble de tous les polygones du plan, la relation « a le même nombre de côtés » est une relation d'équivalence. Plus précisément, si P et Q sont deux polygones, nous disons que $P \sim Q$ si et seulement si P et Q ont le même nombre de côtés. Cela est une relation d'équivalence :

- un polygone P a toujours le même nombre de côtés que lui-même : $P \sim P$;
- si P a le même nombre de côtés que Q ($P \sim Q$), alors Q a le même nombre de côtés que P ($Q \sim P$) ;
- si P a le même nombre de côtés que Q ($P \sim Q$) et que Q a le même nombre de côtés que R ($Q \sim R$), alors P a le même nombre de côtés que R ($P \sim R$).

△

Exemple 1.27.

Soit f une application entre deux ensembles E et F . Nous définissons une relation d'équivalence sur E par

$$x \sim y \Leftrightarrow f(x) = f(y). \quad (1.13)$$

Nous notons par $\pi: E \rightarrow E/\sim$ la projection canonique. L'application

$$\begin{aligned} g: E/\sim &\rightarrow F \\ [x] &\mapsto f(x) \end{aligned} \quad (1.14)$$

est bien définie et injective. Elle n'est pas surjective tant que f ne l'est pas. La **décomposition canonique** de f est

$$f = g \circ \pi. \quad (1.15)$$

△

1.2 Quelques structures algébriques

Nous collectons ici les définitions des principales structures algébriques.

Définition 1.28 (Groupe).

Un **groupe** est un ensemble G muni d'une opération interne $\cdot: G \times G \rightarrow G$ telle que

- (1) pour tous $g, h, k \in G$, $g \cdot (h \cdot k) = (g \cdot h) \cdot k$,
- (2) il existe un élément $e \in G$ tel que $e \cdot g = g \cdot e = g$ pour tout $g \in G$,
- (3) pour tout $g \in G$, il existe un élément $h \in G$ tel que $g \cdot h = h \cdot g = e$.

Notons que nous avons écrit $g \cdot h$ et non $\cdot(g, h)$ comme une notation purement fonctionnelle nous l'aurait suggéré. Dans les exemples concrets, selon les cas, le loi de groupe appliquée à g et h sera notée tantôt $g + h$, tantôt $g \cdot h$ ou, le plus souvent pour un groupe générique, simplement gh .

Définition 1.29 (morphisme, automorphisme).

Soient deux groupes G et H . Un **morphisme** entre G et H est une application $\alpha: G \rightarrow H$ telle que pour tout $g, h \in G$ nous ayons $\alpha(gh) = \alpha(g)\alpha(h)$.

Comme d'habitude, un isomorphisme est un morphisme bijectif. Un **automorphisme** de G est un isomorphisme de G vers G lui-même.

Définition 1.30 (Anneau[10]).

Un **anneau**³ est un triplet $(A, +, \cdot)$ avec les conditions

- (1) $(A, +)$ est un groupe⁴ abélien. Nous notons 0 le neutre.
- (2) La multiplication est associative et nous notons 1 le neutre.
- (3) La multiplication est distributive par rapport à l'addition.

L'anneau $(A, +, \cdot)$ est **commutatif** si pour tout $a, b \in A$ nous avons $a \cdot b = b \cdot a$.

Définition 1.31 (Morphisme d'anneaux[11]).

Si $(A, +, \cdot)$ et $(B, +, \cdot)$ sont des anneaux, un **morphisme d'anneaux** est une application $f: A \rightarrow B$ telle que

- (1) $f(a + b) = f(a) + f(b)$
- (2) $f(a \cdot b) = f(a) \cdot f(b)$
- (3) $f(1) = 1$.

Étant bien entendu que les significations de 1 , $+$ et $\cdot$ sont différentes à gauche et à droite.

1.3 Les naturels

Définition 1.32 ([12]).

Un **triplet naturel** est une triple $(\mathcal{N}, o, s)$ où $\mathcal{N}$ est un ensemble, o est un élément de $\mathcal{N}$ et s est une application $s: \mathcal{N} \rightarrow \mathcal{N}$ satisfaisant les propriétés suivantes :

- (1) s est injective,
- (2) $s(\mathcal{N}) = \mathcal{N} \setminus \{o\}$
- (3) Si $A \subset \mathcal{N}$ est tel que $o \in A$ et $s(A) \subset A$, alors $A = \mathcal{N}$.

Le théorème suivant est typiquement de ceux qui vont demander de gratter la théorie axiomatique des ensembles avec une certaine précision⁵.

Théorème 1.33.

Il existe des triples naturels.

1.34 (Définition de $\mathbb{N}$).

Pour la suite, nous considérons un triple naturel $(\mathcal{N}, o, s)$ et nous notons $\mathbb{N} = \mathcal{N}$ ainsi que $0 = o$. Donc la nature de tous les objets que nous allons considérer à partir de maintenant dépend du choix de triple naturel que nous faisons à présent. Le théorème 1.66 nous assurera que peu de choses devraient réellement dépendre de ce choix.

Nous notons 0 l'élément o et 1 l'élément $s(0)$. C'est tout ce dont nous avons besoin dans l'immédiat.

1.3.1 Applications définies par récurrence

Proposition 1.35 (Récurrence[12]).

Soit un triplet naturel $(\mathcal{N}, o, s)$ et une application $P: \mathcal{N} \rightarrow \{0, 1\}$ vérifiant⁶

3. Nous faisons le choix qu'un anneau admet toujours un neutre pour la multiplication. Certains ouvrages parlent dans ce cas d'anneau unitaire.

4. Groupe, définition 1.28.

5. Ou alors il y a quelque chose qui m'échappe. Si vous connaissez une construction « simple », faites-me le savoir.

6. Les plus pointilleuses diront que 1 n'est pas encore défini. Bon j'avoue. Ce qui est important est que P prenne ses valeurs dans un ensemble contenant deux éléments distincts. Si maintenant vous râlez parce que « deux » est

$$(1) P(0) = 1,$$

$$(2) \text{ pour tout } a \in \mathcal{N}, \text{ si } P(a) = 1, \text{ alors } P(s(a)) = 1.$$

Alors $P(x) = 1$ pour tout $x \in \mathcal{N}$.

Démonstration. Nous posons

$$A = \{x \in \mathcal{N} \text{ tel que } P(x) = 1\}. \quad (1.16)$$

Cet ensemble vérifie la propriété 1.32(3). Donc $A = \mathcal{N}$. $\square$

Théorème 1.36 ([13, 14]).

Soient E un ensemble, g une application de E dans E et b un élément de E . Alors il existe une unique application $f: \mathbb{N} \rightarrow E$ telle que :

$$(1) f(0) = b$$

$$(2) f(s(n)) = g(f(n)) \text{ pour tout } n \in \mathbb{N} \setminus \{0\}.$$

Démonstration. Nous commençons par l'unicité. Soient f_1 et f_2 deux telles applications. Nous posons

$$A = \{n \in \mathbb{N} \text{ tel que } f_1(n) = f_2(n)\}. \quad (1.17)$$

Nous avons $0 \in A$ parce que $f_1(0) = f_2(0) = b$.

Supposons que $f_1(k) = f_2(k)$. Alors nous avons

$$f_1(s(k)) = g(f_1(k)) = g(f_2(k)) = f_2(s(k)). \quad (1.18)$$

Nous en déduisons que $s(k) \in A$. Autrement dit $s(A) \subset A$. La définition 1.32(3) nous indique alors que $A = \mathbb{N}$, c'est à dire que $f_1 = f_2$.

Nous faisons maintenant l'existence en plusieurs étapes.

L'ensemble assez grand Nous considérons l'ensemble $\mathcal{A}$ des parties $A \subset \mathbb{N} \times E$ telles que

$$(1) (0, b) \in A$$

$$(2) (n, x) \in A \Rightarrow (s(n), g(x)) \in A.$$

L'ensemble $\mathcal{A}$ est non vide parce que $\mathbb{N} \times E \in \mathcal{A}$.

Le plus petit Nous posons

$$G = \bigcap_{A \in \mathcal{A}} A, \quad (1.19)$$

et nous prouvons que $G \in \mathcal{A}$. D'abord $(0, b) \in G$ parce que cet élément est dans chacun des $A \in \mathcal{A}$. Ensuite si $(n, x) \in G$, alors pour tout $A \in \mathcal{A}$ nous avons $(n, x) \in A$ et donc $(s(n), g(x)) \in A$. Par conséquent $(s(n), g(x)) \in \bigcup_{A \in \mathcal{A}} A = G$.

Pour $n \in \mathbb{N}$ nous posons

$$G_n = \{x \in E \text{ tel que } (n, x) \in G\}. \quad (1.20)$$

Nous avons en particulier que $b \in G_0$ parce que $(0, b) \in G$.

G contient un (n, x) pour tout n Nous prouvons que pour tout $n \in \mathbb{N}$, il existe $x \in E$ tel que $(n, x) \in G$. Nous faisons ça avec la proposition 1.35 en posant

$$P: \mathbb{N} \rightarrow \{0, 1\}$$

$$n \mapsto \begin{cases} 1 & \text{si } G_n \neq \emptyset \\ 0 & \text{sinon.} \end{cases} \quad (1.21)$$

Vu que $(0, b) \in G$ nous avons $P(0) = 1$. Supposons que $P(k) = 1$ et montrons que $P(s(k)) = 1$. Vu que $P(k) = 1$, il existe $x \in E$ tel que $(k, x) \in G$. De ce fait, $(s(k), g(x)) \in G$, ce qui fait que $G_{s(k)} \neq \emptyset$ et $P(s(k)) = 1$.

encore moins défini, prenez un ensemble quelconque A et dites que P prend ses valeurs dans $\{A, \mathcal{P}(A)\}$. Mais êtes-vous bien certaine que $\mathcal{P}(A) \neq A$?

G_n est un singleton Nous avons vu que G_n n'est jamais vide. Nous allons montrer que G_n est un singleton pour tout n . Pour cela nous posons

$$P: \mathbb{N} \rightarrow \{0, 1\}$$

$$n \mapsto \begin{cases} 1 & \text{si } G_n \text{ est un singleton} \\ 0 & \text{sinon.} \end{cases} \quad (1.22)$$

Nous prouvons par récurrence que $P(n) = 1$ pour tout n .

$P(0) = 1$ Nous commençons par prouver que $P(0) = 1$. Nous savons que $(0, b) \in G_0$. Supposons $a \neq b$ tel que $(0, a) \in G_0$. Alors en posant $G' = G_0 \setminus \{(0, a)\}$ nous avons $G' \in \mathcal{A}$.

En effet $(0, b) \in G'$ parce que $(0, b) \in G$ et $(0, b) \neq (0, a)$. De plus si $(n, x) \in G'$, alors $(s(n), g(x)) \in G$. Mais comme $s(n) \neq 0$ nous avons $(s(n), g(x)) \neq (0, a)$ et donc $(s(n), g(x)) \in G'$.

L'ensemble G' serait un élément de $\mathcal{A}$ strictement inclus à G . Impossible. Donc G_0 est un singleton.

Récurrence Supposons que $P(k) = 1$, c'est à dire que G_k est un singleton. Soit e l'unique élément de $G_k : (k, e) \in G$. Nous avons alors aussi que $(s(k), g(e)) \in G$. Nous devons prouver que si $y \in G_{s(k)}$, alors $y = g(e)$.

Supposons donc $y \neq g(e)$ soit dans $G_{s(k)}$. Nous posons

$$G' = G \setminus \{(s(k), y)\}. \quad (1.23)$$

Nous prouvons que $G' \in \mathcal{A}$. D'abord $(0, b) \in G'$ parce que $s(k) \neq 0$. Soit ensuite $(m, z) \in G'$. Si $m = k$, alors $z = e$ (parce que par hypothèse G_k est un singleton) et nous savons que $(s(m), g(e)) \in G'$. Si par contre $m \neq k$, vu que s est injective, nous avons aussi $s(m) \neq s(k)$. Donc $(s(m), g(z)) \neq (s(k), y)$ et $(s(m), g(z)) \in G'$. Donc $G' \in \mathcal{A}$ et est strictement plus petit que G . Contradiction.

Nous concluons que $G_{s(k)}$ est un singleton, c'est à dire que $P(s(k)) = 1$.

Conclusion Nous avons prouvé que G_n est un singleton pour tout n .

Et enfin Nous définissons $f(n)$ comme étant l'unique élément de G_n . Vu que $(0, b) \in G$ nous avons $G_0 = \{b\}$ et donc $g(0) = b$.

Par définition de f , nous avons $(n, f(n)) \in G$. Parce que $G \in \mathcal{A}$ nous avons alors

$$(s(n), g(f(n))) \in G. \quad (1.24)$$

Autrement dit, $G_{s(n)} = g(f(n))$. Cela montre que

$$f(s(n)) = g(f(n)), \quad (1.25)$$

et donc que f vérifie les propriétés demandées.

□

Corolaire 1.37 ([13]).

Soient deux ensembles X, Y , une application $\alpha: X \rightarrow Y$ et une application $\beta: Y \rightarrow Y$. Alors il existe une unique application $H: X \times \mathbb{N} \rightarrow Y$ telle que

- (1) $H(x, 0) = \alpha(x)$ pour tout élément $x \in X$;
- (2) $H(x, n + 1) = \beta(H(x, n))$ pour tout élément $x \in X$ et pour tout $n \in \mathbb{N}$.

Démonstration. Nous posons $E = \text{Fun}(X, Y)$, $b = \alpha \in E$ et

$$g: E \rightarrow E$$

$$s \mapsto \beta \circ s. \quad (1.26)$$

Le théorème 1.36 donne l'existence d'une application $f: \mathbb{N} \rightarrow E$ telle que

- (1) $f(0) = b$
- (2) $f(n+1) = g(f(n))$.

Nous définissons alors

$$\begin{aligned} H: X \times \mathbb{N} &\rightarrow Y \\ (x, n) &\mapsto f(n)x, \end{aligned} \tag{1.27}$$

et nous vérifions qu'elle satisfait aux exigences.

- (1) D'abord nous avons

$$H(x, 0) = f(0)x = b(x) = \alpha(x). \tag{1.28}$$

- (2) Ensuite,

$$H(x, n+1) = f(n+1)x = g(f(n))x = (h \circ f(n))x = h(f(n)x) = h(H(x, n)). \tag{1.29}$$

Et voilà. □

1.3.2 Addition sur les naturels

Définition 1.38 (élément régulier[15]).

Soit un ensemble E muni d'une opération $*$: $E \times E \rightarrow E$. Un élément $s \in E$ est **régulier à gauche** si pour tout $x, y \in E$ nous avons

$$s * x = s * y \Rightarrow x = y. \tag{1.30}$$

L'élément s est **régulier à droite** si pour tout $x, y \in E$ nous avons

$$x * s = y * s \Rightarrow x = y. \tag{1.31}$$

Il est **régulier** si il est régulier à gauche et à droite.

Proposition-Définition 1.39 ([12, 1]).

Il existe une unique fonction $f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ vérifiant

- (1) $f(a, 0) = a$ pour tout $a \in \mathbb{N}$
- (2) $f(a, s(b)) = s(f(a, b))$ pour tout $a, b \in \mathbb{N}$.

Pour $a, b \in \mathbb{N}$ nous notons $f(a, b) = a + b$.

Lemme 1.40 ([12]).

Pour tout $a \in \mathbb{N}$ nous avons $s(a) = a + 1$.

Démonstration. Nous avons :

$$s(a) = s(a + 0) \tag{1.32a}$$

$$= a + s(0) \tag{1.32b}$$

$$= a + 1. \tag{1.32c}$$

Justifications.

- (1) Pour (1.32a) c'est dans la définition 1.39(1) de la somme.
- (2) Pour (1.32b), c'est dans la définition 1.39(2) de la somme.
- (3) Pour (1.32c). Le symbole « 1 » désigne l'élément $s(0)$ dans $\mathbb{N}$.

□

Proposition 1.41 ([12]).

En ce qui concerne la somme dans $\mathbb{N}$.

- (1) La somme est associative et commutative.
- (2) L'élément 0 est neutre.

(3) Tous les éléments de $\mathbb{N}$ sont réguliers⁷ par rapport à l'addition.

Démonstration. En plusieurs parties.

Associative Nous devons prouver que $(a + b) + c = a + (b + c)$ pour tout $a, b, c \in \mathbb{N}$. Pour ce faire, nous fixons $a, b \in \mathbb{N}$ et nous prouvons l'égalité demandée par récurrence sur c .

Pour $c = 0$, nous avons $(a + b) + c = a + b$ et $a + (b + c) = a + b$. Donc nous sommes d'accord⁸.

Nous vérifions avec $s(c)$:

$$(a + b) + s(c) = s((a + b) + c) \quad (1.33a)$$

$$= s(a + (b + c)) \quad (1.33b)$$

$$= a + s(b + c) \quad (1.33c)$$

$$= a + (b + s(c)). \quad (1.33d)$$

Justifications.

— Pour (1.33b). C'est l'hypothèse de récurrence. À ce stade, je vous conseille d'être capable de rédiger complètement la récurrence et l'appel au théorème 1.36.

Neutre La définition de l'addition contient déjà $a + 0 = a$. Nous prouvons par récurrence que $0 + a = a$ pour tout $a \in \mathbb{N}$.

Pour $a = 0$, l'égalité demandé est correcte : $0 + 0 = 0$ parce que pour tout x dans $\mathbb{N}$, $0 + x = x$.

Pour $s(a)$ nous avons

$$0 + s(a) = s(0 + a) = s(a). \quad (1.34)$$

La dernière égalité est l'hypothèse de récurrence.

Nous posons

$$A = \{a \in \mathbb{N} \text{ tel que } 0 + a = a\}. \quad (1.35)$$

Nous avons prouvé que $0 \in A$ et que $s(A) \subset A$. Le théorème 1.36 nous assure alors que $A = \mathbb{N}$.

Commutativité Nous fixons $a \in \mathbb{N}$ et nous prouvons par récurrence sur b que $a + b = b + a$ pour tout $b \in \mathbb{N}$. Cela va être décomposé en plusieurs étapes.

$a + 0 = 0 + a$ Pour $b = 0$ c'est bon parce que $b + 0 = 0 + b = b$ parce que 0 est neutre.

$a + 1 = 1 + a$ Nous démontrons par récurrence sur a que $a + 1 = 1 + a$. Avec $a = 0$ c'est déjà fait. Pour les autres,

$$s(a) + 1 = (a + 1) + 1 \quad \text{lemme 1.40} \quad (1.36a)$$

$$= (1 + a) + 1 \quad \text{hypothèse récurrence} \quad (1.36b)$$

$$= 1 + (a + 1) \quad \text{associativité} \quad (1.36c)$$

$$= 1 + s(a). \quad (1.36d)$$

$a + b = b + a$ Nous y voici. Nous fixons a et nous prouvons par récurrence que $a + b = b + a$. Pour $b = 0$ c'est déjà fait. Pour les autres,

$$a + s(b) = a + (b + 1) \quad (1.37a)$$

$$= (a + b) + 1 \quad (1.37b)$$

$$= (b + a) + 1 \quad \text{hypothèse récurrence} \quad (1.37c)$$

$$= b + (a + 1) \quad (1.37d)$$

$$= b + (1 + a) \quad \text{commutativité avec 1} \quad (1.37e)$$

$$= (b + 1) + a \quad \text{associativité} \quad (1.37f)$$

$$= s(b) + a. \quad (1.37g)$$

Récurrence terminée.

7. Élément régulier pour une opération, définition 1.38.

8. Notez que nous n'avons pas utilisé le fait que 0 était neutre des deux côtés – chose que nous n'avons pas encore démontré. Nous avons seulement utilisé $a + 0 = a$, qui est dans la définition de la somme.

Régularité Nous devons prouver que, pour tout $a, x, y \in \mathbb{N}$, si $a + x = b + x$ alors $x = y$. Nous allons la faire par récurrence en posant

$$A = \{a \in \mathbb{N} \text{ tel que } \forall x, y \in \mathbb{N}, a + x = a + y \Rightarrow x = y\}. \quad (1.38)$$

Vu que $0 + x = x$ et $0 + y = y$, nous avons $0 \in A$. Supposons à présent que $a \in A$ et montrons que $s(a) \in A$. Soient $x, y \in \mathbb{N}$ tels que $a + x = a + y$. Nous avons :

$$s(a) + x = s(a) + y \quad (1.39a)$$

$$\Rightarrow s(a + x) = s(a + y) \quad (1.39b)$$

$$\Rightarrow a + x = a + y \quad (1.39c)$$

$$\Rightarrow x = y \quad (1.39d)$$

Justifications.

- Pour (1.39b). En utilisant la définition de l'addition et la commutativité, nous avons $s(a) + x = s(a + x)$.
- Pour (1.39c). Parce que s est injective ; c'est dans la définition 1.32 d'un triplet naturel.
- Pour (1.39d). Parce que $a \in A$.

Nous avons prouvé que $s(A) \subset A$, et donc que $A = \mathbb{N}$.

□

Lemme 1.42.

Nous avons $0 \neq 1$.

Démonstration. Par définition $1 = s(0)$. Vu que s est à valeurs dans $\mathbb{N} \setminus \{0\}$, nous ne pouvons pas avoir $s(0) = 0$. □

Lemme 1.43 ([1]).

Si $a + b = 0$, alors $a = b = 0$.

Démonstration. Soient $a, b \in \mathbb{N}$ tels que $a + b = 0$, et supposons que $b \neq 0$. Par la définition 1.32(2), nous avons $b = s(c)$ pour un certain $c \in \mathbb{N}$.

Dans ce cas nous avons $a + b = a + s(c) = s(a + c) \neq 0$ parce que l'image de s ne contient pas 0. Vu qu'en réalité $a + b = 0$, nous avons une contradiction et nous déduisons que $b = 0$.

Maintenant que nous savons que $b = 0$, nous restons avec $0 = a + b = a + 0 = a$. □

1.3.3 Ordre sur les naturels

Définition 1.44 ([12]).

Pour $a, b \in \mathbb{N}$, nous notons $a \leq b$ si il existe $x \in \mathbb{N}$ tel que $a + x = b$.

Nous notons également $a < b$ si $a \leq b$ et $a \neq b$.

Lemme 1.45.

Nous avons $a \leq s(a)$ pour tout $a \in \mathbb{N}$.

Démonstration. Cela est une conséquence du lemme 1.40 : $s(a) = a + 1$. □

Proposition 1.46.

La relation $\leq$ est une relation d'ordre compatible avec l'addition.

Démonstration. Plusieurs choses à vérifier.

Réflexive Nous avons $a \leq a$ parce que $a + 0 = a$.

Antisymétrique Soient $a, b \in \mathbb{N}$ tels que $a \leq b$ et $b \leq a$. Il existe $x, y \in \mathbb{N}$ tels que

$$b = a + x \quad (1.40a)$$

$$a = b + y. \quad (1.40b)$$

En substituant la seconde dans la première, $b = (b + y) + x$ que nous récrivons, en utilisant l'associativité⁹,

$$0 + b = b + (x + y). \quad (1.41)$$

En utilisant la régularité, $0 = x + y$ et donc $x = y = 0$ par le lemme 1.43. Cela donne alors $a = b$.

Transitive Si $a \leq b$ et $b \leq c$, nous avons $n, p \in \mathbb{N}$ tels que $b = a + n$ et $x + b + p$. Donc

$$c = (a + n) + p = a + (n + p), \quad (1.42)$$

ce qui signifie que $a \leq c$. Notez l'utilisation de l'associativité de la somme, démontrée en la proposition 1.41(1).

Compatibilité Soient $a, b, n \in \mathbb{N}$ tels que $a \leq b$. Nous devons montrer que $a + n \leq b + n$. Vu que $a \leq b$, il existe $x \in \mathbb{N}$ tel que $b = a + x$. Du coup,

$$b + n = a + x + n = (a + n) + x, \quad (1.43)$$

qui signifie bien ans $a + n \leq b + n$.

□

Lemme 1.47.

À propos d'ordre et de stricte inégalité.

(1) Si $x \leq a$ et $b \neq 0$, alors $x < a + b$.

(2) Si $x \leq a$, alors $x < s(a)$.

(3) Si $x < a$, alors $s(x) \leq a$.

Démonstration. En plusieurs parties.

Pour (1) Si $x \leq a$, il existe $d \in \mathbb{N}$ tel que $x + d = a$. Nous avons alors aussi

$$x + d + b = a + b, \quad (1.44)$$

ce qui signifie que $x \leq a + b$. Mais si x était égal à $a + b$, nous aurions $d + b = 0$, ce qui impliquerait¹⁰ $d = b = 0$, alors que l'hypothèse stipule que $b \neq 0$. Donc $x < a + b$.

Pour (2) Il s'agit seulement d'utiliser la point (1) avec $b = 1$ et le fait que $s(a) = a + 1$ par le lemme 1.40.

Pour (3) Par hypothèse, il existe $b \neq 0$ tel que $x + b = a$. Vu que $b \neq 0$, il existe $c \in \mathbb{N}$ tel que $b = s(c)$ et donc tel que

$$x + s(c) = a. \quad (1.45)$$

En utilisant le fait que $s(c) = c + 1$ ainsi que l'associativité et la commutativité de l'addition (proposition 1.41(1)) nous avons

$$a = x + s(c) = s(x) + c, \quad (1.46)$$

ce qui prouve que $s(x) \leq a$.

□

Lemme 1.48.

L'élément 0 est l'unique plus petit élément de $\mathbb{N}$.

9. Proposition 1.41(1).

10. Par le lemme 1.43.

Démonstration. Vu que 0 est neutre pour l'addition¹¹, nous avons $a + 0 = a$ pour tout $a \in \mathbb{N}$ et donc $0 \leq a$ pour tout a . Cela est pour dire que 0 est plus petit que tout élément de $\mathbb{N}$.

En ce qui concerne l'unicité, soit $z \in \mathbb{N}$ tel que $z \leq a$ pour tout $a \in \mathbb{N}$. Si $z \neq 0$, il existe $x \in \mathbb{N}$ tel que $z = s(x)$. Nous avons donc $z \geq x$ en même temps que $x \leq z$. Cela implique $z = x$ (parce qu'une relation d'ordre est symétrique) et donc $z = z + 1$. En utilisant la régularité de z pour l'addition nous en déduisons que $0 = 1$, ce qui est impossible par le lemme 1.42. $\square$

Lemme 1.49.

Si $a \leq b$ et $b \leq a$, alors $a = b$.

Démonstration. L'inégalité $a \leq b$ dit qu'il existe $x \in \mathbb{N}$ tel que $a + x = b$. En mettant cela dans l'inégalité $b \leq a$ nous trouvons $a + x \leq a$ qui donne, via la proposition 1.46 : $x \leq 0$. Nous en déduisons que $x = 0$ parce que zéro est l'unique minimum de $\mathbb{N}$ par le lemme 1.48. $\square$

Proposition 1.50.

Le couple $(\mathbb{N}, \leq)$ est totalement ordonné¹².

Démonstration. Soit $a \in \mathbb{N}$. Nous devons prouver que pour tout $x \in \mathbb{N}$ nous avons $x \leq a$ ou $a \leq x$ (non exclusifs). Nous posons

$$A = \{x \in \mathbb{N} \text{ tel que } x \leq a\} \quad (1.47a)$$

$$B = \{x \in \mathbb{N} \text{ tel que } a \leq x\}, \quad (1.47b)$$

et nous prouvons que $A \cup B = \mathbb{N}$ en montrant que $0 \in A \cup B$ et que $s(A \cup B) \subset A \cup B$.

Nous avons $0 \in A \subset A \cup B$ par le lemme 1.48.

Pour étudier $s(A \cup B)$, nous considérons $x \in A \cup B$ et nous subdivisons en deux cas suivant que $x \in A$ ou $x \in B$.

Si $x \in B$ Si $x \in B$, alors $a \leq x \leq s(x)$ parce que $x \leq s(x)$ par le lemme 1.45. Donc $s(x) \in B \subset A \cup B$.

Si $x \in A$ Si $x \in A$, il y a deux possibilités : $x = a$ et $x \neq a$. Si $x = a$, alors $a \leq s(x)$ et donc $s(x) \in A \subset A \cup B$.

Si $x \neq a$, alors le lemme 1.47(3) nous indique que $s(x) \leq a$ et donc $s(x) \in A \subset A \cup B$.

Nous avons donc prouvé que $s(A \cup B) \subset A \cup B$, et donc que $A \cup B = \mathbb{N}$. $\square$

Proposition 1.51 ([12, 1]).

L'ensemble ordonné $(\mathbb{N}, \leq)$ vérifie les choses suivantes.

- (1) L'élément 0 est l'unique minimum de $\mathbb{N}$.
- (2) Toute partie non vide a un unique plus petit élément.
- (3) L'ensemble $\mathbb{N}$ n'a pas de plus grand élément.
- (4) Toute partie non vide majoré a un unique plus grand élément.

Démonstration. Point par point.

Pour (1) C'est le lemme 1.48.

Pour (2) Soit une partie A non vide dans $\mathbb{N}$. Si $0 \in A$, nous avons fini.

L'ensemble B Nous supposons donc que A ne contient pas zéro et nous définissons

$$B = \{n \in \mathbb{N} \setminus A \text{ tel que } n \leq a \forall a \in A\}. \quad (1.48)$$

Un élément particulier dans B L'ensemble B vérifie :

- $0 \in B$
- $B \neq \mathbb{N}$ parce que A est non vide.

11. Proposition 1.41(2).

12. Définition 1.10.

La contraposée de la condition (3) de la définition 1.32 de triplet naturel implique que $s(B) \not\subset B$. Autrement dit, il existe $b \in B$ tel que $s(b) \notin B$.

Deux fonctions sur A Vu que $b \in B$, nous avons une application $c: A \rightarrow \mathbb{N}$ telle que $b + c(a) = a$. Nous avons $c(a) \neq 0$ parce que $c(a) = 0$ signifierait $b = a$, ce qui est impossible parce que $a \in A$ et $b \in B$.

Vu que pour tout $a \in A$, l'élément $c(a)$ est non nul, il existe une fonction $d: A \rightarrow \mathbb{N}$ telle que $c(a) = d(a) + 1$.

$s(b) \in A$ Supposons que $s(b) \notin A$. Alors il existe $a \in A$ tel que $s(b) \leq a$ est faux. Vu que l'ordre est total (proposition 1.50), nous avons

$$a \leq s(b). \quad (1.49)$$

Vu que $b \in B$ nous avons aussi

$$b \leq a. \quad (1.50)$$

Et enfin nous avons

$$b \neq a \quad (1.51)$$

parce que $a \in A$ et $b \in B$.

Les conditions (1.50) et (1.51) se résument en $b < a$. Le lemme 1.47(3) nous indique alors que $s(b) \leq a$. Cela mis à côté de (1.49) conclu que $a = s(b)$, et donc que $s(b)$ est dans A . Contradiction. Nous en concluons que $s(b) \in A$.

$s(b)$ est un minimum de A En utilisant la commutativité et l'associativité de la somme nous avons, pour tout $a \in A$:

$$a = b + c(a) = b + (d(a) + 1) = (b + 1) + d(a) = s(b) + d(a). \quad (1.52)$$

Donc $s(b) \leq a$ pour tout $a \in A$. Mais comme $s(b) \in A$, l'élément $s(b)$ est bien un minimum de A .

Unicité Si a et a' sont des minimums de A , alors $a \leq a'$ et $a' \leq a$. Nous en déduisons que $a = a'$.

Pour (3) Si $M \in \mathbb{N}$ majore tous les éléments de $\mathbb{N}$, alors en particulier $M \geq s(M)$. Mais le lemme 1.45 nous indique que $M \leq s(M)$. Nous avons donc $s(M) = M$, c'est à dire $M = M + 1$. En utilisant la régularité de M ¹³, nous trouvons $0 = 1$, ce qui est impossible par le lemme 1.42.

Pour (4) Soit A une partie non vide et majorée de $\mathbb{N}$.

L'ensemble B Nous posons

$$B = \{n \in \mathbb{N} \setminus A \text{ tel que } a \leq n \forall a \in A\}. \quad (1.53)$$

B est non vide

Soit un majorant M de A : pour tout $a \in A$ nous avons $a \leq M$. Nous avons $s(M) \notin A$, parce que si $s(M)$ était dans A , ce serait un élément de A strictement plus grand que tout $a \in A$. Donc B est non vide parce qu'il contient $s(M)$.

Minimum Vu que B est non vide, il possède un plus petit élément que nous notons b . Nous savons que $b \neq 0$ parce que sinon ce serait que A est vide. Il existe donc $c \in \mathbb{N}$ tel que $b = s(c)$.

$a \leq c$ pour tout $a \in A$ Vu que $s(c) \in B$ nous avons $a < s(c)$ pour tout $a \in A$. Donc, par le lemme 1.47(3) nous avons $s(a) \leq s(c)$, c'est à dire $a + 1 \leq c + 1$. Par régularité nous avons $a \leq c$.

Nous avons prouvé que $a \leq c$ pour toute $a \in A$.

$c \in A$ Si c n'est pas dans A , alors il est dans B et il contredit la minimalité de b . Donc c est dans A .

Conclusion L'élément c est dans A tout en étant plus petit que tout élément de A .

13. Dit plus simplement : en simplifiant par M .

Unicité Si x est un élément minium de A , alors nous avons $x \leq c$ parce que x est minimum et $c \leq x$ parce que c est minimum, et donc $x = c$. □

Lemme 1.52 ([1]).

Quelques affirmations sur l'ordre dans $\mathbb{N}$.

(1) Il n'existe pas de $n \in \mathbb{N}$ tel que $n < 0$.

(2) Si $a, b \in \mathbb{N}$ vérifient $a > b$, alors il n'existe pas de x dans $\mathbb{N}$ tel que $a + x = b$.

Démonstration. En deux parties.

Pour (1) Nous savons par la proposition 1.51(1) que 0 est l'unique minimum de $\mathbb{N}$. Nous avons donc forcément $0 \leq n$. Si n vérifie de plus $n \leq 0$ alors nous avons $n = 0$ par symétrie de la relation d'ordre $\leq$. Il n'est donc pas possible d'avoir $n \neq 0$.

Pour (2) Si $b \leq a$ il existe $c \in \mathbb{N}$ tel que $b + c = a$. Et comme $a \neq b$, c n'est pas nul et il existe $y \in \mathbb{N}$ tel que $c = s(y)$. Bref, nous avons

$$b + s(y) = a. \quad (1.54)$$

Si de plus il existe $x \in \mathbb{N}$ tel que $a + x = b$ nous aurions

$$a + x + s(y) = a. \quad (1.55)$$

Vu que a est régulier pour l'addition¹⁴, nous avons

$$x + s(y) = 0, \quad (1.56)$$

ce qui signifie, par le lemme 1.43 que $x = s(y) = 0$. Vu que s prend ses valeurs dans $\mathbb{N} \setminus \{0\}$, cela est impossible. □

Définition 1.53.

Soient $a, b \in \mathbb{N}$ tels que $a \leq b$. Nous notons par $\{a, \dots, b\}$ l'ensemble

$$\{x \in \mathbb{N} \text{ tel que } a \leq x \leq b\}. \quad (1.57)$$

Proposition 1.54.

Une application $\mathbb{N} \rightarrow \mathbb{N}$ strictement croissante est injective.

Démonstration. Soit une application strictement croissante $f: \mathbb{N} \rightarrow \mathbb{N}$. Soient $a, b \in \mathbb{N}$ tels que $f(a) = f(b)$. Vu que l'ordre est total¹⁵, nous supposons que $a \leq b$. Si $a = b$ nous avons terminé. Nous supposons donc que $a \neq b$, c'est à dire que $a < b$. Par stricte croissance nous avons alors $f(a) < f(b)$ qui signifie $f(a) \leq f(b)$ et $f(a) \neq f(b)$. Contradiction. Il n'existe donc pas de $a \neq b$ tels que $f(a) = f(b)$. L'application f est donc injective. □

Lemme 1.55 ([1]).

Si S n'est pas majoré dans $\mathbb{N}$, alors il existe une bijection $\mathbb{N} \rightarrow S$.

Démonstration. Nous considérons l'application suivante :

$$\begin{aligned} g: S &\rightarrow S \\ n &\mapsto \min\{x \in S \text{ tel que } x > n\}. \end{aligned} \quad (1.58)$$

14. Proposition 1.41(3).

15. Proposition 1.50.

Cette application est bien définie parce que toute partie non vide de $\mathbb{N}$ a un plus petit élément¹⁶. Maintenant nous définissons $f: \mathbb{N} \rightarrow S$ par

$$\begin{cases} f(0) = \min(S) \\ f(n+1) = g(f(n)). \end{cases} \quad \begin{matrix} (1.59a) \\ (1.59b) \end{matrix}$$

C'est le théorème 1.36 qui nous permet de le faire. Nous montrons que f est bijective.

Injective Nous avons que

$$f(n+1) \in \{x \in S \text{ tel que } x > f(n)\}. \quad (1.60)$$

Donc f est strictement croissante. Elle est donc injective.

Surjective Soit $a \in S$. Nous allons voir que a est dans l'image de f . Pour cela nous posons

$$A = \{x \in \mathbb{N} \text{ tel que } f(x) < a\}. \quad (1.61)$$

Cet ensemble est majoré par a . En effet si $x \in A$ nous avons $x \leq f(x) < a$. La partie A de $\mathbb{N}$ possède un maximum. Nous notons $M = \max(A)$. Ce M a deux propriétés intéressantes.

D'abord Vu que $M \in A$, nous avons $f(M) < a$. Une autre façon de dire cela est de dire que

$$a \in \{x \in S \text{ tel que } x > f(M)\}. \quad (1.62)$$

Or $f(M+1) = \min\{x \in S \text{ tel que } x > f(M)\}$. Donc $f(M+1) \leq a$.

Ensuite Vu que M est le maximum de A , $M+1$ majore A , c'est à dire que $f(M+1) \geq a$.

Les deux ensemble Nous avons prouvé que $f(M+1) \leq a$ et $f(M+1) \geq a$. Nous en déduisons, par le lemme 1.49, que $f(M+1) = a$.

□

1.56.

Durant la preuve du lemme 1.55, nous n'avons pas été loin de prouver que

$$(\min(S), S, g) \quad (1.63)$$

est un triple naturel.

Toute partie non bornée de $\mathbb{N}$ donne lieu à un triple naturel.

Définition 1.57 ([1]).

Soit un ensemble muni d'une loi de composition interne $(A, +)$. Soit $n \in \mathbb{N}$ et $a \in A$. Nous définissons $n \times A$ par

$$\begin{cases} 0 \times a = 0 \\ (n+1) \times a = n \times a + a. \end{cases} \quad \begin{matrix} (1.64a) \\ (1.64b) \end{matrix}$$

Définition 1.58.

Un ensemble totalement ordonné muni d'une loi de composition interne $(A, +, \leq)$ **archimédien** si pour tout $x, y \in A$ avec $x > 0$, il existe $n \in \mathbb{N}$ tel que $n \times x \geq y$ (voir la définition 1.57).

1.3.4 Multiplication dans les naturels

Proposition-Définition 1.59.

Il existe une unique fonction $f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ telle que

- (1) $f(a, 0) = 0$ pour tout $a \in \mathbb{N}$
- (2) $f(a, s(b)) = f(a, b) + a$ pour tout $a, b \in \mathbb{N}$.

Cette fonction est la **multiplication** et nous notons $f(a, b) = a \times b$, voire ab quand il n'y a pas d'ambiguïtés. Le nombre $a \times b$ est nommé le **produit** de a par b .

16. Proposition 1.51(2).

Démonstration. En deux parties.

Fonctions définies par récurrence Soit $a \in \mathbb{N}$. Par le théorème 1.36, il existe une unique application $f_a: \mathbb{N} \rightarrow \mathbb{N}$ telle que

$$\begin{cases} f_a(0) = 0 \\ f_a(s(b)) = f_a(b) + a \end{cases} \quad (1.65a)$$

$$(1.65b)$$

Existence Nous considérons, pour chaque $a \in \mathbb{N}$ la fonction f_a définie par les conditions (1.65).

En posant $f(a, b) = f_a(b)$, nous avons une application qui vérifie toutes les conditions.

Unicité Soient des applications f et g vérifiant les propriétés demandées. Soit $a \in \mathbb{N}$. Nous pouvons définir $f_a: \mathbb{N} \rightarrow \mathbb{N}$ et $g_a: \mathbb{N} \rightarrow \mathbb{N}$ par $f_a(n) = f(a, n)$ et $g_a(n) = g(a, n)$.

Les applications f_a et g_a vérifient toutes deux les conditions (1.65). Vue l'unicité, nous avons $f_a = g_a$ pour chaque a , et donc $f = g$.

□

1.60.

Nous supposons que la lectrice sait déjà la priorité des opérations. Elle saura donc interpréter des expressions comme $a \times b + c$ comme voulant dire $(a \times b) + c$ sans que nous ayons à ajouter des parenthèses.

Proposition 1.61 ([12, 1]).

La multiplication a les propriétés suivantes.

(1) $n \times 1 = n$ pour tout $n \in \mathbb{N}$.

(2) $0 \times n = 0$ pour tout $n \in \mathbb{N}$

(3) $1 \times n = n$ pour tout $n \in \mathbb{N}$

(4) L'élément 1 est neutre pour la multiplication.

(5) La multiplication est distributive par rapport à l'addition.

(6) La multiplication est commutative.

(7) La multiplication est associative.

Démonstration. En plein de parties.

Pour (1) Nous avons $n \times 1 = n \times s(0) = (n \times 0) + n = 0 + n = n$.

Pour (2) C'est vrai pour $n = 0$ par la définition 1.59(1). En ce qui concerne $s(n)$, nous avons

$$0 \times s(n) = (0 \times n) + 0 = 0. \quad (1.66)$$

Pour (3) Par la définition, c'est vrai avec $n = 0$. Pour la récurrence,

$$1 \times s(n) = (1 \times n) + 1 = n + 1 = s(n). \quad (1.67)$$

Pour (4) Nous avons déjà prouvé que $1 \times n = n \times 1 = n$.

Pour (5) Soient $a, b \in \mathbb{N}$. Nous prouvons par récurrence sur $c \in \mathbb{N}$ que ¹⁷

$$(a + b) \times c = a \times c + b \times c. \quad (1.68)$$

Pour $c = 0$, nous avons $(a + b) \times 0 = 0$ ainsi que $a \times 0 = b \times 0 = 0$ en vertu des points précédents sur la multiplication par zéro. Pour la récurrence nous utilisons associativité et la commutativité de la somme :

$$(a + b) \times s(c) = (a + b) \times c + (a + b) \quad (1.69a)$$

$$= a \times c + b \times c + a + b \quad (1.69b)$$

$$= (a \times c + a) + (b \times c + b) \quad (1.69c)$$

$$= (a \times s(c)) + (b \times s(c)). \quad (1.69d)$$

17. Nous n'écrivons pas toutes les parenthèses parce que les règles de priorité des opérations sont supposées connues. J'invite cependant le lecteur à remarquer qu'une formalisation de ces règles n'est probablement pas facile. Pour que tout soit rigoureux, il faudrait un algorithme qui parcourt une suite de caractères et l'interprète en ajoutant correctement les parenthèses.

Pour (6) Soit $a \in \mathbb{N}$. Nous prouvons par récurrence sur b que $a \times b = b \times a$. Pour $b = 0$ c'est bon.
Pour la récurrence :

$$a \times s(b) = a \times b + a \quad (1.70a)$$

$$= b \times a + a \quad \text{récurrence} \quad (1.70b)$$

$$= (b \times a) + (1 \times a) \quad (1.70c)$$

$$= (b + 1) \times a \quad \text{distributivité} \quad (1.70d)$$

$$= s(b) \times a. \quad (1.70e)$$

Pour (7) Soient $a, b \in \mathbb{N}$. Nous démontrons par récurrence sur $c \in \mathbb{N}$ que $(a \times b) \times c = a \times (b \times c)$.
Pour $c = 0$ l'égalité est okay. Nous faisons avec $s(c)$:

$$(a \times b) \times s(c) = ((a \times b) \times c) + a \times b \quad (1.71a)$$

$$= (a \times (b \times c)) + a \times b \quad \text{récurrence} \quad (1.71b)$$

$$= ((b \times c) \times a) + b \times a \quad \text{commutativité} \quad (1.71c)$$

$$= (b \times c + b) \times a \quad \text{distributivité} \quad (1.71d)$$

$$= (s(c) + b) \times a \quad \text{définition 1.59(2)} \quad (1.71e)$$

$$= a \times (b \times s(c)) \quad \text{commutativité.} \quad (1.71f)$$

□

Lemme 1.62 ([1]).

La multiplication est compatible avec l'ordre :

$$a \leq b \Rightarrow a \times n \leq b \times n \quad (1.72)$$

pour tout $n \in \mathbb{N}$.

Démonstration. Par la définition 1.44 de l'ordre, si $a \leq b$, il existe $c \in \mathbb{N}$ tel que $b = a + c$. En utilisant la distributivité¹⁸, nous avons

$$b \times n = (a + c) \times n = a \times n + c \times n. \quad (1.73)$$

Nous en déduisons que $b \times n \leq a \times c$ parce qu'en ajoutant $c \times n$ au second, on trouve le premier. □

Lemme 1.63.

Si $a \times b = 0$, alors $a = 0$ ou $b = 0$ (ou les deux).

Démonstration. Supposons que $a \neq 0$. Alors il existe $c \in \mathbb{N}$ tel que $a = s(c)$. Nous avons

$$0 = a \times b = s(c) \times b = c \times b + b. \quad (1.74)$$

Le lemme 1.43 nous dit alors que $c \times b = b = 0$. □

Lemme 1.64 ([1]).

Si $a < b$ et si $n \neq 0$, alors

$$a \times n < b \times n. \quad (1.75)$$

Démonstration. L'hypothèse $a \leq b$ implique qu'il existe $c \in \mathbb{N}$ tel que $a + c = b$. De plus $c \neq 0$ parce que $a \neq b$. En utilisant la distributivité¹⁹, nous avons

$$b \times n = (a + c) \times n = (a \times n) + (c \times n). \quad (1.76)$$

Cela prouve que $a \times n \leq b \times n$. Et comme c et n ne sont pas nuls, nous avons même²⁰ $c \times n \neq 0$ et donc $a \times n < b \times n$. □

18. Proposition 1.61(5).

19. Proposition 1.61(5).

20. Lemme 1.63.

Proposition 1.65 ([1]).

Tous les naturels non nuls sont réguliers par rapport à la multiplication. Autrement dit, si $a \neq 0$, alors nous avons

$$a \times x = a \times y \Rightarrow x = y. \quad (1.77)$$

Démonstration. Soit $a \neq 0$ dans $\mathbb{N}$. Nous supposons que $a \times x = a \times y$. Vu que l'ordre sur $\mathbb{N}$ est total (proposition 1.50), nous pouvons supposer que $y \geq x$; sinon il suffit de permuter les rôles de x et y dans tout ce qui suit.

Il existe $d \in \mathbb{N}$ tel que $y = x + d$. En utilisant l'hypothèse et la distributivité²¹,

$$(a \times x) = a \times (x + d) = (a \times x) + (a \times d). \quad (1.78)$$

Vu que $(a \times x)$ est régulier pour la somme²² nous en déduisons que

$$0 = a \times d. \quad (1.79)$$

Le lemme 1.63 dit alors que $a = 0$ ou que $d = 0$. Vu que l'hypothèse stipule que $a \neq 0$, nous déduisons que $d = 0$, c'est à dire que $x = y$. $\square$

1.3.5 Presque unicité des triplets naturels

Il existe de nombreux triplets naturels; l'existence d'un triplet naturel est un théorème de la théorie des ensembles que nous avons accepté. Nous avons déjà à peu près montré que toute partie non bornée de $\mathbb{N}$ donne lieu à un nouveau triplet naturel. Voir 1.56.

Nous voyons maintenant que tous les triplets naturels sont équivalents au moins pour l'ordre.

Théorème 1.66 ([1]).

Soient des triplets naturels $(\mathcal{N}_1, o_1, s_1)$ et $(\mathcal{N}_2, o_2, s_2)$. Alors

(1) il existe une unique application $f: \mathcal{N}_1 \rightarrow \mathcal{N}_2$ telle que

$$(1a) \quad f(o_1) = o_2$$

$$(1b) \quad f \circ s_1 = s_2 \circ f.$$

(2) Une telle application est une bijection croissante.

Démonstration. En plusieurs points.

Existence Nous voyons $(\mathcal{N}_1, o_1, s_1)$ comme un triple naturel, et $\mathcal{N}_2$ comme une simple ensemble.

Nous pouvons appliquer le théorème 1.36 à $(\mathcal{N}_1, o_1, s_1)$. L'élément o_1 va jouer le rôle de 0 alors que o_2 va jouer le rôle de b . L'application g est s_2 . Bref, il existe une unique application $f: \mathcal{N}_1 \rightarrow \mathcal{N}_2$ telle que

$$(1) \quad f(o_1) = o_2$$

$$(2) \quad f(s_1(n)) = s_2(f(n))$$

pour tout $n \in \mathcal{N}_1$.

Unicité Le théorème 1.36 donne déjà l'unicité. Nous la faisons quand même, juste pour vous faire plaisir. Soit g , une autre application vérifiant les mêmes conditions. Nous posons

$$A = \{x \in \mathcal{N}_1 \text{ tel que } f(x) = g(x)\}. \quad (1.80)$$

Nous avons $f(o_1) = o_2 = g(o_1)$. Donc $o_1 \in A$. Supposons que $P(a) = 1$, c'est à dire que $g(a) = f(a)$. Prenons s_2 des deux côtés :

$$(s_2 \circ g)(a) = (s_2 \circ f)(a), \quad (1.81)$$

ce qui donne $(g \circ s_1)(a) = (f \circ s_1)(a)$. Donc $s_1(a) \in A$.

Nous en déduisons que $A = \mathcal{N}_1$.

21. Proposition 1.61(5).

22. Proposition 1.41(3).

Bijection, définir l'inverse Nous allons trouver un inverse et le lemme 1.7 nous dit que c'est suffisant. La partie « existence », en inversant les rôles de $\mathcal{N}_1$ et $\mathcal{N}_2$ nous donne une application $g: \mathcal{N}_2 \rightarrow \mathcal{N}_1$ telle que

$$(1) \quad g(o_2) = o_1$$

$$(2) \quad g \circ s_2 = s_1 \circ g.$$

Nous allons prouver que g est un inverse de f .

$f \circ g = \text{Id}$ Nous posons $A = \{x \in \mathcal{N}_2 \text{ tel que } (f \circ g)(x) = x\}$. Nous avons

$$f(g(o_2)) = f(o_1) = o_2, \quad (1.82)$$

et donc $o_2 \in A$.

Supposons que $x \in A$. Alors

$$(f \circ g)(s_2(x)) = (f \circ \underbrace{g \circ s_2}_{s_1 \circ g})(x) \quad (1.83a)$$

$$= (\underbrace{f \circ s_1}_{=s_2 \circ f} \circ g)(x) \quad (1.83b)$$

$$= (s_2 \circ f \circ g)(x) \quad (1.83c)$$

$$= s_2((f \circ g)(x)) \quad (1.83d)$$

$$= s_2(x) \quad (1.83e)$$

Donc $s_2(x) \in A$. Nous en déduisons que $A = \mathcal{N}_2$ par le point (3) de la définition 1.32 de triple naturel.

$g \circ f = \text{Id}$ J'imagine que c'est la même chose que l'autre²³.

□

Proposition 1.67.

L'ensemble structuré $(\mathbb{N}, +, \times, \leq)$ est archimédien²⁴. En d'autres termes, pour tout $a, b \in \mathbb{N} \setminus \{0\}$, il existe $n \in \mathbb{N}$ tel que

$$b < n \times a. \quad (1.84)$$

Démonstration. Soient $a, b \in \mathbb{N}$ avec $a \neq 0$.

Si $a > b$, nous avons le résultat avec $n = 1$.

Si $a = b$, en prenant $n = s(1)$ nous avons le résultat. En effet $s(1) \times a = a + a$. Vu que $a \neq 0$, nous avons $a + a \geq a$ et $a + a \neq a$, donc $s(1) \times a > a$.

La vraie vie est avec $a < b$. Nous posons

$$X = \{x \in \mathbb{N} \text{ tel que } 1 \leq x \times a \leq b\} \quad (1.85)$$

et

$$B = \{x \times a \text{ tel que } x \in X\}. \quad (1.86)$$

L'ensemble X est non vide parce que $1 \in X$. L'ensemble B est alors également non vide, et majoré par b . La proposition 1.51(4) nous indique alors que B possède un plus grand élément que nous allons noter $x_0 \times a$ ($x_0 \in X$).

Nous posons $n = s(x_0)$, et nous avons

$$x_0 \times a < x_0 \times a + a = s(x_0) \times a = n \times a. \quad (1.87)$$

Nous en déduisons que $n \times a$ n'est pas dans B parce que $x_0 \times a$ est le plus grand élément de B . Donc x_0 n'est pas dans X ; nous n'avons donc pas les inégalités

$$1 \leq n \times a \leq b. \quad (1.88)$$

Laquelle des deux inégalité est fausse? Vu que $n = s(x_0) \geq 1$ et que $a \geq 1$, nous avons $1 \leq n \times a$. Donc c'est la seconde inégalité qui est fausse. Nous avons donc $n \times a > b$. □

23. J'ai pas fait les calculs; écrivez-moi si ça pose un problème.

24. Définition 1.58.

Définition 1.68.

Soit A un ensemble muni d'une loi de composition interne²⁵ notée $+$. Si nous avons une application $\alpha: \mathbb{N} \rightarrow A$, alors nous définissons la notation $\sum_{i=0}^N \alpha(i)$ par récurrence de la façon suivante :

- (1) $\sum_{i=0}^0 \alpha(i) = \alpha(0)$,
- (2) $\sum_{i=0}^k \alpha(i) = \sum_{i=0}^{k-1} \alpha(i) + \alpha(k)$.

1.69.

Si vous êtes attentif, vous remarquerez que la définition 1.68 a besoin du théorème 1.36 pour s'assurer que $\sum_{i=0}^N$ est bien définie pour tout $N \in \mathbb{N}$.

Proposition 1.70 (La multiplication est une somme itérée[12]).

Pour tout $a, b \in \mathbb{N}$, nous avons

$$\sum_{i=1}^n a = a \times n. \quad (1.89)$$

Démonstration. Nous le faisons par récurrence en partant de $n = 1$. Avec $n = 1$ nous avons $\sum_{i=1}^1 a = a$, et $a \times 1 = a$. Donc c'est bon.

Pour la récurrence nous avons :

$$a \times s(n) = a \times n + a = \sum_{i=1}^n a + a = \sum_{i=1}^{n+1} a = \sum_{i=1}^{s(n)} a. \quad (1.90)$$

□

Lemme 1.71.

Soit $a > 1$. Pour tout $n \geq 1$ nous avons $na \leq a^n$.

Démonstration. Par récurrence. Avec $n = 1$ nous avons bien $a \leq a$; pas de problèmes. Supposons que $na \leq a^n$, et faisons le pas de récurrence. Nous avons :

$$(n+1)a = na + a \quad (1.91a)$$

$$\leq na + na \quad \text{parce que } a \leq na \quad (1.91b)$$

$$= 2na \quad (1.91c)$$

$$\leq 2a^n \quad \text{récurrence} \quad (1.91d)$$

$$\leq aa^n \quad \text{parce que } a \geq 2 \quad (1.91e)$$

$$= a^{n+1}. \quad (1.91f)$$

□

Proposition 1.72 ([12]).

Soit $a > 1$. Alors

- (1) l'application $n \mapsto a^n$ est strictement croissante ;
- (2) l'ensemble $\{a^n \text{ tel que } n \in \mathbb{N}\}$ n'est pas majoré.

Démonstration. Nous avons

$$a^{n+1} = a^n \times a < a^n \times 1 = a^n. \quad (1.92)$$

L'inégalité stricte est parce que $a > 1$. Cela prouve le premier point.

Pour le second point, soit $m \in \mathbb{N}$. Nous devons trouver $N \in \mathbb{N}$ tel que $a^N \geq m$. Vu que $\mathbb{N}$ est archimédien²⁶, nous pouvons considérer N tel que $Na > b$. Le lemme 1.43 nous assure alors que

$$b < Na \leq a^N. \quad (1.93)$$

□

25. Peut-être un anneau, mais comme nous avons l'intention, dans les propositions 1.70 et suivantes, de faire des sommes vers $(\mathbb{N}, +)$, plutôt un monoïde.

26. Proposition 1.67.

Théorème 1.73 (division euclidienne [12]).

Pour tout $a \in \mathbb{N}$, pour tout $b \in \mathbb{N} \setminus \{0\}$, il existe un unique couple $(q, r) \in \mathbb{N}^2$ tel que $a = bq + r$ avec $0 \leq r < b$.

Si $r = 0$, nous disons que a est **divisible** par b .

Démonstration. Existence puis unicité.

Existence Nous posons

$$A = \{bx \text{ tel que } x \in \mathbb{N}, bx \leq a\}. \quad (1.94)$$

L'ensemble A contient 0 (avec $x = 0$) et est majoré par a . Donc il possède un plus grand élément que nous notons bq . Vu que $bq \in A$, nous avons $bq \leq a$ et donc il existe $r \in \mathbb{N}$ tel que

$$bq + r = a. \quad (1.95)$$

Il reste à montrer que $r < b$. Supposons que $r \geq b$. Il existerait alors un x tel que $b + x = r$. En mettant ça dans (1.95),

$$bq + b + x = a, \quad (1.96)$$

c'est à dire $b(q + 1) + x = a$, qui signifierait $b(q + 1) \leq a$, ce qui est faux parce que bq est le plus grand élément de A .

Unicité Supposons que nous ayons

$$a = bq + r = bq' + r' \quad (1.97)$$

avec $0 \leq r < b$ et $0 \leq r' < b$. Il y a trois possibilités : $q' < q$, $q' = q$ et $q' > q$.

Si $q' < q$ Alors il existe $x \in \mathbb{N}$ tel que $q' + x = q$, nous nous avons

$$b(q' + x) + r = bq' + bx + r, \quad (1.98)$$

ce qui, après distribution et simplification, donne $r' = bx + r$. Vu que nous avons $x \geq 1$, nous avons alors

$$r' = bx + r \geq b + r \geq b. \quad (1.99)$$

Cela n'est pas possible parce que $r' < b$. Le cas $q' < q$ n'est pas possible.

Si $q' = q$ Nous avons alors immédiatement $bq + r = bq + r'$ et donc $r = r'$. Unicité.

Si $q' > q$ En posant $q + x = q'$ nous trouvons la même impossibilité que dans le cas $q' < q$.

□

1.3.6 Écriture d'un naturel dans une base

1.74.

Nous avons déjà donné la notation $1 = s(0)$. Nous continuons avec $2 = s(1)$, $3 = s(2)$, $4 = s(3)$, $5 = s(4)$, $6 = s(5)$, $7 = s(6)$, $8 = s(7)$ et $9 = s(8)$.

Nous allons maintenant voir comment écrire des nombres plus grands.

Si $b > 1$ et $N \in \mathbb{N}$ sont donnés, nous notons

$$C_{b,N} = \{u \in \{0, \dots, b-1\}^{N+1} \text{ tel que } u_N \neq 0\}. \quad (1.100)$$

où les u_i sont numérotés à partir de 0 ; donc dire $u_N \neq 0$ revient à dire que le *dernier* est non nul, et non l'avant dernier. Nous définissons²⁷

$$\begin{aligned} \varphi_{b,N} : C_{b,N} &\rightarrow \mathbb{N} \\ u &\mapsto \sum_{i=0}^N u_i b^i. \end{aligned} \quad (1.101)$$

Cette application $\varphi_{b,N}$ sera encore bien étudiée pour la partie décimale d'un réel. Voir la définition 11.316.

27. Le symbole de sommation est défini par 1.68.

Lemme 1.75 ([12]).

Soient $b > 1$, $N \geq 0$ ainsi que $u \in C_{b,N}$. Alors

$$a^N \leq \varphi_{b,N}(u) < a^{N+1}. \quad (1.102)$$

Démonstration. En séparant la somme nous avons

$$\varphi_{b,N}(u) = u_N b^N + \sum_{i=0}^{N-1} i_i b^i. \quad (1.103)$$

Vu que $u_N \geq 1$ nous avons $b^N \leq u_N b^N$, et donc

$$b^N \leq u_N b^N \leq \varphi_{b,N}(u). \quad (1.104)$$

Voilà qui prouve la première inégalité de (1.102).

Pour prouver que $\varphi_{b,N}(u) < b^{N+1}$, nous faisons une récurrence sur N .

Pour $N = 1$ Nous devons prouver que $\varphi_{b,0}(u) < a$. Par définition $\varphi_{b,N}(u) = u_0$. Vu que $u \in \{0, \dots, b-1\}^{N+1}$, nous avons $u_0 \leq b-1 < b$.

Récurrence Nous supposons que pour tout $u \in C_{b,N}$ nous avons $\varphi_{b,N}(u) < b^{N+1}$. Et nous devons montrer que pour tout $v \in C_{b,N+1}$ nous avons $\varphi_{b,N+1}(v) < b^{N+2}$.

Nous posons $u = (v_0, \dots, v_N)$; nous avons alors

$$\varphi_{b,N+1}(v) = v_{N+1} b^{N+1} + \sum_{i=0}^N v_i b^i \quad (1.105a)$$

$$= v_{N+1} b^{N+1} + \varphi_{b,N}(u) \quad (1.105b)$$

$$< v_{N+1} b^{N+1} + b^{N+1} \quad \text{récurrence} \quad (1.105c)$$

$$= (v_{N+1} + 1) b^{N+1} \quad (1.105d)$$

$$\leq b b^{N+1} \quad \text{parce que } v_{N+1} \leq b-1 \quad (1.105e)$$

$$= b^{N+2}. \quad (1.105f)$$

□

Lemme 1.76 ([1]).

Soient $x \in \mathbb{N}$ ainsi que $b \geq 2$. Nous posons

$$N = \max\{k \in \mathbb{N} \text{ tel que } b^k \leq x\}. \quad (1.106)$$

Alors

(1) Si $n > N$ alors $\varphi_{b,n}(u) > x$ pour tout $u \in C_{b,n}$.

(2) Si $n < N$ alors $\varphi_{b,n}(u) < x$ pour tout $u \in C_{b,n}$.

Démonstration. En deux parties.

Si $n > N$ Nous avons, par définition de $C_{b,n}$ que $u_n \neq 0$, de telle sorte que

$$\varphi_{b,n}(u) \geq u_n b^n \geq b^n > x. \quad (1.107)$$

La dernière inégalité est due au fait que $n \notin A$.

Si $n < N$ Nous avons

$$x \geq b^N > \varphi_{b,n}(u). \quad (1.108)$$

Le seconde inégalité est une conséquence du lemme 1.75.

□

Théorème 1.77 ([12]).

Soit $b \geq 2$. Si $x \in \mathbb{N}$, alors il existe un unique $N \in \mathbb{N}$ et un unique $u \in C_{b,N}$ tels que

$$x = \varphi_{b,N}(u). \quad (1.109)$$

Démonstration. Nous commençons par $x < b$. Dans ce cas, $N = 0$ parce que si $u_k \neq 0$ avec $k \neq 0$, nous avons

$$\sum_{i=0}^N u_i b^i \geq u_k b^k \geq b > x. \quad (1.110)$$

Donc $x = x_0 b^0 = u_0$. Bref, dans le cas $x < b$ nous avons obligatoirement $N = 0$ et $u_0 = x$.

Nous faisons à présent le cas $x \geq b$. Prouvons que $N \geq 1$. Si $N = 0$, alors $\varphi_{b,0}(u) = u_0 < b \leq a$. Donc $N \geq 1$, et nous pouvons parler de $N - 1$.

Unicité, préambule Le lemme 1.76 nous indique que si $x = \varphi_{b,N}(u)$ pour un certain $N \in \mathbb{N}$ et un certain $u \in C_{b,N}$, alors

$$N = \max\{k \in \mathbb{N} \text{ tel que } b^k \leq x\}. \quad (1.111)$$

Nous posons

$$X_k = \sum_{i=k}^N u_i b^{i-k}, \quad (1.112)$$

et nous allons montrer que le couple (X_{k+1}, u_k) est le résultat de la division euclidienne²⁸ de X_k par b .

D'abord, $u_k < b$, donc ça a bien la tête d'un reste. Ensuite, pour le quotient,

$$bX_{k+1} + u_k = b \sum_{i=k+1}^N u_i b^{i-(k+1)} + u_k \quad (1.113a)$$

$$= \sum_{i=k+1}^N u_i b^{i-k} + u_k \quad (1.113b)$$

$$= \sum_{i=k}^N u_i b^{i-k} \quad (1.113c)$$

$$= X_k. \quad (1.113d)$$

Unicité En quoi cela fait-il avancer la choucroute? Supposons que $\varphi_{b,N}(u) = \varphi_{b,M}(v)$. Alors nous avons déjà prouvé que

$$M = N = \max\{k \in \mathbb{N} \text{ tel que } b^k \leq x\}. \quad (1.114)$$

Ensuite nous devons montrer que $u = v$. Nous posons $X_k = \sum_{i=k}^N u_i b^{i-k}$ et $Y_k = \sum_{i=k}^N v_i b^{i-k}$. Notez que

$$X_0 = Y_0 = x. \quad (1.115)$$

Si $X_k = Y_k$, alors par unicité de la division euclidienne nous avons $X_{k+1} = Y_{k+1}$ et $u_k = v_k$. Par récurrence nous avons $X_k = Y_k$ et $u_k = v_k$ pour tout k .

Existence Soit $x \in \mathbb{N}$. Nous posons $y_0 = x$ et

$$y_k = ay_{k+1} + u_k \quad (1.116)$$

avec $u_k < b$. Vos l'unicité dans la division euclidienne et le théorème²⁹ 1.36 permettant la définition par récurrence, ces conditions définissent deux suites (u_k) et (y_k) dans $\mathbb{N}$.

28. Théorème 1.73.

29. Nous ne citerons pas toujours ce théorème à chaque fois que nous définissons quelque chose par récurrence.

Montrons qu'il existe un $N \in \mathbb{N}$ tel que $y_n = 0$ pour tout $n \geq N + 1$. Nous avons :

$$2y_{k+1} \leq by_{k+1} \quad \text{parce que } b \geq 2 \quad (1.117a)$$

$$\leq y_k \quad \text{pcq } by_{k+1} + u_k = y_k. \quad (1.117b)$$

Bref : $2y_{k+1} \leq y_k$. Par récurrence³⁰ nous trouvons que

$$2^k y_k \leq x \quad (1.118)$$

parce que $y_0 = x$. Par le lemme 1.71, si k est assez grand,

$$2ky_k \leq 2^k y_k \leq x. \quad (1.119)$$

Vu que $\mathbb{N}$ est archimédien³¹, nous pouvons considérer $s \in \mathbb{N}$ tel que $2s > x$. À ce moment nous avons

$$y_n = 0 \quad (1.120)$$

pour tout $n \geq s$. Nous posons

$$N = \max\{k \text{ tel que } y_k \neq 0\}. \quad (1.121)$$

Prouvons par récurrence sur l que

$$y_{N-l} = \sum_{i=N-l}^N u_i b^{(i+l)-N}. \quad (1.122)$$

Notez que $i + l \geq N - l + l = N$, donc $(i + l) - N$ a un sens.

Pour $l = 0$ Avec $l = 0$ nous avons $\sum_{i=N-l}^N u_i b^{(i+l)-N} = u_N$. Il faut donc voir que $y_N = u_N$.

Nous avons

$$y_N = by_{N+1} + u_N. \quad (1.123)$$

En se rappelant que $y_{N+1} = 0$, nous avons le résultat.

Pour $l + 1$ Pour la récurrence nous avons le calcul suivant :

$$y_{N-l-1} = by_{N-l} + u_{N-l-1} \quad (1.124a)$$

$$= b \sum_{i=N-l}^N u_i b^{(i+l)-N} + u_{N-l-1} \quad (1.124b)$$

$$= \sum_{i=N-l}^N u_i b^{(i+l)-N+1} + u_{N-l-1} \quad (1.124c)$$

$$= \sum_{i=N-l-1}^N u_i b^{(i+l+1)-N}. \quad (1.124d)$$

La récurrence est faite. L'égalité (1.122) est validée pour tout l .

En posant $l = N$ dans (1.122) nous trouvons

$$y_0 = \sum_{i=0}^N u_i b^i. \quad (1.125)$$

Mais la définition de la suite (y_k) contient $y_0 = x$. Donc nous avons prouvé que

$$x = \sum_{i=0}^N u_i b^i = \varphi_{b,N}(u). \quad (1.126)$$

30. Faut-il citer la proposition 1.35 et donner explicitement la fonction P ?

31. Proposition 1.67.

□

Exemple 1.78.

Comment écrire le nombre b en base b ? Nous devons trouver un N et une suite (u_i) tels que

$$b = \sum_{i=0}^N u_i b^i. \quad (1.127)$$

Il est facile de voir que le choix $N = 1$ et $u = (0, 1)$ fonctionne bien : $b = 1 \times b^1 + 0$. Nous avons donc

$$b = \varphi_{b,1}(1, 0). \quad (1.128)$$

Nous écrivons cela plus sobrement $b = 10$. △

1.79.

À part des cas très exceptionnels, nous utilisons toujours la base $b = s(9) = s^9(0)$. Nous nous permettons donc d'écrire « 64 » le nombre $\varphi_{s(9),2}(6, 4)$. Vous saviez que tout groupe simple d'ordre $\varphi_{s(9),2}(6, 0)$ est isomorphe au groupe alterné $A_{\varphi_{s(9),0}(5)}$? C'est la proposition 5.40.

La proposition suivante dit que le nombre qui a le plus de chiffres est le plus grand.

Proposition 1.80 ([12]).

Si $u \in C_{b,N}$ et $v \in C_{b,M}$ avec $M > N$ alors $\varphi_{b,N}(u) < \varphi_{b,M}(v)$.

Démonstration. Le lemme 1.75 nous dit que

$$b^N \leq \varphi_{b,N}(u) < b^{N+1} \quad (1.129)$$

et

$$b^M \leq \varphi_{b,M}(v) < b^{M+1}. \quad (1.130)$$

Vu que $M > N$ nous avons $b^{N+1} \leq b^M$ et donc

$$\varphi_{b,N}(u) < b^{N+1} \leq b^M \leq \varphi_{b,M}(v). \quad (1.131)$$

□

La proposition suivante dit que si deux nombres s'écrivent avec le même nombre de chiffres, le plus grand est celui dont le premier chiffre différent est le plus grand. Autrement dit, les nombres en écriture de position se classent par ordre lexicographique.

Proposition 1.81.

Soient $u, v \in C_{b,N}$ tels que $u_i = v_i$ pour $i = r + 1, \dots, N$. Si $u_r > v_r$ alors $\varphi_{b,N}(u) > \varphi_{b,N}(v)$.

Démonstration. En découpant les sommes nous avons

$$\varphi_{b,N}(u) = \sum_{i=r+1}^N u_i b^i + u_r b^r + \sum_{i=0}^{r-1} u_i b^i \quad (1.132)$$

et

$$\varphi_{b,N}(v) = \sum_{i=r+1}^N v_i b^i + v_r b^r + \sum_{i=0}^{r-1} v_i b^i. \quad (1.133)$$

Vu que $b^r > \sum_{i=0}^{r-1} u_i b^i$ (lemme 1.75), nous avons aussi que

$$b^r + \sum_{i=0}^{r-1} u_i b^i > \sum_{i=0}^{r-1} v_i b^i. \quad (1.134)$$

Et le calcul final :

$$\varphi_{b,N}(v) < \sum_{i=r+1}^N v_i b^i + v_r b^r + b^r + \sum_{i=0}^{r-1} u_i b^i \quad \text{pcq (1.134)} \quad (1.135a)$$

$$= \sum_{i=r+1}^N u_i b^i + (v_r + 1) b^r + \sum_{i=0}^{r-1} u_i b^i \quad (1.135b)$$

$$\leq \sum_{i=r+1}^N u_i b^i + u_r b^r + \sum_{i=0}^{r-1} u_i b^i \quad \text{pcq } u_r \geq v_r + 1 \quad (1.135c)$$

$$= \sum_{i=0}^N u_i b^i \quad (1.135d)$$

$$= \varphi_{b,N}(u). \quad (1.135e)$$

Et voila. □

1.4 Les entiers

Proposition-Définition 1.82 ([12]).

Soient $a, b, a', b' \in \mathbb{N}$. Nous disons que $(a, b) \sim (a', b')$ si et seulement si

$$a + b' = b + a' \quad (1.136)$$

(1) Cela est une relation d'équivalence sur $\mathbb{N}^2$.

(2) Si $(a, b) \sim (a', b')$ et $(x, y) \sim (x', y')$ alors

$$(a + x, b + y) \sim (a' + x', b' + y'). \quad (1.137)$$

L'ensemble des **entiers** est

$$\mathbb{Z} = (\mathbb{N} \times \mathbb{N}) / \sim. \quad (1.138)$$

Démonstration. En plusieurs points.

Symétrie C'est la commutativité de la somme dans $\mathbb{N}$, proposition 1.41(1).

Réflexive Immédiat.

Transitive Nous supposons que $(a, b) \sim (u, v)$ et que $(u, v) \sim (x, y)$. Alors nous avons

$$a + v = u + b \quad (1.139a)$$

$$u + y = v + x. \quad (1.139b)$$

En additionnant membre à membre,

$$a + v + u + y = u + b + v + x. \quad (1.140)$$

La commutativité nous permet de mettre u et v à droite dans chacun des deux membres. Ensuite la proposition 1.41(3) nous permet de simplifier par $u + v$. Il reste $a + y = b + x$, qui signifie $(a, b) \sim (x, y)$.

Pour (2) L'hypothèse donne les égalités

$$a + b' = b + a' \quad (1.141a)$$

$$x + y' = y + x' \quad (1.141b)$$

En sommant, et en utilisant l'associativité,

$$(a + x) + (b' + y') = (b + y) + (a' + x'). \quad (1.142)$$

Cela signifie bien que $(a + x, b + y) \sim (a' + x', b' + y')$.

□

Lemme 1.83.

Soient $a, b \in \mathbb{N}$. Nous avons $\overline{(a, b)} = \overline{(0, 0)}$ si et seulement si $a = b$.

Démonstration. Dire que $\overline{(a, b)} = \overline{(0, 0)}$ est équivalent à dire que $(a, b) \sim (0, 0)$, qui est encore équivalent à dire que $a + 0 = b + 0$, ou encore que $a = b$. □

Proposition-Définition 1.84 ([12]).

Soient $a, b, x, y \in \mathbb{N}$. L'application

$$\begin{aligned} f: \overline{(a, b)} \times \overline{(x, y)} &\rightarrow \mathbb{Z} \\ ((a', b'), (x', y')) &\mapsto (a' + x', b' + y') \end{aligned} \quad (1.143)$$

est constante.

Nous nommons sa valeur $\overline{(a, b)} + \overline{(x, y)}$.

Démonstration. Cela est une conséquence de la proposition 1.82(2). □

Proposition 1.85.

La paire $(\mathbb{Z}, +)$ est un groupe abélien.

Démonstration. En plusieurs points.

Neutre Le neutre est $e = \overline{(0, 0)}$. En effet,

$$\overline{(a, b)} + \overline{(0, 0)} = \overline{(a + 0, b + 0)} = \overline{(a, b)}. \quad (1.144)$$

De même $e + \overline{(a, b)} = \overline{(a, b)}$ par commutativité de la somme dans $\mathbb{N}$.

Inverse Il est facile de vérifier que $\overline{(b, a)}$ est l'inverse de $\overline{(a, b)}$.

Associativité Calcul direct en utilisant l'associativité dans $\mathbb{N}$. □

Proposition 1.86.

L'application

$$\begin{aligned} \iota: \mathbb{N} &\rightarrow \mathbb{Z} \\ n &\mapsto \overline{(n, 0)} \end{aligned} \quad (1.145)$$

est un morphisme³² injectif.

Démonstration. Le fait que ce soit un morphisme est le calcul

$$\iota(a + b) = \overline{(a + b, 0)} = \overline{(a, 0)} + \overline{(b, 0)} = \iota(a) + \iota(b). \quad (1.146)$$

Pour l'injectivité, supposons que $\iota(a) = \iota(b)$. Alors $\overline{(a, 0)} = \overline{(b, 0)}$, c'est à dire $a + 0 = b + 0$. Donc $a = b$. □

1.4.1 Opposé**Lemme 1.87.**

Tout élément de $\mathbb{Z}$ a un représentant de la forme $(a, 0)$ ou $(0, b)$.

Démonstration. Soient $a, b \in \mathbb{N}$. Si $b \leq a$, alors nous avons

$$(a, b) \sim (a - b, 0) \quad (1.147)$$

où la différence est calculée dans $\mathbb{N}$ et a un sens parce que nous avons supposé $b \leq a$. Si par contre $a \leq b$ alors

$$(a, b) \sim (0, b - a). \quad (1.148)$$

Vu que l'ordre sur $\mathbb{N}$ est total³³, tous les cas sont couverts. □

32. Certes $\mathbb{N}$ n'est pas un groupe, donc le mot « morphisme » est un peu abusé, mais vous voyez ce que je veux dire.

33. Proposition 1.50.

Lemme-Définition 1.88.

Soit $z \in \mathbb{Z}$. L'application³⁴

$$\begin{aligned} f: z &\rightarrow \mathbb{Z} \\ (a, b) &\mapsto \overline{(b, a)} \end{aligned} \quad (1.149)$$

est constante.

Nous nommons $-z$ sa valeur.

Démonstration. Soient (a, b) et (x, y) dans z . Nous avons successivement :

- $(a, b) \sim (x, y)$.
- $a + y = b + x$.
- $(b, a) \sim (y, x)$
- $\overline{(b, a)} = \overline{(y, x)}$
- $f(a, b) = f(x, y)$.

D'où la constance de f . □

Lemme 1.89.

Nous avons

- (1) $\mathbb{Z} = \iota(\mathbb{N}) \cup -\iota(\mathbb{N})$
- (2) $\iota(\mathbb{N}) \cap -\iota(\mathbb{N}) = \{0\}$.

Démonstration. Nous avons

$$\iota(\mathbb{N}) = \{\overline{(n, 0)} \text{ tel que } n \in \mathbb{N}\} \quad (1.150a)$$

$$-\iota(\mathbb{N}) = \{\overline{(0, n)} \text{ tel que } n \in \mathbb{N}\}. \quad (1.150b)$$

Faisons maintenant les deux points.

Pour (1) Nous savons par le lemme 1.87 que tous les éléments de $\mathbb{Z}$ sont de la forme (1.150a) ou (1.150b).

Pour (2) Si $z \in \iota(\mathbb{N}) \cap -\iota(\mathbb{N})$, il existe $n, m \in \mathbb{N}$ tels que $\overline{(n, 0)} = \overline{(0, m)}$, ce qui signifie en particulier que $(n, 0) \sim (0, m)$ ou encore que $n + m = 0$. Le lemme 1.43 fait alors que $n = m = 0$.

Nous avons donc $z = \overline{(0, 0)} = 0$. □

Lemme 1.90.

Toute partie bornée de $\mathbb{Z}$ possède un plus grand élément.

Proposition 1.91.

Soit $a, b \in \mathbb{Z}$ tels que a divise b . Alors $|a| \leq |b|$.

Lemme 1.92.

L'ensemble $\mathbb{Z}$ est infini dénombrable.

1.5 Quelques résultats de cardinalité

1.5.1 Équipotence, surpotence, subpotence

Les notions d'équipotence, surpotence et de subpotence permettent de comparer les « tailles » des ensembles sans avoir besoin de la théorie des ordinaux. Tout ceci ne sera pas très souvent utile par la suite. Un exemple d'utilisation de ces notions est le théorème de Steinitz 6.127 qui démontre l'existence de clôture algébrique pour tout corps.

³⁴. Pour rappel, z est une classe d'équivalence dans $\mathbb{N} \times \mathbb{N}$, c'est à dire une partie de $\mathbb{N} \times \mathbb{N}$. Ça a un sens de prendre z comme ensemble sur lequel on définit une fonction.

Définition 1.93 ([16, 17]).

Soient deux ensembles A et B .

- (1) Les ensembles A et B sont **équipotents** si il existe une bijection entre A et B . Nous notons $A \approx B$.
- (2) L'ensemble A est **surpotent** à B si il existe une surjection de A vers B . Nous notons $A \geq B$.
- (3) L'ensemble A est **subpotent** à B si il existe une injection de A vers B . Nous notons $A \leq B$.

Nous disons également « strictement » surpotent quand il y a surpotence mais pas équipotence, et de même pour la subpotence. Les symboles $>$ et $<$ sont alors utilisés.

Proposition 1.94 ([1, 13]).

L'ensemble A est subpotent à B si et seulement si B est surpotent à A .

Démonstration. En deux parties.

$\Rightarrow$ Nous supposons que A est subpotent à B . Il existe une injection $\varphi: A \rightarrow B$. Nous définissons $f: B \rightarrow A$ par

$$f(x) = \begin{cases} \varphi^{-1}(x) & \text{si } x \in \varphi(A) \\ a & \text{sinon} \end{cases} \quad (1.151)$$

où a est un élément quelconque de A . Cette application est bien définie parce que φ est injective, de telle sorte que φ^{-1} est bien définie. Vu que φ est définie sur tout a , l'application f est une surjection.

$\Leftarrow$ Nous supposons que B est surpotent à A . Il existe donc une surjection $\varphi: B \rightarrow A$. Pour chaque $x \in A$ nous considérons un élément $b_x \in \varphi^{-1}(x)$, qui existe parce que φ est surjective. Nous considérons ensuite l'application

$$\begin{aligned} f: A &\rightarrow B \\ x &\mapsto b_x. \end{aligned} \quad (1.152)$$

Nous prouvons que f est une injection. Supposons que $x, y \in A$ soient tels que $f(x) = f(y)$. Nous avons $b_x = b_y$. Donc

$$x = \varphi(b_x) = \varphi(b_y) = y. \quad (1.153)$$

Nous avons prouvé que $x = y$, et donc que f est injective.

□

Vu que l'ensemble des ensembles n'existe pas³⁵, nous n'allons pas énoncer le fait que ces notions donnent une relation d'ordre sur les ensembles; il faudrait parler de classes et nous ne nous en sortirions pas. Nous allons toutefois énoncer quelques résultats qui vont dans ce sens. Pour en savoir plus, vous pouvez lire les différentes pages de Wikipédia sur les nombres cardinaux.

1.5.2 Un peu d'infinité

Définition 1.95 (ensemble Dedekind infini).

Un ensemble est **infini** s'il peut être mis en bijection avec un de ses sous-ensembles propres (c'est-à-dire différent de lui-même).

Un ensemble est **fini** si il n'est pas infini.

1.96.

Nous adoptons les notions d'ensembles finis et infinis au sens de Dedekind. De nombreuses sources (dont wikipédia [18, 19]) définissent un ensemble fini comme étant un ensemble en bijection avec une partie de $\mathbb{N}$ de la forme $\{0, \dots, N\}$. Alors un ensemble est infini si il n'est pas fini.

Cependant, d'une part les deux définitions d'ensembles infinis ne sont pas équivalentes, mais d'autre part, elles sont équivalentes si on accepte l'axiome du choix³⁶. Or le Frido accepte l'axiome

35. Voir le corolaire 1.126.

36. Et même seulement l'axiome du choix dénombrable; si vous voulez en savoir plus, lisez la page wikipédia [20].

du choix sans vergogne et sous toutes ses formes. Nous démontrerons donc, en utilisant le lemme de Zorn, qu'un ensemble A est fini (définition 1.95) si et seulement si il existe une bijection $\{0, \dots, N\} \rightarrow A$ pour un certain $N \in \mathbb{N}$. Ce sera le théorème 1.103.

Lemme 1.97.

Toute partie d'un ensemble fini est finie.

Démonstration. Nous allons prouver la contraposée : si un ensemble contient une partie infinie, alors il est infini. Soit $A \subset B$ où A est infini. Nous allons prouver que B est infini. En vertu de la définition 1.95, existe une partie $A' \subsetneq A$ et une bijection $\sigma: A' \rightarrow A$.

Nous considérons la partie $B' = A' \cup (B \setminus A)$, qui est une partie stricte de B . Vu que $A' \cap (B \setminus A) = \emptyset$, nous pouvons définir

$$\begin{aligned} \varphi: B' &\rightarrow B \\ x &\mapsto \begin{cases} \sigma(x) & \text{si } x \in A' \\ x & \text{si } x \in B \setminus A. \end{cases} \end{aligned} \quad (1.154)$$

Montrons que φ est une bijection.

Surjectif Nous avons $\varphi(A') = A$ et $\varphi(B \setminus A) = B \setminus A$. Donc

$$\varphi(B') = \varphi(A') \cup \varphi(B \setminus A) = A \cup (B \setminus A) = B. \quad (1.155)$$

Injectif Si $\varphi(x) = \varphi(y)$, nous avons 4 possibilités suivant que x et y sont dans A' ou $B \setminus A$.

Si $x, y \in A'$, alors $\varphi(x) = \varphi(y)$ implique $\sigma(x) = \sigma(y)$ et donc $x = y$ parce que σ est injective.

Si $x \in A'$ et $y \in B \setminus A$ alors $\varphi(x) = \sigma(x) \in A$ et $\varphi(y) = y \in B \setminus A$. Ce cas n'est pas possible. Le cas $x \in B \setminus A$ et $y \in A'$ n'est pas possible non plus.

Si $x, y \in B \setminus A$, alors $\varphi(x) = \varphi(y)$ implique immédiatement $x = y$.

Nous avons une bijection entre B' et B alors que B' est un sous-ensemble strict de B . Donc B est infini. $\square$

Proposition 1.98 ([1]).

Si A est fini et si $\omega \notin A$, alors $A \cup \{\omega\}$ est fini.

Démonstration. Supposons que $A \cup \{\omega\}$ est infini. Il existe un sous-ensemble strict de $A \cup \{\omega\}$ en bijection avec $A \cup \{\omega\}$. Soient donc $B \subsetneq A \cup \{\omega\}$ et $\sigma: B \rightarrow A \cup \{\omega\}$ une bijection.

Il y a deux possibilités : soit ω est dans B , soit non.

$\omega \notin B$ Alors $B \subset A$, et il existe $x \in B$ tel que $\sigma(x) = \omega$. Considérons $B' = B \setminus \{x\}$; cela est une partie propre de A . Ensuite nous définissons

$$\begin{aligned} \varphi: B \setminus \{x\} &\rightarrow A \\ a &\mapsto \sigma(a). \end{aligned} \quad (1.156)$$

C'est injectif parce que σ est injective, et c'est surjectif parce que

$$\varphi(B \setminus \{x\}) = \sigma(B) \setminus \{\omega\} = \sigma(B) \setminus \{\omega\} = (A \cup \{\omega\}) \setminus \{\omega\} = A. \quad (1.157)$$

Pour la dernière égalité nous avons utilisé le fait que ω n'est pas dans A .

Si $\omega \in B$ Vu que B est une partie propre de $A \cup \{\omega\}$, il existe $x \in A \setminus B$. Nous considérons $B' = (B \setminus \{\omega\}) \cup \{x\}$ et nous définissons

$$\begin{aligned} \varphi: B' &\rightarrow A \\ b &\mapsto \begin{cases} \sigma(b) & \text{si } b \neq x \\ \sigma(\omega) & \text{si } b = x. \end{cases} \end{aligned} \quad (1.158)$$

Nous montrons à présent que φ est une bijection.

Injectif Soient u, v tels que $\varphi(u) = \varphi(v)$. Il y a 4 possibilités suivant que u ou v est égal à x .

Si $u = v = x$ on est bon.

Si $u = x$ et $v \neq x$, alors $\varphi(u) = \sigma(\omega)$ et $\varphi(v) = \sigma(v)$. Mais $x \neq \omega$ parce que $x \in A$, donc cette situation n'est pas possible parce que σ est injective.

Si $u \neq x$ et $v \neq x$, alors $\varphi(u) = \sigma(u)$ et $\varphi(v) = \sigma(v)$. Dans ce cas l'injectivité de σ fait que $x = y$.

Surjective Soit $y \in A$. Vu que $\sigma: B \rightarrow A \cup \{\omega\}$ est surjective, il existe $b \in B$ tel que $\sigma(b) = y$. Si $b \neq \omega$ alors $\varphi(b) = \sigma(b) = y$. Si au contraire $b = \omega$, alors $\varphi(x) = \sigma(\omega) = y$. Dans les deux cas, y est dans l'image de φ .

Dans tous les cas nous avons construit une bijection entre une partie propre $B \subsetneq A \cup \{\omega\}$ et $A \cup \{\omega\}$. $\square$

La proposition suivante est à peu près prise comme définition d'un ensemble fini dans [21] qui donne également une preuve de l'équivalence avec notre définition.

Proposition 1.99.

L'ensemble $\mathbb{N}$ est infini³⁷.

Démonstration. Nous considérons la partie propre³⁸

$$A = \{n \in \mathbb{N} \text{ tel que } n \geq 1\}. \quad (1.159)$$

Ensuite nous posons

$$\begin{aligned} \sigma: \mathbb{N} &\rightarrow A \\ x &\mapsto s(x). \end{aligned} \quad (1.160)$$

Le fait que σ prenne ses valeurs dans A est parce que s prend ses valeurs dans $\mathbb{N} \setminus \{0\} = A$.

σ est injective Parce que s l'est.

σ est surjective C'est dans la définition 1.32(2)

Nous avons donc une bijection entre $\mathbb{N}$ et un sous-ensemble strict. $\square$

Lemme 1.100.

Soit $N \in \mathbb{N}$. La partie $\{0, \dots, N\}$ est finie.

Démonstration. Par récurrence sur N . Avec $N = 0$, la partie $\{0\}$ est finie parce que son seul sous-ensemble propre est $\emptyset$ qui n'est pas en bijection avec $\{0\}$.

Supposons que $\{0, \dots, N\}$ est fini. Alors $\{0, \dots, N\} \cup \{N+1\}$ est fini par le lemme 1.98. $\square$

Proposition 1.101 ([1]).

Si A est infini et si $\sigma: A \rightarrow B$ est injective, alors B est infini.

Démonstration. Nous allons prouver que $\sigma(A)$ est une partie infinie de B . Vu que A est infini, nous pouvons considérer une partie $A' \subsetneq A$ et une bijection $\varphi_A: A' \rightarrow A$. Nous définissons

$$\begin{aligned} \varphi_B: \sigma(A') &\rightarrow \sigma(A) \\ y &\mapsto \sigma\left(\varphi\left(\sigma^{-1}(y)\right)\right). \end{aligned} \quad (1.161)$$

Cette définition a un sens parce que si $y \in \sigma(A')$, alors il existe un unique $x \in A'$ tel que $\sigma(x) = y$ parce que σ est injective. De là, $\varphi_A(x) \in A$ et nous pouvons lui appliquer σ .

Nous montrons que φ_B est une bijection.

37. Définition 1.95.

38. Le fait que ce soit une partie propre est dû au fait que 0 n'est pas dedans d'une part parce que le lemme 1.45 dit que $0 \leq 1$, et d'autre part parce que le lemme 1.43 donne $0 \neq 1$.

Injective Supposons que $\varphi_B(a) = \varphi_B(b)$, c'est à dire que

$$(\sigma \circ \varphi_A \circ \sigma^{-1})(a) = (\sigma \circ \varphi_A \circ \sigma^{-1})(b). \quad (1.162)$$

Étant donné que σ et φ_A sont injectives, nous avons $\sigma^{-1}(a) = \sigma^{-1}(b)$. En appliquant σ des deux côtés, nous trouvons $a = b$.

surjective Soit $y \in \sigma(A)$. En prenant $x \in (\sigma \circ \varphi_A^{-1} \circ \sigma^{-1})(y)$ nous avons $\varphi_B(x) = y$.

Donc B contient une partie infinie $(\sigma(A))$. Le lemme 1.97 conclut que B est infini. $\square$

Lemme 1.102.

À propos d'applications entre ensembles finis.

- (1) Si $\sigma: A \rightarrow B$ est une application quelconque et si A est fini, alors $\sigma(A)$ est une partie finie de B .
- (2) Si $\sigma: A \rightarrow B$ est surjective et si A est fini, alors B est fini.

Démonstration. Nous allons utiliser le lemme de Zorn. Nous considérons l'ensemble

$$\mathcal{A} = \{X \subset A \text{ tel que } \sigma: X \rightarrow \sigma(A) \text{ est injective}\} \quad (1.163)$$

que nous ordonnons (partiellement) par l'inclusion.

$\mathcal{A}$ est inductif Soit une partie totalement ordonnée $\mathcal{F}$ de $\mathcal{A}$. Nous considérons $Y = \bigcup_{X \in \mathcal{F}} X$, et nous prouvons que Y est un majorant de $\mathcal{F}$.

Pour cela nous commençons par prouver que $Y \in \mathcal{A}$. Soient $a, b \in Y$ tels que $\sigma(a) = \sigma(b)$. Il existe $X_1, X_2 \in \mathcal{F}$ tels que $a \in X_1$ et $b \in X_2$. Supposons pour fixer les idées que $X_1 \leq X_2$ ($\mathcal{F}$ étant totalement ordonné nous avons toujours $X_1 \leq X_2$ ou $X_2 \leq X_1$). Vu que l'ordre est l'inclusion, cela signifie que $X_1 \subset X_2$. Nous avons donc $a, b \in X_2$, alors que σ est injective sur X_2 . Donc $\sigma(a) = \sigma(b)$ implique $a = b$, et σ est injective sur Y . Nous avons donc prouvé que $Y \in \mathcal{A}$.

Vu que pour tout $X \in \mathcal{F}$ nous avons $X \subset Y$, nous avons $X \leq Y$ (dans $\mathcal{A}$) pour tout $X \in \mathcal{F}$. Bref, Y est un majorant de $\mathcal{F}$ dans $\mathcal{A}$.

Toute partie totalement ordonnée de $\mathcal{A}$ est majorée. Cela signifie que $\mathcal{A}$ est inductif³⁹.

Zorn L'ensemble $\mathcal{A}$ étant inductif et non vide (les singletons dans A sont dans $\mathcal{A}$), il possède un maximum par le lemme de Zorn 1.17. Nous nommons A' un élément maximum dans $\mathcal{A}$.

Bijective L'application $\sigma: A' \rightarrow \sigma(A)$ est injective parce que $A' \in \mathcal{A}$. Nous devons prouver qu'elle est surjective.

Supposons que $y \in \sigma(A) \setminus \sigma(A')$. Alors il existe $a \in A \setminus A'$ tel que $\sigma(a) = y$. Dans ce cas, la partie $A' \cup \{a\}$ est un majorant de A' dans $\mathcal{A}$, ce qui est impossible.

Donc $\sigma: A' \rightarrow \sigma(A)$ est bijective.

Conclusion L'ensemble A' est fini en tant que partie de l'ensemble fini A (lemme 1.97). L'application σ étant injective, la proposition 1.101 conclut que $\sigma(A')$ est fini. Et comme $\sigma(A')$ n'est autre que $\sigma(A)$ nous avons fini.

La partie (1) est prouvée. La partie (2) est maintenant facile. La partie (1) dit que $\sigma(A)$ est une partie finie de B , mais si σ est surjective, alors $\sigma(A) = B$. $\square$

Proposition-Définition 1.103 (Cardinal d'un ensemble fini[1]).

Un ensemble est fini si et seulement si il est en bijection avec $\{0, \dots, N\}$ pour un certain N .

Dans ce cas, le nombre $N + 1$ est le **cardinal** de I , et est noté $\text{Card}(I)$.

39. Plus précisément c'est l'ensemble ordonné $(\mathcal{A}, \subset)$ qui est inductif.

Démonstration. Soit un ensemble A en bijection avec $\{0, \dots, N\}$. Nous avons vu que $\{0, \dots, N\}$ est fini dans le lemme 1.100. Le lemme 1.102(2) conclut que A est fini.

Le vrai sport est de faire l'implication inverse. Nous supposons que A est un ensemble fini, et nous allons prouver qu'il est en bijection avec $\{0, \dots, N\}$ pour un N bien choisit. Nous allons utiliser le lemme de Zorn. Soit

$$\mathcal{A} = \{(N, \varphi) \text{ tel que } \varphi: \{0, \dots, N\} \rightarrow A \text{ est injective}\}. \quad (1.164)$$

Nous mettons sur $\mathcal{A}$ la relation d'ordre donnée par $(N_1, \varphi_1) \leq (N_2, \varphi_2)$ lorsque

- (1) $N_1 \leq N_2$
- (2) φ_2 étend φ_1 , c'est à dire que $\varphi_2 = \varphi_1$ sur $\{0, \dots, N_1\}$.

A est inductif Soit une partie $\mathcal{F}$ totalement ordonnée de $\mathcal{A}$. Nous considérons la partie suivante de $\mathbb{N}$:

$$S = \{n \in \mathbb{N} \text{ tel que } \exists (n, \varphi) \in \mathcal{F}\}. \quad (1.165)$$

Si S est majoré, alors il a un maximum (proposition 1.51(4)). Si M est le maximum de S , le (M, φ) de $\mathcal{F}$ qui correspond à ce maximum est un majorant de $\mathcal{F}$.

Supposons –pour l'absurde– que $\mathcal{F}$ n'est pas majoré ; en particulier S n'est pas majoré. Pour chaque $n \in S$, il existe une application φ_n telle que $(n, \varphi_n) \in \mathcal{F}$. Cela nous permet de définir

$$\begin{aligned} \phi: S &\rightarrow A \\ n &\mapsto \varphi_n(n). \end{aligned} \quad (1.166)$$

Montrons que ϕ est injective. Si $\phi(m) = \phi(n)$, alors $\varphi_m(m) = \varphi_n(n)$. Supposons pour fixer les idées que $n \leq m$. Vu que (n, φ_n) et (m, φ_m) sont dans $\mathcal{F}$ qui est ordonné, φ_m prolonge φ_n ; en particulier $\varphi_n(n) = \varphi_m(n)$. Mais comme φ_m est injective, $m = n$.

Nous avons donc une injection $\phi: S \rightarrow A$. Mais S est non borné et donc infini⁴⁰. La proposition 1.101 conclut que A est infini, ce qui est contraire aux hypothèses.

Donc $\mathcal{F}$ a un majorant et $\mathcal{A}$ est inductif.

Lemme de Zorn Le lemme de Zorn dit que $\mathcal{A}$ a un maximum.

Conclusion Soit (N, φ) un maximum de $\mathcal{A}$. Nous allons prouver que $\varphi: \{0, \dots, N\} \rightarrow A$ est une bijection. Que φ soit injective est une conséquence du fait qu'elle est dans $\mathcal{A}$.

Pour prouver que φ est surjective, nous supposons qu'elle ne l'est pas. Soit $a \in A$ qui n'est pas dans l'image de φ . En posant

$$\begin{aligned} \phi: \{0, \dots, N+1\} &\rightarrow A \\ x &\mapsto \begin{cases} \varphi(x) & \text{si } x \neq N+1 \\ a & \text{si } x = N+1, \end{cases} \end{aligned} \quad (1.167)$$

le couple $(N+1, \phi)$ majore strictement (N, φ) . Cela est une contradiction.

□

Nous ne définissons pas ce qu'est le cardinal d'un ensemble infini ; c'est très compliqué et ça ne nous servira pas.

Lemme 1.104 ([1]).

Union d'ensembles finis.

- (1) Si A et B sont des ensembles finis disjoints, alors $A \cup B$ est fini et

$$\text{Card}(A \cup B) = \text{Card}(A) + \text{Card}(B). \quad (1.168)$$

40. Le lemme 1.55 dit qu'il existe une bijection entre S et $\mathbb{N}$. De là nous concluons que S est infini parce qu'un ensemble en bijection avec un ensemble infini est infini par la proposition 1.101.

(2) Si A et B sont des ensembles finis, alors $A \cup B$ est fini.

(3) Si A est fini et si $B \subset A$ alors

$$\text{Card}(A \setminus B) = \text{Card}(A) - \text{Card}(B). \quad (1.169)$$

(4) Si A et B sont des ensembles, alors

$$\text{Card}(A \cup B) = \text{Card}(A) + \text{Card}(B) - \text{Card}(A \cap B). \quad (1.170)$$

(5) Si les $\{A_i\}_{i=1, \dots, n}$ sont des ensembles, alors

$$\text{Card}\left(\bigcup_{i=1}^n A_i\right) = \sum_{i=1}^n \text{Card}(A_i). \quad (1.171)$$

(6) Si I ou J est infini, alors $I \cup J$ est infini.

Démonstration. Point par point.

Pour (1) Vu que A et B sont finis, la proposition 1.103 nous dit qu'il existe des naturels N et M ainsi que des bijections $\varphi_A: \{0, \dots, N\} \rightarrow A$ et $\varphi_B: \{0, \dots, M\} \rightarrow B$. Maintenant l'application

$$\begin{aligned} \varphi: \{0, \dots, M+N+1\} &\rightarrow A \cup B \\ n &\mapsto \begin{cases} \varphi_A(n) & \text{si } n \leq N \\ \varphi_B(n - N - 1) & \text{si } n > N \end{cases} \end{aligned} \quad (1.172)$$

est une bijection. Le fait que A et B soient disjoints est important pour l'injectivité. La proposition 1.103 nous dit qu'alors $A \cup B$ est fini. De plus, par définition le cardinal de $A \cup B$ est $N + M$.

Pour (2) Nous ne supposons plus que A et B sont disjoints. Nous posons $I = A$ et $J = B \setminus A$. Avec ça, I et J sont disjoints et finis (comme parties des ensembles finis, lemme 1.97), et vérifient $I \cup J = A \cup B$. Le point (1) indique que $I \cup J$ est fini.

Pour (3) L'ensemble A peut être écrit sous la forme d'une union disjointe : $A = B \cup (A \setminus B)$. Les ensembles B et $A \setminus B$ étant disjoints, nous avons

$$\text{Card}(A) = \text{Card}(B) + \text{Card}(A \setminus B). \quad (1.173)$$

Pour (4) Nous utilisons quelques égalités d'ensembles pour ramener $A \cup B$ à des cas déjà traités :

$$A \cup B = A \cup (B \setminus A) = A \cup (B \setminus (A \cap B)). \quad (1.174)$$

Nous avons en particulier utilisé $B \setminus A = B \setminus (A \cap B)$. La chose intéressante dans (1.174) est que l'union est disjointe et que $A \cap B \subset B$. Nous pouvons donc écrire

$$\text{Card}(A \cup B) = \text{Card}(A) + \text{Card}(B \setminus (A \cap B)) = \text{Card}(A) + \text{Card}(B) - \text{Card}(A \cap B). \quad (1.175)$$

Pour (5) Récurrence en utilisant le point (4).

Pour (6) Toute partie d'un ensemble fini est finie (lemme 1.97). Donc si $I \cup J$ était fini, I et J devraient l'être.

□

Définition 1.105.

Un ensemble est **dénombrable** s'il peut être mis en bijection avec $\mathbb{N}$. Il est **non dénombrable** s'il est infini et ne peut pas être mis en bijection avec $\mathbb{N}$.

Une chose vraiment amusante avec cette définition que l'on met en rapport avec la définition 1.95, c'est qu'un ensemble fini n'est ni dénombrable ni non dénombrable⁴¹.

41. Beaucoup de sources disent qu'un ensemble est dénombrable lorsqu'il est en bijection avec une partie de $\mathbb{N}$. Cela laisse la porte ouverte aux ensembles finis. Par exemple Wikipédia[22].

Lemme 1.106.

Si A est dénombrable et si il existe une surjection $f: A \rightarrow B$, alors B est fini ou dénombrable.

Lemme 1.107.

Si A est un ensemble fini ou dénombrable, alors il existe une surjection $\mathbb{N} \rightarrow A$.

1.5.3 Dénombrabilité et ensemble des naturels**Proposition 1.108** ([1, 13]).

Toute partie infinie de $\mathbb{N}$ est dénombrable.

Démonstration. Soit A , une partie infinie de $\mathbb{N}$.

Définition de σ Nous voulons construire une application $\sigma: \mathbb{N} \rightarrow A$ telle que

$$\begin{cases} \sigma(0) = \min(A) & (1.176a) \\ \sigma(k+1) = \min(A \setminus \sigma(\{0, \dots, k\})) & (1.176b) \end{cases}$$

Les lâches, par prudence, diront juste que c'est défini par récurrence et n'insisteront pas. Nous, nous insistons.

Nous allons définir $\sigma(n)$ à l'aide du théorème 1.36. Pour cela nous posons $E = \mathcal{P}(A)$, $b = \emptyset$ et

$$\begin{aligned} g: E &\rightarrow E \\ Z &\mapsto \begin{cases} A & \text{si } Z = A \\ Z \cup \{\min(A \setminus Z)\} & \text{sinon.} \end{cases} \end{aligned} \quad (1.177)$$

Notons que la proposition 1.51(2) nous indique que toute partie non vide de $\mathbb{N}$ possède un minimum ; la définition de g a donc un sens. Le théorème 1.36 donne alors une application $f: \mathbb{N} \rightarrow E$ telle que

- (1) $f(0) = b = \emptyset$
- (2) $f(n+1) = g(f(n))$ pour tout $n \geq 0$.

Prouvons par récurrence que $f(n)$ est un ensemble fini pour tout n . D'abord $f(0) = \emptyset$. Ensuite, si $n \geq 0$ est tel que $f(n)$ est fini, alors en particulier $f(n) \neq A$ et nous avons

$$f(n+1) = g(f(n)) = f(n) \cup \{\min(A \setminus f(n))\}. \quad (1.178)$$

Dans ce cas, $f(n+1)$ est également fini comme union de deux ensembles finis.

Nous posons

$$\sigma(n) = \min(A \setminus f(n)). \quad (1.179)$$

Avec $n = 0$, nous avons $\sigma(0) = \min(A \setminus \emptyset) = \min(A)$. La condition (1.176a) est donc déjà satisfaite.

Nous devons encore prouver (1.176b). Pour tout n , la relation entre $f(n)$ et $\sigma(n)$ est donnée par

$$\begin{cases} f(0) = \emptyset & (1.180a) \\ f(n+1) = f(n) \cup \sigma(n). & (1.180b) \end{cases}$$

Par récurrence nous avons alors

$$f(n) = \bigcup_{k=0}^{n-1} \{\sigma(k)\} = \sigma(\{0, \dots, n-1\}) \quad (1.181)$$

pour tout $n \geq 1$. Nous avons alors la condition 1.176b en substituant (1.181) dans la définition (1.179) écrite avec $n+1$:

$$\sigma(n+1) = \min(A \setminus f(n+1)) = \min(A \setminus \sigma(\{0, \dots, n\})). \quad (1.182)$$

σ est strictement croissante Vu que $A \setminus \sigma\{0, \dots, k\} \subset A \setminus \sigma\{0, \dots, k-1\}$, le minimum est plus grand ou égal : $\sigma(k+1) \geq \sigma(k)$. Mais $\sigma(k+1)$ est sélectionné dans l'ensemble $A \setminus \sigma\{0, \dots, k\}$, qui ne contient justement pas $\sigma(k)$. Donc $\sigma(k+1) \neq \sigma(k)$.

σ est définie sur $\mathbb{N}$ Il faut montrer que pour tout k , l'ensemble $A \setminus \sigma\{0, \dots, k\}$ est non vide. Si il l'était, cela signifierait que $A \subset \sigma\{0, \dots, k\}$. Par le lemme 1.102(1), la partie $\sigma\{0, \dots, k\}$ est finie dans $\mathbb{N}$. Le lemme 1.97 dit alors qu'en tant que partie de $\sigma\{0, \dots, k\}$, l'ensemble A est fini. Mais comme les hypothèses disent que A est infini, nous avons une contradiction et nous concluons que σ est bien définie sur tout $\mathbb{N}$.

σ est injective Une application $\mathbb{N} \rightarrow \mathbb{N}$ strictement croissante est injective par la proposition 1.54.

σ est surjective Soit $a \in A$. Vu que σ est strictement croissante et que $\sigma(0) \geq 0$, nous avons $\sigma(a) \geq a$. Si $\sigma(a) = a$ nous avons terminé. Supposons $\sigma(a) > a$. Alors

$$\min(A \setminus \sigma\{0, \dots, a\}) > a. \quad (1.183)$$

Si $\sigma(\{0, \dots, a\})$ ne contenait pas a , alors $A \setminus \sigma(\{0, \dots, a\})$ le contiendrait et nous n'aurions pas l'inégalité (1.183). Donc $a \in \sigma(\{0, \dots, a\})$ et a est bien dans l'image de σ .

□

1.109.

La proposition 1.108 pourrait être prouvée plus facilement en acceptant le théorème de Cantor-Schröder-Bernstein 1.121. Il existe une injection $A \rightarrow \mathbb{N}$ parce que A est une partie de $\mathbb{N}$. Mais vu que A est infini, il possède une partie dénombrable. Cela donne une surjection $A \rightarrow \mathbb{N}$ et donc une injection $\mathbb{N} \rightarrow A$. Le théorème de Cantor-Schröder-Bernstein conclu.

Cela dit, une telle preuve demanderait des outils plus complexes.

1.110.

La proposition suivante donne une bijection explicite entre $\mathbb{N}$ et $\mathbb{N} \times \mathbb{N}$. Elle n'a rien de transcendante, mais je ne résiste pas à la donner ici parce qu'elle est utilisée dans l'article *Un peu de programmation transfinie* de David Madore⁴². Son utilité est de pouvoir créer un langage de programmation pouvant traiter des paires d'entiers rien qu'en traitant des entiers.

Proposition 1.111 (Une bijection $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$).

La fonction

$$f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$$

$$(x, y) \mapsto \begin{cases} y^2 + x & \text{si } x < y \\ x^2 + x + y & \text{si } y \leq x. \end{cases} \quad (1.184)$$

est une bijection.

Démonstration. Il s'agit de prouver qu'elle est injective et surjective. Dans la suite, tous les nombres sont des entiers positifs.

f est injective Pour $k \in \mathbb{N}$ donné, nous allons prouver que

- (1) l'équation $f(x, y) = k$ possède au maximum une solution avec $x < y$,
- (2) l'équation $f(x, y) = k$ possède au maximum une solution avec $y \leq x$,
- (3) si $k = y^2 + x$ avec $x < y$ alors il est impossible que $k = x'^2 + x' + y'$ avec $y' \leq x'$.

On y va.

42. Et comme j'aime beaucoup cet article, il me fallait une excuse pour le placer ici.

<http://www.madore.org/~david/weblog/d.2017-08-18.2460.html>.

- (1) Nous supposons $y^2 + x = t^2 + z$ avec $x < y$ et $z < t$. Pour fixer les idées, nous supposons $t > y$ et nous posons $t = y + s$ ($s \geq 1$). En substituant, et en isolant z ,

$$z = x - 2sy - s^2 \quad (1.185a)$$

$$< x - 2sy \quad (1.185b)$$

$$< x - 2sx \quad (1.185c)$$

$$= x(1 - 2s) \quad (1.185d)$$

$$< 0. \quad (1.185e)$$

Impossible parce que $z \geq 0$.

- (2) De même nous supposons $x^2 + x + y = z^2 + z + t$ avec $y \leq x$ et $t \leq z$. Nous posons $z = x + s$, et nous déballons le même genre de calculs en isolant t .
- (3) Enfin nous supposons $y^2 + x = z^2 + z + t$ avec $x < y$ et $t \leq z$. Les plus courageux diviseront en trois cas : $y < z$, $y = z$ et $y > z$ et feront les calculs. Par exemple, pour le cas $y > z$ nous posons $y = z + s$ et nous substituons :

$$(y + s)^2 + x = z^2 + z + t \quad (1.186)$$

qui donne

$$x = z + t - 2zs - s^2 < 2z - 2zs - s^2 = 2z(1 - s) - s^2 \leq -s < 0 \quad (1.187)$$

parce que $s \geq 1$, donc $1 - s \leq 0$.

f est surjective Nous devons prouver que tous les éléments de $\mathbb{N}$ sont dans l'image de $\mathbb{N} \times \mathbb{N}$ par f . En premier lieu, $0 = f(0, 0)$. C'est un bon début. Soit $a \in \mathbb{N}$ non nul ; nous montrons que tous les nombres de a^2 à $(a + 1)^2$ sont des images de f . D'abord $a^2 = f(0, a)$, ensuite les nombres

$$f(1, a), f(2, a), \dots, f(a - 1, a) \quad (1.188)$$

prennent les valeurs $a^2 + 1, \dots, a^2 + a - 1$. Enfin nous avons $f(a, 0) = a^2 + a$ et les nombres $f(a, 1), \dots, f(a, a)$ prennent les valeurs de $a^2 + a + 1$ à $a^2 + 2a = (a + 1)^2 - 1$.

□

Sachez que cette fonction s'étend aux ordinaux (mais là ce n'est plus pour rigoler).

Corolaire 1.112.

Il existe des parties $\{\mathbb{N}_i\}_{i \in \mathbb{N}}$ telles que $\bigcup_{i \in \mathbb{N}} \mathbb{N}_i = \mathbb{N}$ et que chaque $\mathbb{N}_i$ soit en bijection avec $\mathbb{N}$

Démonstration. Nous considérons la bijection $f: \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$ donnée par (l'inverse de celle donnée) par la proposition 1.111, et nous posons

$$\mathbb{N}_i = f^{-1}(i, \mathbb{N}). \quad (1.189)$$

L'application

$$f: \mathbb{N}_i \rightarrow \{(i, k)\}_{k \in \mathbb{N}} \quad (1.190)$$

est une bijection. Or l'ensemble $\{(i, k)\}_{k \in \mathbb{N}}$ est évidemment en bijection avec $\mathbb{N}$. Par composition nous avons le résultat. □

Lemme 1.113 ([1]).

Si il existe une surjection $\mathbb{N} \rightarrow A$, alors A est fini ou dénombrable.

Démonstration. Pour chaque $a \in A$, l'ensemble $f^{-1}(a)$ est une partie de $\mathbb{N}$.

Une application La proposition 1.51(2) nous permet de poser

$$\begin{aligned} \sigma: A &\rightarrow \mathbb{N} \\ a &\mapsto \min(f^{-1}(a)). \end{aligned} \quad (1.191)$$

σ est injective Supposons que $\sigma(a) = \sigma(b)$. Nous appelons x ce nombre :

$$x = \min(f^{-1}(a)) = \min(f^{-1}(b)). \quad (1.192)$$

Nous avons $x \in f^{-1}(a) \cap f^{-1}(b)$, ce qui implique que $f(x) = a$ et que $f(x) = b$; donc $a = b$.
Donc σ est une injection.

A est infini Si A est fini, le lemme est prouvé. Donc à partir de maintenant nous supposons que A est infini. Le but est de prouver qu'il est dénombrable, c'est à dire de construire une bijection $A \rightarrow \mathbb{N}$.

$\sigma(A)$ est dénombrable Vu que $\sigma: A \rightarrow \mathbb{N}$ est injective et que A est infini, la proposition 1.101 dit que $\sigma(A)$ est infini dans $\mathbb{N}$. La proposition 1.108 nous dit alors que $\sigma(A)$ est dénombrable. Soit une bijection $\varphi: \sigma(A) \rightarrow \mathbb{N}$.

La candidate bijection Nous posons

$$f = \varphi \circ \sigma: A \rightarrow \mathbb{N} \quad (1.193)$$

et nous allons prouver que c'est une bijection.

Injective Vu que φ et σ sont injectives, l'égalité $(\varphi\sigma)(a) = (\varphi\sigma)(b)$ implique immédiatement $a = b$.

Surjective Soit $k \in \mathbb{N}$. Vu que φ et σ sont des injections, nous pouvons poser $a = (\sigma^{-1}\varphi^{-1})(k)$. Il est alors immédiat que $f(a) = k$.

□

Proposition 1.114 ([1, 22]).

Une union dénombrable d'ensembles finis ou dénombrables est finie ou dénombrable.

Démonstration. Soient A_i des ensembles finis ou dénombrables. Nous posons $A = \bigcup_{i \in \mathbb{N}} A_i$, et nous considérons les parties $\mathbb{N}_i$ du corolaire 1.112. Vu que A_i est dénombrable ou fini et que $\mathbb{N}_i$ est dénombrable, il existe une surjection $\varphi_i: \mathbb{N}_i \rightarrow A_i$.

Nous définissons $s: \mathbb{N} \rightarrow \mathbb{N}$ par $n \in \mathbb{N}_{s(n)}$, et nous posons enfin

$$\begin{aligned} \varphi: \mathbb{N} &\rightarrow A \\ n &\mapsto \varphi_{s(n)}(n). \end{aligned} \quad (1.194)$$

Nous prouvons que φ est surjective.

Soit $a \in A_i$. Il existe $n \in \mathbb{N}_i$ tel que $a = \varphi_i(n)$. Mais comme $n \in \mathbb{N}_i$, nous avons $s(n) = i$. Donc

$$a = \varphi_i(n) = \varphi_{s(n)}(n) = \varphi(n). \quad (1.195)$$

Donc $\varphi: \mathbb{N} \rightarrow A$ est surjective.

Le lemme 1.113 conclu que A est fini ou dénombrable. □

Lemme 1.115 ([1]).

Si N est un ensemble dénombrable, alors il existe une bijection $g: \{1, 2\} \times N \rightarrow N$.

Démonstration. D'abord nous définissons une bijection $\varphi: \{0, 1\} \times \mathbb{N} \rightarrow \mathbb{N}$ par

$$\begin{aligned} \varphi: \{0, 1\} \times \mathbb{N} &\rightarrow \mathbb{N} \\ (n, k) &\mapsto 2k + n. \end{aligned} \quad (1.196)$$

Ensuite si $f: \mathbb{N} \rightarrow N$ est une bijection, il suffit de poser $g(n, k) = f(\varphi(n, k))$. □

Proposition 1.116 ([22]).

Si N est un ensemble dénombrable, alors pour tout $n \in \mathbb{N}$, l'ensemble N^n est dénombrable.

Les ensembles dénombrables sont les plus petits ensembles infinis possibles, comme en témoigne la proposition suivante.

Proposition 1.117.

Tout ensemble infini contient une partie en bijection avec $\mathbb{N}$.

Démonstration. Soient un ensemble infini E_0 et une partie propre E_1 en bijection avec E_0 . Nous notons $\varphi: E_0 \rightarrow E_1$ une bijection.

Soit $x_0 \in E_0 \setminus E_1$ (axiome du choix et tout ça). Nous définissons

$$\begin{aligned} \psi: \mathbb{N} &\rightarrow \{\varphi^k(x_0)\} \\ n &\mapsto \varphi^n(x_0) \end{aligned} \quad (1.197)$$

et nous allons prouver que c'est une bijection. Que ce soit surjectif est immédiat. Pour l'injectivité, soit $\varphi^k(x_0) = \varphi^l(x_0)$ avec $k \neq l$. Supposons pour fixer les notations que $k > l$. Alors, vu que φ est inversible nous pouvons écrire

$$x_0 = \varphi^{k-l}(x_0) = \varphi(\varphi^{k-l-1}(x_0)) \quad (1.198)$$

où il est entendu que $\varphi^0(x_0) = x_0$. Cela signifie que x_0 est dans l'image de φ , c'est-à-dire dans E_1 , ce que nous avons exclu par choix de x_0 dans $E_0 \setminus E_1$. Donc en réalité $\varphi^k(x_0) \neq \varphi^l(x_0)$ dès que $k \neq l$. $\square$

Proposition 1.118.

Toute partie d'un ensemble fini est finie, et toute partie d'un ensemble dénombrable est finie ou dénombrable.

Lemme 1.119.

Soit un ensemble E non dénombrable ainsi qu'une application $f: E \rightarrow F$ où F est un ensemble quelconque. Si $f(E)$ est dénombrable (ou fini), alors il existe $y \in f(E)$ tel que $f^{-1}(y)$ est indénombrable.

Démonstration. Nous avons

$$E = \bigcup_{y \in F} f^{-1}(y). \quad (1.199)$$

Si tous les $f^{-1}(y)$ sont dénombrables, alors E est une union dénombrable (F est dénombrable) d'ensembles dénombrables. Il serait donc dénombrable (proposition 1.114), ce qui est contraire à l'hypothèse. $\square$

1.5.4 Théorème de Cantor-Schröder-Bernstein

Lemme 1.120 ([23]).

Soient un ensemble A et une partie B de A . Si il existe une injection $f: A \rightarrow B$ alors il existe une bijection $\alpha: A \rightarrow B$.

Nous donnons deux preuves de ce lemme.

Première preuve de 1.120. Nous posons $Y = A \setminus B$ et nous décomposons la preuve en étapes.

Les $f^k(Y)$ sont disjoints Vu que f prend ses valeurs dans B , nous avons $f^k(Y) \subset B$ pour tout k . Et vu que $Y = A \setminus B$, nous avons

$$f^k(Y) \cap Y = \emptyset \quad (1.200)$$

pour tout k . L'application f étant injective, elle vérifie $f(C \cap D) = f(C) \cap f(D)$. Nous appliquons f^m des deux côtés de (1.200) :

$$f^{k+m}(Y) \cap f^m(Y) = \emptyset \quad (1.201)$$

pour tout $k, m \in \mathbb{N}$.

Une décomposition Nous posons

$$X = \bigcup_{k \in \mathbb{N}} f^k(Y) = Y \cup \bigcup_{k=1}^{\infty} f^k(Y). \quad (1.202)$$

Vu que $f(X) \subset B$ nous avons l'égalité

$$B = f(X) \cup (B \setminus f(X)). \quad (1.203)$$

$A \setminus X = B \setminus f(X)$ Supposons $x \in A \setminus X$. Vu que $Y = A \setminus B$ est dans X , l'élément x n'est pas dans $A \setminus B$ et donc est dans B parce qu'il est dans A . Mais x n'est pas dans X et en particulier pas dans $f(X)$ parce que $f(X) \subset X$. Donc x est dans $B \setminus f(X)$.

Dans l'autre sens, nous supposons que $x \in B \setminus f(X)$. Vu que $B \subset A$ nous avons $x \in A$. Comme x est hors de $f(X)$, il est hors des $f^k(Y)$ pour $k \geq 1$. Mais $x \in B$, donc x est hors de $A \setminus B = f^0(Y)$. Donc x est hors de $f^k(Y)$ pour tout $k \geq 0$. Donc x est hors de X .

La bijection Nous considérons l'application

$$\alpha: A \rightarrow B$$

$$x \mapsto \begin{cases} f(x) & \text{si } x \in X \\ x & \text{si } x \in A \setminus X. \end{cases} \quad (1.204)$$

Nous démontrons dans les points suivants que α est bijective.

Injective Nous supposons $\alpha(x) = \alpha(y)$. Il y a 4 possibilités suivant que x et y soient dans X ou $A \setminus X$.

Si $x, y \in X$ alors $f(x) = f(y)$ et donc $x = y$ parce que f est injective.

Si $x \in X$ et $y \in A \setminus X$, alors $f(x) = y$. Mais $f(x) \in f(X)$ et $y \in A \setminus X = B \setminus f(X)$. Donc l'élément $f(x) = y$ est dans $f(X) \cap (B \setminus f(X)) = \emptyset$. Il n'est donc pas possible d'avoir $\alpha(x) = \alpha(y)$ avec $x \in X$ et $y \in A \setminus X$.

Si $x \in A \setminus X$ et $y \in X$, c'est la même chose.

Si $x, y \in A \setminus X$, alors $x = \alpha(x) = \alpha(y) = y$.

Surjective Soit $y \in B$. Il y a deux possibilités : $y \in X$ et $y \in A \setminus X$. La première se divise en deux : $y \in Y$ et $y \in \bigcup_{k=1}^{\infty} f^k(Y)$. On y va.

$y \in Y$ Ce cas n'est pas possible parce que $y \in B$ alors que $Y = A \setminus B$.

$y \in f^k(Y)$ avec $k \geq 1$ Nous avons

$$y \in f(f^{k-1}(Y)) \subset f(X) \subset \alpha(A). \quad (1.205)$$

$y \in A \setminus X$ Alors $y = \alpha(y)$.

□

Deuxième preuve de 1.120[13]. Nous posons $Y = A \setminus B$ et

$$\mathcal{M} = \{M \subset A \text{ tel que } Y \cup f(M) \subset M\}. \quad (1.206)$$

Nous allons dire de nombreuses choses à propos de ce $\mathcal{M}$.

$\mathcal{M}$ est non vide Nous avons $A \in \mathcal{M}$ parce que Y et $f(A)$ sont dans A .

Si $M \in \mathcal{M}$ alors $Y \subset M$ C'est dans la définition de $\mathcal{M}$.

Encore un ensemble Vu que $\mathcal{M}$ est non vide, nous pouvons poser

$$X = \bigcap_{M \in \mathcal{M}} M \quad (1.207)$$

sans nous poser trop de questions. Cela étant fait, nous pouvons passer aux choses sérieuses.

$f(X) \subset M$ pour tout $M \in \mathcal{M}$ Soit $M \in \mathcal{M}$. Nous avons

$$f(X) \subset f(M) \quad (1.208a)$$

$$\subset Y \cup f(M) \quad (1.208b)$$

$$\subset M \quad (1.208c)$$

Justifications.

— Pour (1.208a). Parce que $X \subset \mathcal{M}$.

— Pour (1.208c). Parce que $M \in \mathcal{M}$.

$X \in \mathcal{M}$ Vu que $Y \subset M$ pour tout M dans $\mathcal{M}$, nous avons $Y \subset \bigcap_{M \in \mathcal{M}} M = X$. Nous devons prouver $f(X) \subset X$. Nous venons de prouver que $f(X) \subset M$ pour tout $M \in \mathcal{M}$, donc

$$f(X) \subset \bigcap_{M \in \mathcal{M}} M = X. \quad (1.209)$$

L'ensemble X est le plus petit élément de $\mathcal{M}$ pour l'inclusion.

$Y \cup f(X) \subset X$ Ça fait partie de $X \in \mathcal{M}$. Mais c'est bien de le dire explicitement parce que nous allons l'utiliser quelque fois dans la suite.

$Y \cup f(X) \in \mathcal{M}$ Vu que $X \in \mathcal{M}$, nous savons déjà que $Y \cup f(X) \subset X$. En appliquant f des deux côtés,

$$f(Y \cup f(X)) \subset f(X). \quad (1.210)$$

En ajoutant Y des deux côtés,

$$Y \cup f(Y \cup f(X)) \subset Y \cup f(X), \quad (1.211)$$

et donc $Y \cup f(X) \in \mathcal{M}$.

$Y \cup f(X) = X$ Nous savons déjà que $Y \cup f(X) \in \mathcal{M}$. Vu que X est le plus petit élément de $\mathcal{M}$, nous avons

$$X \subset Y \cup f(X). \quad (1.212)$$

L'inclusion inverse étant déjà faite, nous avons l'égalité.

$B \setminus f(X) = A \setminus X$ Nous avons :

$$A \setminus X = A \setminus (Y \cup f(X)) \quad (1.213a)$$

$$= (A \setminus Y) \cap (A \setminus f(X)) \quad (1.213b)$$

$$= B \cap (A \setminus f(X)) \quad (1.213c)$$

$$= (B \cap A) \setminus f(X) \quad (1.213d)$$

$$= B \setminus f(X). \quad (1.213e)$$

Justifications :

— Pour (1.213b). Complémentaire de réunion, lemme 1.19(2).

— Pour (1.213c). Parce que $A \setminus Y = B$ du fait que $Y = A \setminus B$.

— Pour (1.213d). Lemme 1.19(3).

— Pour (1.213e). Parce que $B \subset A$.

Notre bijection Nous voulons définir

$$\begin{aligned} \alpha: A &\rightarrow B \\ x &\mapsto \begin{cases} f(x) & \text{si } x \in X \\ x & \text{si } x \in A \setminus X. \end{cases} \end{aligned} \quad (1.214)$$

Pour y parvenir, nous devons prouver que α prend effectivement ses valeurs dans B . Ensuite nous prouverons que α est une bijection.

α prend ses valeurs dans B Si $x \in X$ nous avons $\alpha(x) = f(x) \in B$. Si au contraire $x \in A \setminus X$ nous avons

$$\alpha(x) = x \in A \setminus X = B \setminus f(X) \subset B. \quad (1.215)$$

α est injective Soient $x, y \in A$ tels que $\alpha(x) = \alpha(y)$. Il y a quatre possibilités suivant que x et y sont dans X ou dans $A \setminus X$.

$x \in X, y \in X$ Alors $f(x) = \alpha(x) = \alpha(y) = f(y)$. Vu que f est injective, nous trouvons que $x = y$.

$x \in X, y \in A \setminus X$ Nous avons $\alpha(x) = f(x) \in f(X)$ et $\alpha(y) = y \in A \setminus X = B \setminus f(X)$. Il n'est donc pas possible d'avoir $\alpha(x) = \alpha(y)$ dans ce cas.

$x \in A \setminus X, y \in X$ Idem.

$x \in A \setminus X, y \in A \setminus X$ Dans ce cas nous avons $\alpha(x) = x$ et $\alpha(y) = y$. Donc $x = y$.

α est surjective Soit $b \in B$. Il y a deux possibilités : $b \in f(X)$ ou $b \notin f(X)$.

Si $b \in f(X)$ Soit $x \in X$ tel que $f(x) = b$. Alors $\alpha(x) = f(x) = b$.

Si $b \notin f(X)$ Alors $b \in B \setminus f(X) = A \setminus X$, et donc $\alpha(b) = b$.

□

Théorème 1.121 (Cantor-Schröder-Bernstein).

Soient deux ensembles A et B pour lesquels il existe des injections $f: A \rightarrow B$ et $g: B \rightarrow A$. Alors il existe une bijection entre A et B .

Démonstration. La composée $g \circ f: A \rightarrow A$ est injective et prend ses valeurs dans $g(f(A)) \subset g(B) \subset A$. Bref, l'application $g \circ f: A \rightarrow g(B)$ est injective. Le lemme 1.120 donne alors une bijection $\varphi: A \rightarrow g(B)$.

Nous montrons que $g^{-1} \circ \varphi: A \rightarrow B$ est une bijection.

Injective Nous supposons $x, y \in A$ tels que

$$g^{-1}(\varphi(x)) = g^{-1}(\varphi(y)). \quad (1.216)$$

Nous appliquons g des deux côtés : $\varphi(x) = \varphi(y)$. Vu que φ est une bijection, cela entraîne $x = y$.

Surjective Soit $b \in B$. En posant $a = \varphi^{-1}(g(b))$ nous avons bien $(g^{-1} \circ \varphi)(a) = b$.

□

1.5.5 Comparabilité cardinale

Le théorème de comparabilité cardinale énonce que si A et B sont des ensemble, alors nous avons toujours $A \geq B$ ou $A \leq B$ (ou les deux ; dans ce cas $A \approx B$ par Cantor-Schröder-Bernstein).

Théorème 1.122 (Théorème de comparabilité cardinale[1, 24, 25]).

Entre deux ensembles, il existe forcément une injection de l'un dans l'autre.

Démonstration. Nous allons montrer que le graphe d'une injection de A dans B ou de B dans A est donné par un élément maximal (au sens de l'inclusion) de l'ensemble (inductif) des graphes d'injections d'une partie de A dans une partie de B .

Nous allons utiliser le lemme de Zorn 1.17 à l'ensemble⁴³

$$\mathcal{A} = \left\{ (X, Y, \varphi) \text{ tel que } \begin{cases} X \subset A \\ Y \subset B \\ \varphi: X \rightarrow Y \text{ est injective.} \end{cases} \right\} \quad (1.217)$$

43. Attention : dans le Frido, la notation $f: A \rightarrow B$, signifie que f est définie sur tout l'ensemble A , mais pas qu'elle est surjective sur B .

que nous ordonnons par, l'inclusion, c'est à dire par $(X_1, Y_1, \varphi_1) < (X_2, Y_2, \varphi_2)$ lorsque $X_1 \subset X_2$, $Y_1 \subset Y_2$ et $\varphi_2|_{X_1} = \varphi_1$.

Nous passons rapidement sur le fait que cet ensemble est inductif, et nous considérons tout de suite un élément maximal (X, Y, φ) . Il y a deux possibilités : soit $\varphi(X) = B$, soit $\varphi(X) \neq B$.

Si $\varphi(X) = B$ Dans ce cas, $\varphi: X \rightarrow B$ est une surjection. L'ensemble A est donc surpotent à B .

La proposition 1.94 conclut que B est subpotent à A .

Si $\varphi(X) \neq B$ Nous subdivisons en deux nouveaux cas : soit $X = A$, soit $X \neq A$.

Si $X = A$ Alors nous avons une injection $\varphi: A \rightarrow B$, et c'est bon.

Si $X \neq A$ Nous sommes dans le cas $X \neq A$ et $\varphi(X) \neq B$. Soient $a \in A \setminus X$ et $b \in B \setminus \varphi(X)$.

Nous considérons l'application

$$\begin{aligned} \psi: X \cup \{a\} &\rightarrow Y \cup \{b\} \\ x &\mapsto \begin{cases} \varphi(x) & \text{si } x \in X \\ b & \text{si } x = a. \end{cases} \end{aligned} \quad (1.218)$$

Cela est une application injective. Donc le triple $(X \cup \{a\}, Y \cup \{b\}, \psi)$ majore (X, Y, φ) .

Nous avons une contradiction et ce cas n'est pas possible. □

1.123.

Le théorème de comparabilité cardinale couplé au théorème de Cantor-Schröder-Bernstein nous indique que pour tout ensembles A et B , nous avons soit $A \leq B$, soit $B \leq A$. Et si $A \leq B \leq A$, alors $A \approx B$.

Nous ne sommes pas loin de dire que la relation $\leq$ donne un ordre total sur l'ensemble des ensembles. C'est très beau sauf que l'ensemble des ensembles n'existe pas⁴⁴. Il faudrait parler de *classe* des ensembles, mais ça nous mènerait trop loin. Toujours est-il que ces deux théorèmes montrent qu'on n'est pas loin d'avoir un ordre sur les ensembles, et que cela est une des bases possibles pour développer les nombres cardinaux.

1.5.6 Théorème de Cantor, ensemble des ensembles

Théorème 1.124 (Cantor[26]).

Un ensemble est toujours strictement subpotent à son ensemble des parties.

Démonstration. Soit un ensemble E et son ensemble des parties $\mathcal{P}(E)$. Nous commençons par prouver qu'il n'existe pas de surjection $E \rightarrow \mathcal{P}(E)$. Soit en effet une application $f: E \rightarrow \mathcal{P}(E)$. Nous posons

$$D = \{x \in E \text{ tel que } x \notin f(x)\}. \quad (1.219)$$

Nous prouvons que D ne peut pas être dans l'image de f . Supposons que $y \in E$ soit tel que $f(y) = D$.

Si $y \in D$ Alors par définition de D , nous avons $y \notin f(y) = D$. Contradiction.

Si $y \notin D$ Alors $y \in f(y) = D$, contradiction.

Donc aucune surjection $f: E \rightarrow \mathcal{P}(E)$ n'existe. En particulier par de bijections.

Par ailleurs, l'application $g: \mathcal{P}(E) \rightarrow E$ qui fait $g(\{a\}) = a$ (et n'importe quoi d'autre sur les autres éléments de $\mathcal{P}(E)$) est une surjection $\mathcal{P}(E) \rightarrow E$.

Donc $\mathcal{P}(E)$ est toujours strictement surpotent à E . □

1.125.

Le théorème de Cantor implique en particulier qu'il existe (au moins) une infinité dénombrable d'ensemble infinis de cardinalité différentes (plus évidemment une infinité dénombrable d'ensembles finis de cardinalité différentes).

Pour tout ensemble A , il est donc possible de dire « soit E , un ensemble strictement surpotent à A ».

44. Corolaire 1.126.

Corolaire 1.126.

Il n'existe pas d'ensemble contenant tous les ensembles.

Démonstration. Si E était un tel ensemble, nous aurions $\mathcal{P}(E) \subset E$ parce que les éléments de $\mathcal{P}(E)$ sont des ensembles. Or cela donnerait une surjection $E \rightarrow \mathcal{P}(E)$ alors que cela est impossible par le théorème de Cantor 1.124. $\square$

1.5.7 Ajouter ou soustraire des cardinalités

Nous allons prouver une série de résultats que nous pourrions résumer en « ajouter ou retrancher des parties de cardinalité plus petite ne change pas la cardinalité ».

Lemme 1.127 ([1]).

Si A est infini et B est fini, alors $A \cup B \approx A$.

Démonstration. Nous supposons que A et B sont disjoints⁴⁵. La proposition 1.103 nous permet de considérer une bijection $\psi: \{1, \dots, n\} \rightarrow B$.

Vu que A est infini, la proposition 1.117 nous permet de considérer $N \subset A$ et une bijection $\varphi: \mathbb{N} \rightarrow N$.

Maintenant, il s'agit seulement d'insérer B dans A en le mettant « au début » de N et en décalant les autres. La bijection est

$$f: A \cup B \rightarrow A$$

$$x \mapsto \begin{cases} x & \text{si } x \in A \setminus N \\ \varphi(\varphi^{-1}(x) + n) & \text{si } x \in N \\ \varphi(\psi^{-1}(x)) & \text{si } x \in B. \end{cases} \quad (1.220)$$

$\square$

Lemme 1.128.

Si A est infini et si A est surpotent à B , alors $A \approx A \cup B$.

Démonstration. Il existe évidemment une injection $A \rightarrow A \cup B$. Donc le théorème de Cantor-Schröder-Bernstein 1.121 nous indique que trouver une injection $A \cup B \rightarrow A$ suffira pour la peine.

Nous allons utiliser le lemme de Zorn 1.17 avec l'ensemble

$$\mathcal{A} = \left\{ (X, \varphi_X) \text{ tel que } \begin{cases} X \subset B \\ \varphi_X: A \cup X \rightarrow A \text{ est injective.} \end{cases} \right\} \quad (1.221)$$

muni de l'ordre de l'inclusion : $(X, \varphi_X) < (Y, \varphi_Y)$ si $X \subset Y$ et $\varphi_Y(x) = \varphi_X(x)$ pour tout $x \in A \cup X$.

A est inductif Soit une famille $\mathcal{F} = \{(X_i, \varphi_i)\}_{i \in I}$ complètement ordonnée indexée par l'ensemble I . En posant $X = \bigcup_{i \in I} X_i$ et $\varphi(x) = \varphi_i(x)$ dès que $x \in A \cup X_i$, l'élément (X, φ) majore $\mathcal{F}$.

Un maximum Le lemme de Zorn nous assure que $\mathcal{A}$ possède (au moins) un élément maximum. Soit un tel élément maximum (X, φ) .

$X \approx B$ Ah oui, vous auriez aimé avoir $X = B$. Mais non ; il n'y a pas de garanties. Nous allons montrer que $X \approx B$, et ça suffira.

Vu que $X \subset B$, si X n'est pas équipotent à B , il est strictement inclus à B . Nous pouvons donc considérer

$$b \in B \setminus X \quad (1.222a)$$

$$a \in A \setminus \varphi(X). \quad (1.222b)$$

45. Adaptez la démonstration au cas où l'intersection n'est pas vide.

Nous considérons alors l'élément $(Y, \psi) \in \mathcal{A}$ défini par

$$Y = X \cup \{b\} \quad (1.223a)$$

$$\psi(x) = \begin{cases} a & \text{si } x = b \\ \varphi(x) & \text{sinon .} \end{cases} \quad (1.223b)$$

Cet élément majore (X, φ) .

Donc $X \approx B$.

Résumé de la situation Nous avons $A \approx A \cup X$ ainsi que une injection $\varphi: A \cup X \rightarrow A$ et une bijection $\psi: B \rightarrow X$.

Conclusion si A est disjoint de B Si A et B sont disjoints, nous avons une bijection

$$l: A \cup B \rightarrow A$$

$$x \mapsto \begin{cases} \varphi(x) & \text{si } x \in A \\ \varphi(\psi(x)) & \text{si } x \in B. \end{cases} \quad (1.224)$$

Conclusion si A n'est pas disjoint de B Il suffit de poser $C = B \setminus A$ et avons

$$A \cup B = [A \cup (A \cap B)] \cup C. \quad (1.225)$$

Cette union est disjointe, $A \cup (A \cap B)$ est surpotent à A et C est subpotent à B . La conclusion est donc encore valable.

□

La proposition suivante sera utilisée en théorie de la mesure, dans l'exemple 14.61.

Proposition 1.129 ([27, 13]).

Si S est un ensemble infini alors il existe une bijection $\varphi: \{0, 1\} \times S \rightarrow S$.

Démonstration. Nous posons $A = \{0\} \times S$ et $B = \{1\} \times S$. L'ensemble A est infini et surpotent à B (pas strictement, mais quand même).

Donc A est idempotent à $A \cup B$ par le lemme 1.127. Mais A est idempotent à S , donc

$$S \approx A \approx A \cup B = \{0, 1\} \times S. \quad (1.226)$$

□

Corolaire 1.130.

Si A est un ensemble infini, alors A possède deux sous-ensembles disjoints A_1 et A_2 qui sont tout deux en bijection avec A .

Démonstration. La proposition 1.129 donne une bijection $\varphi: \{1, 2\} \times A \rightarrow A$. Il suffit de poser $A_1 = \varphi(1, A)$ et $A_2 = \varphi(2, A)$. □

Maintenant que nous pouvons mettre dans A deux copies disjointes de A , il n'est pas très étonnant que nous puissions en mettre une infinité dénombrable. C'est en substance ce que signifie la proposition suivante.

Proposition 1.131.

Si A est infini, alors $A \times \mathbb{N} \approx A$.

Démonstration. La démonstration se base sur le fait qu'à l'intérieur de A , nous pouvons construire autant de copies de A deux à deux disjointes que nous le voulons. La k^e « copie » sera naturellement l'image de $k \times A$.

Voyons tout cela en détail.

Ce que nous allons faire Nous allons construire, pour tout $i \geq 1$ des parties $A_i, B_i \subset A$ telles que

- $A_i \cap B_i = \emptyset$,
- $A_i, B_i \subset B_{i-1}$,
- $A_i \approx B_i \approx A$,
- $A_i \cap A_j = \emptyset$ si $i \neq j$

La construction Nous commençons à zéro en utilisant le corolaire 1.130 pour construire des parties disjointes A_0 et B_0 de A telles que $A_0 \approx B_0 \approx A$.

Ensuite, vu que $B_0 \approx A$, il existe A_1 et B_1 dans B_0 tels que $A_1 \cap B_1 = \emptyset$ et $A_1 \approx B_1 \approx B_0 \approx A$. Cela est notre construction pour $i = 1$.

Pour la récurrence, vu que $A_i \approx B_i \approx A$, nous considérons A_{i+1} et B_{i+1} dans B_i tels que $A_{i+1} \cap B_{i+1} = \emptyset$ et $A_{i+1} \approx B_{i+1} \approx B_i \approx A$. C'est encore le corolaire 1.130 qui fait le travail.

Les propriétés Nous avons $A_i \cap A_{i+1} = \emptyset$ parce que $A_i \cap A_{i+1} \subset A_i \cap B_i = \emptyset$.

Nous devons encore montrer que $A_i \cap A_j = \emptyset$ dès que $i \neq j$. Supposons que $j > i$. Nous avons les inclusions

$$A_j \subset B_{j-1} \subset B_{j-2} \subset \dots \subset B_i. \quad (1.227)$$

Donc $A_j \cap A_i \subset B_i \cap A_i = \emptyset$.

Une injection Nous pouvons à présent écrire une injection qui termine presque la preuve. Pour cela nous considérons pour tout i , une bijection $\psi_i: A \rightarrow A_i$. Ensuite nous posons

$$\begin{aligned} \varphi: A \times \mathbb{N} &\rightarrow A \\ (a, k) &\mapsto \psi_k(a). \end{aligned} \quad (1.228)$$

Si $\varphi(a, k) = \varphi(b, l)$, alors $\psi_k(a) = \psi_l(b)$. L'élément $\psi_k(a)$ est donc dans $A_k \cap A_l$; ce n'est possible que si $k = l$. Donc $\psi_l(a) = \psi_l(b)$. Cette dernière égalité n'est possible que si $a = b$ parce que ψ_l est une bijection.

Donc φ est une injection, et nous avons prouvé que $A \times \mathbb{N} \leq A$.

La bijection Nous venons de prouver que $A \times \mathbb{N} \leq A$. La surpotence $A \times \mathbb{N} \geq A$ étant évidente, le théorème de Cantor-Schröder-Bernstein 1.121 conclut que $A \times \mathbb{N} \approx A$. □

Lemme 1.132 ([1]).

Sois un ensemble A muni de deux sous-ensembles B et B' équipotents et disjoints. Alors $A \setminus B$ est équipotent à $A \setminus B'$.

Démonstration. Soit une bijection $\psi: B' \rightarrow B$. L'application

$$\begin{aligned} \varphi: A \setminus B &\rightarrow A \setminus B' \\ x &\mapsto \begin{cases} x & \text{si } x \notin B' \\ \psi(x) & \text{si } x \in B'. \end{cases} \end{aligned} \quad (1.229)$$

fait la bijection. □

Lemme 1.133 ([28]).

Si A est un ensemble infini et si $B < A$, alors $A \approx A \setminus B$.

Démonstration. Nous pouvons écrire

$$A = (A \setminus B) \cup B. \quad (1.230)$$

Le théorème de comparabilité cardinale 1.122 nous indique que soit $A \setminus B \leq B$, soit $A \setminus B \geq B$. Nous allons voir les deux cas.

Si $A \setminus B \geq B$ Dans ce cas, $(A \setminus B) \cup B \approx A \setminus B$ par le lemme 1.128. Dans ce cas, notre résultat est prouvé parce que $A = (A \setminus B) \cup B \approx A \setminus B$.

Si $A \setminus B \leq B$ Dans ce cas, le lemme 1.128 nous indique que $A = (A \setminus B) \cup B \approx B$. Mais $A \approx B$ est exclu par l'hypothèse. Ce cas est donc impossible.

□

Lemme 1.134 ([1]).

Si A est infini et si B est une partie strictement subpotente de A , alors il existe $U \subset A$ disjoint de B et équipotent à B .

Démonstration. Le lemme 1.133 nous donne une bijection $\varphi: A \rightarrow A \setminus B$. Il suffit alors de poser $U = \varphi(B)$. Cette partie est disjointe de B parce que φ prend ses valeurs dans $A \setminus B$. □

Lemme 1.135 ([29]).

Soit un ensemble infini A ainsi qu'un sous-ensemble $B \subset A$. Nous supposons l'existence d'une fonction surjective $f: B \rightarrow B \times B$.

Alors $B \leq B \times B \leq B \leq A$.

Démonstration. La première est l'hypothèse sur f . La seconde est l'existence (évidente) d'une surjection $B \times B \rightarrow B$. La troisième est le fait que B soit inclus à A . □

Lemme 1.136 ([29]).

Soit un ensemble infini A ainsi qu'un sous-ensemble strictement subpotent $B \subset A$. Nous supposons l'existence d'une fonction surjective $f: B \rightarrow B \times B$.

Alors f peut être étendue en une injection $f: D \rightarrow D \times D$ où $D \subset A$ contient strictement B .

Démonstration. Par le lemme 1.134, nous considérons une partie $U \subset A$ disjointe de B et équipotent à B . Nous pouvons faire le développement

$$(B \cup U) \times (B \cup U) = (B \times B) \cup (B \times U) \cup (U \times B) \cup (U \times U). \quad (1.231)$$

Nous savons que B est surpotent à U (il est même équipotent); donc le lemme 1.128 nous dit que $B \cup U \approx B$. De plus il existe une bijection $B \rightarrow U$, donc

$$B \approx B \times B \approx B \times U \approx U \times B \approx U \times U. \quad (1.232)$$

Et enfin, la réunion d'ensembles équipotents est équipotent. Bref, nous avons une bijection

$$\varphi: U \rightarrow (U \times B) \cup (B \times U) \cup (U \times U). \quad (1.233)$$

Et enfin nous définissons

$$g: B \cup U \rightarrow (B \times U) \times (B \cup U) \\ x \mapsto \begin{cases} f(x) & \text{si } x \in B \\ \varphi(x) & \text{si } x \in U. \end{cases} \quad (1.234)$$

Cette définition est bonne parce que U et B sont disjoints, et g est injective. □

Le théorème suivant est une généralisation de la proposition 1.129. Elle implique, entre autres choses, qu'il existe une bijection entre $\mathbb{R}$ et $\mathbb{R} \times \mathbb{R}$. Pour le cas de $\mathbb{N} \times \mathbb{N} \approx \mathbb{N}$, il y a la proposition 1.111 qui donne une bijection explicite et donc sans axiome du choix et sans lemme de Zorn.

Théorème 1.137.

Si A est infini, alors $A \approx A \times A$.

Démonstration. Une fois de plus, ce sera le lemme de Zorn qui va s'y coller. Soit l'ensemble

$$\mathcal{A} = \left\{ (X, \varphi) \text{ tel que } \begin{cases} X \subset A \\ \varphi: X \rightarrow X \times X \text{ est surjective.} \end{cases} \right\} \quad (1.235)$$

Cet ensemble est non vide parce que A est infini ; il contient donc une partie dénombrable N , et nous connaissons la surjection $\mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$ du lemme 1.111.

Nous ordonnons $\mathcal{A}$ par l'inclusion : $(X, \varphi) \leq (Y, \phi)$ lorsque $X \subset Y$ et $\phi|_X = \varphi$. La tambouille usuelle montre que $\mathcal{A}$ est un ensemble inductif et le lemme de Zorn 1.17 donne l'existence d'un élément maximum que nous notons (B, φ) .

Vu que B est subpotent à A (parce qu'il est inclus), soit il est strictement subpotent soit il est équipotent. Nous commençons par montrer que B ne peut pas être strictement subpotent à A .

En effet, si nous avions une surjection $B \rightarrow B \times B$, alors que B est strictement subpotent à A . Le lemme 1.136 nous dit alors que φ peut être étendue, ce qui contredirait la maximalité de (B, φ) .

Donc la partie B est équipotente à A : il existe une bijection $g: A \rightarrow B$. Mais nous avons une surjection $B \rightarrow B \times B$ et donc aussi une injection $B \times B \rightarrow B$. Vu que nous avons par ailleurs une injection $B \rightarrow B \times B$, le théorème de Cantor-Schröder-Bernstein 1.121 nous donne une bijection $\phi: B \times B \rightarrow B$. Avec ça, l'application

$$\begin{aligned} f: A \times A &\rightarrow A \\ (a, b) &\mapsto \phi(g(a), g(b)) \end{aligned} \tag{1.236}$$

est une bijection. Donc les ensembles A et $A \times A$ sont équipotents. $\square$

Lemme 1.138.

Si A est infini, et si pour tout $i \in \mathbb{N}$ nous avons $A_i \approx A$, alors

$$\bigcup_{i \in \mathbb{N}} A_i \approx A. \tag{1.237}$$

Démonstration. Pour chaque $i \in \mathbb{N}$ nous avons une bijection $\varphi_i: A_i \rightarrow A$. Nous posons

$$\begin{aligned} \varphi: A \times \mathbb{N} &\rightarrow \bigcup_{i=0}^{\infty} A_i \\ (a, i) &\mapsto \varphi_i(a). \end{aligned} \tag{1.238}$$

Cette application est surjective mais peut-être pas injective parce que les A_i peuvent avoir des intersections non vides. Nous avons alors le calcul

$$A \approx A \times \mathbb{N} \tag{1.239a}$$

$$\geq \bigcup_{i=0}^{\infty} A_i \tag{1.239b}$$

$$\geq A \tag{1.239c}$$

Justifications :

- Pour (1.239a), c'est la proposition 1.131.
- Pour (1.239b), c'est la surjection (1.238).
- Pour (1.239c), c'est le fait que seulement A_0 possède déjà une surjection vers A .

Donc $\bigcup_i A_i$ est à la fois surpotent et subpotent à A . Il est donc équipotent par le théorème 1.121. $\square$

1.6 Groupes

1.6.1 Définition, unicité du neutre

Lemme-Définition 1.139 (Unicités).

L'inverse et le neutre sont uniques, c'est-à-dire :

- (1) il existe un unique élément $e \in G$ tel que $eg = ge = g$ pour tout $g \in G$,

(2) pour tout $g \in G$, il existe un unique élément $h \in G$ tel que $gh = hg = e$.

Le e ainsi défini est nommé **neutre** de G . Le h tel que $gh = hg = e$ est nommé l'**inverse** de g et est noté g^{-1} .

Démonstration. Chaque point séparément.

(1) Supposons que e_1 et e_2 vérifient la propriété. Nous avons pour tout $g \in G$: $e_1g = ge_1 = g$. En particulier pour $g = e_2$ nous écrivons $e_1e_2 = e_2e_1 = e_2$. Mais en partant dans l'autre sens : $e_2g = ge_2 = g$ avec $g = e_1$ nous avons $e_2e_1 = e_1e_2 = e_1$. En égalant ces deux valeurs de e_2e_1 nous avons $e_1 = e_2$.

Pour la suite de la preuve nous écrivons e l'unique neutre de G .

(2) Supposons que k_1 et k_2 soient deux inverses de g . On considère alors le produit k_1gk_2 . Puisque $k_1g = e$, on a $k_1gk_2 = ek_2 = k_2$; mais, comme $gk_2 = e$, on a aussi $k_1gk_2 = k_1e = k_1$. Le produit est donc à la fois égal à k_1 et à k_2 , et donc $k_1 = k_2$. □

Lemme 1.140.

Soient deux groupes G et H . Si $\alpha: G \rightarrow H$ est un morphisme de groupes, alors

(1) $\alpha(e_G) = e_H$.

(2) $\alpha(g^{-1}) = \alpha(g)^{-1}$.

Lemme-Définition 1.141.

Soit un groupe G . L'ensemble des automorphismes de G , noté $\text{Aut}(G)$, est un groupe pour la composition.

Définition 1.142.

Un groupe G est **abélien** ou **commutatif** si pour tous g et h dans G , $gh = hg$.

Lemme 1.143.

Si G est un groupe et si $h \in G$, alors les applications

$$\begin{aligned} L_h: G &\rightarrow G \\ g &\mapsto hg \end{aligned} \tag{1.240}$$

et

$$\begin{aligned} R_h: G &\rightarrow G \\ g &\mapsto gh \end{aligned} \tag{1.241}$$

sont des bijections.

Démonstration. D'abord si $L_h(g_1) = L_h(g_2)$, alors $hg_1 = hg_2$ et en multipliant à gauche par h^{-1} nous avons $g_1 = g_2$; donc L_h est injective. Ensuite L_h est surjective parce que si $g \in G$, alors $g = L_h(h^{-1}g)$.

Pour l'application R_h , la preuve est une simple adaptation. □

1.6.2 Classes de conjugaison

Définition 1.144 (classe de conjugaison).

Soit un groupe G et un élément $g \in G$. La **classe de conjugaison** de g est la partie

$$C_g = \{kgk^{-1} \text{ tel que } k \in G\}. \tag{1.242}$$

Lemme 1.145.

Un groupe est abélien si et seulement si ses classes de conjugaison sont des singletons.

Démonstration. Supposons que G soit abélien. Alors

$$C_g = \{kgk^{-1} \text{ tel que } k \in G\} = \{g\}. \quad (1.243)$$

Donc les classes de conjugaison sont des singletons.

Dans l'autre sens, si les classes sont des singletons, on a $kgk^{-1} = g$ pour tous $k, g \in G$. Cela signifie immédiatement que G est abélien. $\square$

1.6.3 Permutations, groupe symétrique

Nous donnons ici quelques éléments à propos du groupe symétrique. Beaucoup de choses supplémentaires sont reportées à la section 5.6. Voir aussi le thème 64.

Définition 1.146.

Soit un ensemble E . Une **permutation** de l'ensemble E est une bijection $E \rightarrow E$. Le **groupe symétrique** de E le groupe des bijections $E \mapsto E$; il est noté S_E .

Le **groupe symétrique** S_n est le groupe des permutations de l'ensemble $\{1, \dots, n\}$. C'est donc l'ensemble des bijections $\{1, \dots, n\} \rightarrow \{1, \dots, n\}$.

Définition 1.147.

Une **transposition** est une permutation⁴⁶ qui inverse deux éléments. Plus précisément, une bijection $\sigma: E \rightarrow E$ est une transposition si il existe $a, b \in E$ tels que

$$\sigma(x) = \begin{cases} a & \text{si } x = b \\ b & \text{si } x = a \\ x & \text{sinon.} \end{cases} \quad (1.244)$$

Lemme 1.148 ([30]).

Le groupe symétrique S_n est un ensemble fini contenant $n!$ éléments.

Lemme 1.149 ([31]).

Deux résultats.

- (1) Tout groupe est isomorphe à un sous-groupe d'un groupe symétrique.
- (2) Tout groupe fini d'ordre n est isomorphe à un sous-groupe de S_n .

Démonstration. Soit, pour $g \in G$ donné, l'application

$$\begin{aligned} \tau_g: G &\rightarrow G \\ x &\mapsto gx. \end{aligned} \quad (1.245)$$

Cela est une bijection de G . En effet, d'une part, $\tau_g(x) = y$ pour $x = g^{-1}y$ (surjection) et, d'autre part, $\tau_g(x) = \tau_g(y)$ implique $gx = gy$ et donc $x = y$ (injection).

Nous avons donc $\tau_g \in S_G$. De plus l'application

$$\begin{aligned} \varphi: G &\rightarrow S_G \\ g &\mapsto \tau_g \end{aligned} \quad (1.246)$$

est un morphisme de groupe. Il est injectif parce que si $\tau_g = \tau_h$ alors $gx = hx$ pour tout x . En particulier $g = h$.

Donc $\varphi: G \rightarrow \text{Image}(\varphi)$ est un isomorphisme entre G et un sous-groupe de S_G .

Un groupe fini de cardinal n est isomorphe à un sous-groupe de S_G ; or S_G est isomorphe à un des S_n . $\square$

46. Une permutation est une bijection, définition 1.146.

1.6.4 Décomposition en cycles

Définition 1.150.

Le **support** d'une permutation σ est l'ensemble constitué des éléments modifiés par σ :

$$\text{supp } \sigma = \{i \in \{1, \dots, n\} \text{ tel que } \sigma(i) \neq i\}.$$

Définition 1.151.

Nous disons qu'un élément $\sigma \in S_n$ **inverse** les nombres $i < j$ si $\sigma(i) > \sigma(j)$. Soit N_σ le nombre d'inversions que $\sigma \in S_n$ possède (c'est le nombre de couples (i, j) avec $i < j$ tels que $\sigma(i) > \sigma(j)$). L'entier

$$\epsilon(\sigma) = (-1)^{N_\sigma} \quad (1.247)$$

est la **signature** de σ .

Un **élément du groupe symétrique** S_n peut être décomposé en produit de cycles de supports disjoints de la façon suivante. Pour $\sigma \in S_n$, nous écrivons d'abord le cycle qui correspond à l'orbite de 1. Ce sera le cycle

$$(1, \sigma(1), \sigma^2(1), \dots, \sigma^k(1)) \quad (1.248)$$

avec $\sigma^{k+1}(1) = 1$. Ensuite nous recommençons avec le plus petit élément de $\{1, \dots, n\}$ à ne pas être dans ce cycle, et puis le suivant, etc. La *structure* d'une telle décomposition est la donnée des nombres k_i donnant le nombre de cycles de longueur i .

Lemme 1.152 ([32]).

Soit $\sigma = (i_1, \dots, i_k) \in S_n$, un cycle de longueur k et $\theta \in S_n$. Alors

$$\theta\sigma\theta^{-1} = (\theta(i_1), \dots, \theta(i_k)). \quad (1.249)$$

Tous les cycles de longueur k sont conjugués entre eux.

Proposition 1.153 (Classes de conjugaison et structure en cycles[33]).

Une classe de conjugaison⁴⁷ dans S_n est formée des permutations ayant une décomposition en cycles disjoints de même structure. Autrement dit, deux permutations σ et σ' sont conjuguées si et seulement si le nombre k_i de cycles de longueur i dans σ est le même que le nombre k'_i de cycles de longueur i dans σ' .

Démonstration. Soit $\sigma = c_1 \dots c_m$ la décomposition de σ en cycles de supports disjoints. Les c_i sont des cycles de supports disjoints. Si τ est une permutation, alors

$$\sigma' = \tau\sigma\tau^{-1} = (\tau c_1 \tau^{-1}) \dots (\tau c_m \tau^{-1}), \quad (1.250)$$

mais $\tau c_i \tau^{-1}$ est un cycle de même longueur que c_i , puisque le lemme 1.152 nous dit que si $\sigma = (a_1, \dots, a_k)$, alors $\tau\sigma\tau^{-1} = (\tau(a_1), \dots, \tau(a_k))$. Notons encore que les cycles $\tau c_i \tau^{-1}$ restent à support disjoints.

Donc tous les éléments de la classe de conjugaison de σ sont des permutations de même structure de σ .

Réciproquement, si $\sigma' = c'_1 \dots c'_m$ est une décomposition de σ' en cycles disjoints tels que la longueur de c_i est la même que la longueur de c'_i , alors il suffit de construire des permutations τ_i telles que $\tau_i c_i \tau_i^{-1} = c'_i$, à travers le lemme 1.152. Comme les supports des c_i et des c'_i sont disjoints, la permutation $\tau_1 \dots \tau_m$ conjugue σ et σ' . $\square$

Exemple 1.154.

Voyons les classes de conjugaison de S_3 . Étant donné que ce groupe agit par définition sur un ensemble à 3 éléments, aucun élément de S_3 ne possède un cycle de plus de 3 éléments. Il y a donc seulement des cycles de longueur deux ou trois (à part les triviaux). Aucun élément de S_3 n'a une décomposition en cycles disjoints contenant deux cycles de deux ou un cycle de deux et un de trois.

47. Définition 1.144.

En résumé il y a trois classes de conjugaison dans S_3 . La première est celle contenant seulement l'identité. La seconde est celle contenant les cycles de longueur deux et la troisième contient les cycles de longueur 3.

Ce sont donc

$$C_1 = \{\text{Id}\} \quad (1.251a)$$

$$C_2 = \{(1, 2), (1, 3), (2, 3)\} \quad (1.251b)$$

$$C_3 = \{(1, 2, 3), (2, 1, 3)\}. \quad (1.251c)$$

△

Exemple 1.155.

Les classes de conjugaison de S_4 . Nous savons que les classes de conjugaison dans S_4 sont caractérisées par la structure des décompositions en cycles (proposition 1.153). Le groupe symétrique S_4 possède donc les classes de conjugaison suivantes.

- (1) Le cycle vide qui représente la classe constituée de l'identité seule.
- (2) Les transpositions (de type (a, b)) qui sont au nombre de 6.
- (3) Les 3-cycles. Pour savoir **quel est leur nombre** nous commençons par remarquer qu'il y a 4 façons de prendre 3 nombres parmi 4 et ensuite 2 façons de les arranger. Il y a donc 8 éléments dans cette classe de conjugaison.
- (4) Les 4-cycles. Le premier est arbitraire (parce que c'est cyclique). Pour le second il y a 3 possibilités, et deux possibilités pour le troisième ; le quatrième est alors automatique. Cette classe de conjugaison contient donc 6 éléments.
- (5) Les doubles transpositions, du type $(a, b)(c, d)$. Dans ce cas, tous les nombres sont permutés, et l'image de 1 détermine la double transposition. Il y a 3 images possibles, et donc 3 éléments dans cette classe.

△

Proposition 1.156.

Tout élément de S_n peut être écrit sous la forme d'un produit fini de transpositions.

Cette décomposition n'est pas à confondre avec celle en cycles de support disjoints. Par exemple $(1, 2, 3) = (1, 3)(1, 2)$.

Proposition-Définition 1.157.

Si une permutation peut être écrite sous forme d'un produit d'un nombre pair de permutations, alors toute décomposition en permutations sera en quantité paire.

*Une telle permutation est une **permutation paire**.*

Lemme 1.158 ([34]).

Un k -cycle est une permutation impaire si k est pair et paire si k est impair.

Proposition 1.159 ([32]).

Soit S_n le groupe symétrique.

- (1) *L'application $\epsilon: S_n \rightarrow \{1, -1\}$ est l'unique homomorphisme surjectif de S_n sur $\{-1, 1\}$.*
- (2) *Si $s = t_1 \cdots t_k$ est le produit de k transpositions, alors $\epsilon(s) = (-1)^k$.*

Démonstration. Soit $\sigma, \theta \in S_n$. Afin de montrer que $\epsilon(\sigma\theta) = \epsilon(\sigma)\epsilon(\theta)$, nous divisons les couples (i, j) tels que $i \leq j$ en 4 groupes suivant que $\theta(i) \geq \theta(j)$ et $\sigma(\theta(i)) \geq \sigma(\theta(j))$. Nous notons N_1, N_2, N_3 et N_4 le nombre de couples dans chacun des quatre groupes :

(i, j)	$\sigma(\theta(i)) < \sigma(\theta(j))$	$\sigma(\theta(i)) > \sigma(\theta(j))$
$\theta(i) < \theta(j)$	N_1	N_2
$\theta(i) > \theta(j)$	N_3	N_4

Nous avons immédiatement $N_\theta = N_3 + N_4$ et $N_{\sigma\theta} = N_2 + N_4$. Les éléments qui participent à N_σ sont ceux où $\theta(i)$ et $\theta(j)$ sont dans l'ordre inverse de $\sigma(\theta(i))$ et $\sigma(\theta(j))$ (parce que θ est une bijection). Donc $N_\sigma = N_2 + N_3$. Par conséquent nous avons

$$\epsilon(\sigma)\epsilon(\theta) = (-1)^{N_2+N_3}(-1)^{N_3+N_4} = (-1)^{N_2+N_4} = (-1)^{N_{\sigma\theta}} = \epsilon(\sigma\theta). \quad (1.252)$$

Nous avons prouvé que ϵ est un homomorphisme. Pour montrer que ϵ est surjectif sur $\{-1, 1\}$ nous devons trouver un élément $\tau \in S_n$ tel que $\epsilon(\tau) = -1$. Si τ est la transposition $1 \leftrightarrow 2$ alors le couple $(1, 2)$ est le seul à être inversé par τ et nous avons $\epsilon(\tau) = -1$.

Avant de montrer l'unicité, nous montrons que si $\sigma = t_1 \dots t_k$ alors $\epsilon(\sigma) = (-1)^k$. Pour cela il faut montrer que $\epsilon(\tau) = -1$ dès que τ est une transposition. Soit τ_{ij} , la transposition (i, j) et $\theta = (i, i+1, \dots, j-1)$ alors le lemme 1.152 dit que

$$\tau_{ij} = \theta\tau_{j-1,j}\theta^{-1}. \quad (1.253)$$

La signature étant un homomorphisme,

$$\epsilon(\tau_{ij}) = \epsilon(\theta)\epsilon(\tau_{j-1,j})\epsilon(\theta)^{-1} = \epsilon(\tau_{j-1,j}) = -1. \quad (1.254)$$

Nous passons maintenant à la partie unicité de la proposition. Soit un homomorphisme surjectif $\varphi: S_n \rightarrow \{-1, 1\}$ et τ , une transposition telle que $\varphi(\tau) = -1$ (qui existe parce que sinon φ ne serait pas surjectif⁴⁸). Si τ' est une autre transposition, il existe $\sigma \in S_n$ tel que $\tau' = \sigma\tau\sigma^{-1}$ (lemme 1.152). Dans ce cas, $\varphi(\tau') = \varphi(\tau) = -1$, et si $\sigma = \tau_1 \dots \tau_k$,

$$\varphi(\sigma) = (-1)^k = \epsilon(\sigma). \quad (1.255)$$

□

Corolaire 1.160.

Si $\sigma \in S_n$, alors

$$\epsilon(\sigma) = \epsilon(\sigma^{-1}). \quad (1.256)$$

Démonstration. Comme dit par la proposition 1.159, ϵ est un homomorphisme, donc

$$\epsilon(\sigma)\epsilon(\sigma^{-1}) = \epsilon(\sigma\sigma^{-1}) = \epsilon(\text{Id}) = 1. \quad (1.257)$$

Vu que $\epsilon(\sigma)$ et $\epsilon(\sigma^{-1})$ ne peuvent être que ± 1 , ils doivent être tous les deux 1 ou tous les deux -1 pour que le produit soit 1. □

1.7 Anneaux

Définition 1.161.

Un *isomorphisme d'anneaux* est un morphisme bijectif.

La distributivité de la partie (3) de la définition 1.30 ne traite que de l'addition ; pas de la soustraction. Voici une lemme qui dit que ça fonctionne quand même.

Lemme 1.162 ([13]).

Soient un anneau A ainsi que $a, b, c \in A$. Alors

$$a(b - c) = ab - ac. \quad (1.258)$$

Démonstration. Nous avons le calcul suivant :

$$a(b - c) + ac = a((b - c) + c) \quad (1.259a)$$

$$= ab. \quad (1.259b)$$

Justifications :

48. Nous utilisons ici le fait que tous les éléments de S_n sont des produits de transpositions, proposition 1.156.

- Pour 1.259a. Distributivité.
- Pour 1.259b. Parce que $(b - c) + c = b$.

Nous avons donc $a(b - c) + ac = ab$ et donc l'égalité demandée en ajoutant $-ac$ des deux côtés. $\square$

Lemme 1.163.

Pour tout élément a d'un anneau nous avons $a \cdot 0 = 0$.

Démonstration. L'élément 0 est le neutre de l'addition. Il peut être écrit $1 - 1$, et en utilisant la distributivité sous la forme du lemme 1.162,

$$a \cdot 0 = a \cdot (1 - 1) = a - a = 0. \quad (1.260)$$

Notons que la dernière égalité s'écrit en détail $a - a = a + (-a)$ qui donne le neutre de l'addition. $\square$

Proposition 1.164.

Dans un anneau⁴⁹ non nul, le neutre pour l'addition est distinct du neutre pour la multiplication.

Démonstration. Supposons par contraposée que dans un anneau A , $1 = 0$. Alors, pour tout $a \in A$, on a $a = 1a = 0a = (1 - 1)a = a - a = 0$, d'où l'on déduit $-a = 0$ et par suite, $a = 0$. $\square$

Lemme 1.165 ([1]).

Un peu d'arithmétique. Soit un anneau A et un élément $a \in A$.

- (1) $1 \times 1 = 1$.
- (2) $(-1) \times a = -a$.
- (3) $-(-a) = a$.
- (4) $(-1) \times (-1) = 1$.

Démonstration. En plusieurs parties.

Pour (1) La définition de 1 est que $1 \times a = a$ pour tout a . En particulier pour $a = 1$ nous avons le résultat.

Pour (2) Nous avons

$$(-1) \times a + a = a \times ((-1) + 1) = a \times 0 = 0. \quad (1.261)$$

Nous avons utilisé le fait que la multiplication était distributive et que le zéro était absorbant (lemme 1.163).

Pour (3) Nous avons $-a + a = 0$ par définition de la notation $-a$. Donc a est bien l'inverse de $-a$ pour l'addition.

Pour (4) En utilisant les points (2) et (3) nous avons

$$(-1) \times (-1) = -(-1) = 1. \quad (1.262)$$

$\square$

Soit X un ensemble et un anneau $(A, +, \times)$. Nous considérons $\text{Fun}(X, A)$ l'ensemble des applications $X \rightarrow A$. Cet ensemble devient un anneau avec les définitions

$$(f + g)(x) = f(x) + g(x) \quad (1.263a)$$

$$(fg)(x) = f(x)g(x). \quad (1.263b)$$

Cela est la **structure canonique** d'anneau sur $\text{Fun}(X, A)$.

49. Définition 1.30.

Définition 1.166.

Le **centralisateur** de $x \in A$ dans A est l'ensemble

$$\{y \in A \text{ tel que } xy = yx\}, \quad (1.264)$$

le **centre** de A est

$$\{y \in A \text{ tel que } xy = yx, \forall x \in A\}. \quad (1.265)$$

Définition 1.167 (Idéal dans un anneau).

Un sous-ensemble $I \subset A$ est un **idéal à gauche** à gauche si

- (1) I est un sous-groupe pour l'addition,
- (2) pour tout $a \in A$, $aI \subset I$.

Lorsqu'un ensemble est idéal à gauche et à droite, nous disons que c'est un **idéal bilatère**. Lorsque nous parlons d'idéal sans précisions, nous parlons d'idéal bilatère.

Proposition-Définition 1.168.

Soit A , un anneau, I un idéal bilatère⁵⁰ de A . Nous considérons la relation d'équivalence $x \sim y$ si et seulement si $x - y \in I$. Sur le quotient⁵¹

$$A/\sim = A/I, \quad (1.266)$$

nous mettons les opérations

- (1) $[x] + [y] = [x + y]$
- (2) $[x][y] = [xy]$.

Nous avons alors les résultats suivants :

- (1) Les opérations sont bien définies,
- (2) l'ensemble A/I , muni de ces opérations, est un anneau
- (3) la surjection canonique $\pi: A \rightarrow A/I$ est un morphisme.

Cet anneau est appelé **anneau quotient**.

Démonstration. En plusieurs parties.

Pour (1) Nous savons que, par définition,

$$\bar{x} = \{x + i \text{ tel que } i \in I\}. \quad (1.267)$$

Calculons le produit de représentants génériques de $\bar{x}$ et de $\bar{y}$:

$$(x + i_1)(y + i_2) = xy + xi_2 + yi_1 + i_1i_2. \quad (1.268)$$

Vu que I est un idéal nous avons $xi_2 + yi_1 + i_1i_2 \in I$ et donc bien

$$(x + i_1)(y + i_2) \in \bar{xy}. \quad (1.269)$$

Pour (2) Il s'agit de vérifier les conditions de la définition 1.30.

Vu que $(A, +)$ est un groupe abélien de neutre 0, nous avons

$$[a] + [b] = [a + b] = [b + a] = [b + a], \quad (1.270)$$

ainsi que

$$[a] + [0] = [a + 0] = [a] \quad (1.271)$$

et

$$[a] + ([b] + [c]) = [a] + [b + c] = [a + b + c] = [a + b] + [c]. \quad (1.272)$$

50. Définition 1.167.

51. Définition 1.24.

Donc $(A/I, +)$ est un groupe abélien de neutre $[0]$.

L'associativité de A donne l'associativité dans A/I :

$$([a][b])[c] = [ab][c] = [abc] = [a][bc] = [a]([b][c]). \quad (1.273)$$

Et enfin pour la distributivité,

$$[a]([b] + [c]) = [a][b + c] = [a(b + c)] = [ab + ac] = [ab] + [ac] = [a][b] + [a][c]. \quad (1.274)$$

Nous avons prouvé que A/I est un anneau de neutre $[0]$ et d'unité $[1]$.

Pour (3) Nous devons vérifier les trois conditions de la définition 1.31. Cela est immédiat parce que $\pi(x) = [x]$. □

Définition 1.169.

Soient A un anneau commutatif et $S \subset A$. Nous disons que $\delta \in A$ est un **PGCD** de S si

- (1) δ divise tous les éléments de S .
- (2) si d divise également tous les éléments de S , alors d divise δ .

Nous disons que $\mu \in A$ est un **PPCM** de S si

- (1) $S \mid \mu$,
- (2) si $S \mid m$, alors $\mu \mid m$.

Remarque 1.170.

Au sens de la définition 1.169, le pgcd n'est pas unique. Dans $\mathbb{Z}$ par exemple les nombres 4 et -4 sont tout deux pgcd de $\{4, 16\}$.

Dans $\mathbb{Z}$ cependant, nous modifions implicitement la définition et nous n'acceptons que les positifs, de telle sorte à ce que l'unique pgcd soit effectivement le plus grand pour l'ordre usuel sur $\mathbb{Z}$.

Pour l'unicité dans $\mathbb{Z}$, voir 3.20.

1.7.1 Anneau intègre

Définition 1.171 (Diviseurs dans un anneau).

Soient $a, b \in A$. On dit que a divise b , ou que a est un **diviseur (à gauche)** de b s'il existe $c \in A$ tel que $ac = b$. On dit que c est un diviseur de b à droite si $ca = b$ pour un certain $c \in A$.

Un cas particulier est le cas des diviseurs de zéro. L'absence de tels diviseurs dans un anneau est une propriété intéressante : on dit dans ce cas que l'anneau est intègre. Nous étudions ces anneaux plus en détail en section 1.10.

Un élément $a \in A$ est **régulier à droite** si $ba = 0$ implique $b = 0$. Il est régulier à gauche si $ab = 0$ implique $b = 0$.

Définition 1.172 (Éléments nilpotents, unipotents et inversibles).

On dit que $a \in A$ est **nilpotent** s'il existe $n \in \mathbb{N}$ tel que $a^n = 0$. Il est dit **unipotent** si $a - 1$ est nilpotent, c'est-à-dire si $(a - 1)^n = 0$ pour un certain $n \in \mathbb{N}$.

Un élément $a \in A$ est dit **inversible** s'il existe $b \in A$ tel que $ab = 1$.

L'ensemble $U(A)$ des éléments inversibles de A est un groupe pour la multiplication. Nous notons $A^* = A \setminus \{0\}$.

Conformément à la définition 1.171 de diviseur, nous posons la définition suivante pour les diviseurs de zéro.

Définition 1.173 ([35]).

Un élément $a \neq 0$ est un **diviseur de zéro à gauche** s'il existe $x \neq 0$ tel que $xa = 0$. L'élément a est un **diviseur de zéro à droite** s'il existe $y \neq 0$ tel que $ay = 0$.

Nous disons que a est un **diviseur de zéro** si il est un diviseur de zéro à gauche ou à droite.

Proposition-Définition 1.174 (Anneau intègre[1]).

Soit A un anneau non réduit à $\{0\}$. Les assertions suivantes sont équivalentes :

- (1) A ne possède pas de diviseurs de zéro.
- (2) La règle du produit nul s'applique dans A : pour tous $a, b \in A$, si $ab = 0$, alors $a = 0$ ou $b = 0$.
- (3) On peut simplifier par un même élément non-nul, deux expressions produit dans A qui sont égales : pour tous $a, b, c \in A$ avec $a \neq 0$, si $ab = ac$, alors $b = c$.

Un anneau non réduit à $\{0\}$ qui vérifie ces propriétés est dit **intègre**.

Démonstration. En trois implications.

(1) implique (2) Si $ab = 0$ avec $a, b \neq 0$ alors a est un diviseur de zéro. Vu que nous supposons que A n'a pas de diviseurs de zéros, soit a soit b est nul.

(2) implique (3) Si $ab = ac$, alors $a(b - c) = 0$ et l'hypothèse dit que soit $a = 0$, soit $b - c = 0$. Donc si $a \neq 0$, alors $b - c = 0$.

(3) implique (1) Si $A = \{0\}$, le point (3) n'est pas applicable.

Si $a \neq 0$ et $xa = 0$, alors nous avons aussi $xa = 0 \times a$. Par propriété de simplification, $x = 0$. Donc a n'est pas un diviseur de zéro à gauche. Nous prouvons de la même façon qu'il n'y a pas de diviseurs de zéro à droite.

□

1.7.2 Fonction puissance

Voici une première définition de la fonction puissance. Il y en aura d'autres, de plus en plus générales. Voir le thème 36.

Définition 1.175.

Si A est un anneau, si $a \in A$ et si $n \in \mathbb{N}$, nous définissons a^n par récurrence :

- (1) $a^0 = 1$ (l'unité pour la multiplication dans A),
- (2) $a^{k+1} = a \cdot a^k$.

Le lemme suivant dit que le point (2) de la définition 1.175 aurait pu être écrit $a^k \cdot a$ au lieu de $a \cdot a^k$.

Lemme 1.176 ([1]).

Si A est un anneau, si $a \in A$ et si $n \in \mathbb{N}$, alors

$$a^n = a \cdot a^{n-1} = a^{n-1} \cdot a. \quad (1.275)$$

Démonstration. Cela se prouve par récurrence. Pour $n = 1$ c'est l'égalité $a = a^0 a$ qui est correcte parce que par définition $a^0 = 1$.

Supposons que le résultat soit bon pour n et voyons ce que ça donne pour $n + 1$:

$$a^{n+1} = aa^n \quad \text{Définition de } a^{n+1} \quad (1.276a)$$

$$= a(a^{n-1}a) \quad \text{hypothèse de récurrence pour } a^n \quad (1.276b)$$

$$= (aa^{n-1})a \quad \text{associativité} \quad (1.276c)$$

$$= a^n a \quad \text{Définition de } a^n. \quad (1.276d)$$

□

1.8 Le groupe et anneau des entiers

Certes $(\mathbb{Z}, +)$ est un groupe mais en ajoutant la multiplication, $(\mathbb{Z}, +, \times)$ devient un anneau ⁵²

52. Définition 1.30.

1.8.1 Division euclidienne

Théorème-Définition 1.177 (Division euclidienne[36]).

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$, avec $0 \leq r < b$, tel que

$$a = bq + r. \quad (1.277)$$

L'opération $(a, b) \mapsto (q, r)$ ainsi définie est la **division euclidienne**. Le nombre q est le **quotient** et r est le **reste** de la division de a par b .

Démonstration. Remarquons que $r = a - bq$, et donc, une fois l'existence et l'unicité de q établie, celle de r suivra.

Unicité Nous supposons avoir $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tels que

$$\begin{cases} 0 \leq r < b \\ a = bq + r. \end{cases} \quad (1.278a)$$

$$(1.278b)$$

Ce système implique que

$$0 \leq a - bq < b. \quad (1.279)$$

En ajoutant qb dans les trois membres de cette inégalité,

$$qb \leq a < (q+1)b. \quad (1.280)$$

Cela implique que

$$q = \max\{k \in \mathbb{Z} \text{ tel que } kb \leq a\}. \quad (1.281)$$

Donc q est unique et la relation $a = bq + r$ implique que r est également unique.

$$E = \{q \in \mathbb{Z} \mid bq \leq a\}.$$

C'est un sous-ensemble d'entiers non-vide (il contient $-|a|$) et admet $|a|$ comme majorant ; il admet donc un maximum q par le lemme 1.90. Ce maximum vérifie

$$bq \leq a < b(q+1). \quad (1.282)$$

Cela donne $0 \leq a - bq < b$ et le résultat en posant $r = a - bq$.

□

1.8.2 PGCD, PPCM et Bézout

Vu que $\mathbb{Z}$ est un anneau intègre, nous avons la définition 1.169 de pgcd et de ppcm.

Proposition 1.178 (PPCM et PGCD).

Soient $p, q \in \mathbb{Z}^*$.

- (1) Le pgcd de p et q est le plus grand diviseur commun de p et q .
- (2) Le ppcm de p et q est leur plus petit multiple commun.

Démonstration. Démontrons le premier point. Notons δ le pgcd de p et q . Si d est un diviseur commun de p et q , alors d divise δ . Dans $\mathbb{Z}$, $d \mid \delta$ implique $d \leq \delta$ (proposition 1.91). □

Lemme 1.179.

Soient $p, q \in \mathbb{Z}^*$. Les entiers $\text{ppcm}(p, q)$ et $\text{pgcd}(p, q)$ fournissent les isomorphismes de groupes suivants :

$$p\mathbb{Z} \cap q\mathbb{Z} = \text{ppcm}(p, q)\mathbb{Z} \quad (1.283a)$$

$$p\mathbb{Z} + q\mathbb{Z} = \text{pgcd}(p, q)\mathbb{Z}. \quad (1.283b)$$

Définition 1.180.

Si $\text{pgcd}(p, q) = 1$, nous disons que p et q sont **premiers entre eux**. Si nous avons un ensemble d'entiers a_i , nous disons qu'ils sont premiers **dans leur ensemble** si 1 est le PGCD de tous les a_i ensemble.

Les nombres 2, 4 et 7 ne sont pas premiers deux à deux (à cause de 2 et 4), mais ils sont premiers dans leur ensemble parce qu'il n'y a pas de diviseurs communs à tout le monde.

Théorème 1.181 (Théorème de Bézout ⁵³[37], thème 53).

Deux entiers non nuls $a, b \in \mathbb{Z}^*$ sont premiers entre eux si et seulement s'il existe $u, v \in \mathbb{Z}$ tels que

$$au + bv = 1 \quad (1.284)$$

Démonstration. Soit $d = \text{pgcd}(a, b)$ et des nombres u, v tels que $au + bv = 1$. Le PGCD d divise à la fois a et b , et donc divise $au + bv$. Nous en déduisons que d divise 1 et est par conséquent égal à 1.

Nous supposons maintenant que $\text{pgcd}(a, b) = 1$ et nous considérons l'ensemble

$$E = \{au + bv \text{ tel que } u, v \in \mathbb{Z}\} \cap \mathbb{N}^*. \quad (1.285)$$

C'est-à-dire l'ensemble des nombres strictement positifs pouvant s'écrire sous la forme $au + bv$. Cet ensemble est non vide parce qu'il contient par exemple soit a soit $-a$. Soit m le plus petit élément de E et écrivons

$$m = au_1 + bv_1. \quad (1.286)$$

Par le théorème de division euclidienne ⁵⁴ (avec a et m), il existe des entiers uniques q et r tels que

$$a = mq + r \quad (1.287)$$

avec $0 \leq r < m$. En remplaçant m par sa valeur (1.286), $a = (au_1 + bv_1)q + r$ et

$$r = a(1 - u_1q) - bv_1q, \quad (1.288)$$

c'est-à-dire que $r \in \mathbb{Z}a + \mathbb{Z}b$ en même temps que $0 \leq r < m$. Si r était strictement positif, il serait dans E . Mais cela est impossible par minimalité de m . Donc $r = 0$ et a est divisible par m .

De la même façon nous prouvons que b est divisible par m . Vu que m divise à la fois a et b nous avons $m = 1$. $\square$

Une généralisation de Bézout 1.181 à plus de 2 variables.

Proposition 1.182.

Si $\{a_i\}_{i=1,\dots,N}$ sont des entiers tels que $\text{pgcd}(a_1, \dots, a_N) = 1$, alors il existe des entiers $\{u_i\}_{i=1,\dots,N}$ tels que

$$\sum_i a_i u_i = 1. \quad (1.289)$$

Corolaire 1.183.

Soient p et q deux entiers premiers entre eux. Alors

$$p\mathbb{Z} + q\mathbb{Z} = \mathbb{Z}; \quad (1.290)$$

en particulier, pour tout $x \in \mathbb{Z}$, il existe u_x, v_x entiers tels que $u_x p + v_x q = x$.

Notons que l'application $p\mathbb{Z} + q\mathbb{Z}$ vers $\mathbb{Z}$ n'est évidemment pas injective : les u_x et v_x ne sont pas uniques à x fixé.

53. Il y a une super application ici : https://perso.univ-rennes1.fr/matthieu.romagny/agreg/dvt/mauvais_prix.pdf.

54. Théorème 1.177.

Démonstration. Soit $x \in \mathbb{Z}$. Le théorème de Bézout nous donne k et l tels que $kp + lq = 1$. Du coup, $(xk)p + (xl)q = x$. $\square$

La proposition suivante établit que si x est assez grand, alors il peut même être écrit comme une combinaison de p et q à coefficients positifs. Elle sera utilisée pour démontrer que les états apériodiques d'une chaîne de Markov peuvent être atteints à tout moment (assez grand), voir la définition 38.47 et ce qui suit.

Proposition 1.184.

Soient a et b deux éléments de $\mathbb{N}$ premiers entre eux. Il existe $N > 0$ tel que tout $x > N$ appartient à $a\mathbb{N} + b\mathbb{N}$.

Démonstration. Soient a et b , premiers entre eux, et $x \in \mathbb{N}$. Disons tout de suite, pour éviter les cas triviaux et pénibles, que x , a et b sont strictement positifs.

Une décomposition pour x On applique le théorème 1.177 de division euclidienne à x et $a + b$: il existe des entiers p_x, r_x , uniques, tels que

$$\begin{cases} x = (p_x - 1)(a + b) + r_x & (1.291a) \\ 0 \leq r_x < a + b. & (1.291b) \end{cases}$$

En d'autres termes, $p_x(a + b)$ est le premier multiple de $a + b$ supérieur ou égal à x . De plus, p_x est strictement positif car x l'est. Il existe alors des entiers u et v tels que

$$ua + vb = p_x(a + b) - x \quad (1.292)$$

par le corolaire 1.183. Ainsi, x peut s'écrire

$$x = (p_x - u)a + (p_x - v)b. \quad (1.293)$$

Des maximums Il s'agit maintenant de savoir si nous pouvons être assuré d'avoir $p_x > u$ et $p_x > v$ dès que x est assez grand. Pour cela, grâce au corolaire 1.183, nous considérons les nombres u_i et v_i définis par

$$u_i a + v_i b = i \quad (1.294)$$

pour $i = 1, \dots, a + b$. Nous posons $u^* = \max\{u_i\}$, $v^* = \max\{v_i\}$, et $p^* = \max\{u^*, v^*\}$. Nous posons alors $N = p^*(a + b)$, et considérons $x > N$.

Nouvelle décomposition pour x Nous voulons écrire

$$x = (p_x - u_k)a + (p_x - v_k)b \quad (1.295)$$

pour un certain k . Cela demande $u_k a + v_k b = ua + vb = p_x(a + b) - x$ par l'équation (1.292).

Vu que $p_x(a + b) - x > 0$, les nombres u_k et v_k existent : il suffit de prendre $k = p_x(a + b) - x$.

Conclusion Avec tous ces choix, nous avons d'abord $x > p^*(a + b)$ et donc

$$x = (p_x - 1)(a + b) + r_x > p^*(a + b), \quad (1.296)$$

ce qui donne

$$(p_x - 1)(a + b) > p^*(a + b) - r_x > (p - 1)(a + b). \quad (1.297)$$

ou encore $p_x > p^*$. Nous avons finalement

$$p_x \geq p^* \geq u^* \geq u_k \quad (1.298)$$

et

$$p_x \geq p^* \geq v^* \geq v_k. \quad (1.299)$$

De ce fait, la décomposition (1.295) est celle que nous voulions. $\square$

1.185.

Une méthode pour obtenir les entiers naturels u et v qui permettent la décomposition $x = au + bv$ est d'abord de choisir u_0 et v_0 tels que au_0 et bv_0 soient les plus proches possibles de $x/2$, puis de décomposer le nombre (relativement petit) $x - au_0 - bv_0$ en $au_1 + bv_1$. Deux nombres u et v qui fonctionnent sont alors $u = u_0 + u_1$ et $v = v_0 + v_1$.

Exemple 1.186.

Écrivons $1000 = u \cdot 7 + v \cdot 5$ avec $u, v \in \mathbb{N}$. D'abord $72 \cdot 7 = 504$ et $100 \cdot 5 = 500$. Nous avons donc

$$1004 = 72 \cdot 7 + 100 \cdot 5. \quad (1.300)$$

Ensuite $4 = 25 - 21 = -3 \cdot 7 + 5 \cdot 5$. Au final,

$$1000 = 75 \cdot 7 + 95 \cdot 5. \quad (1.301)$$

△

1.8.3 Sous-groupes de $(\mathbb{Z}, +)$ **Proposition 1.187.**

Une partie H du groupe $(\mathbb{Z}, +)$ est un sous-groupe si et seulement s'il existe $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.

Démonstration. Soit $H \neq \{0\}$ un sous-groupe de $\mathbb{Z}$. L'ensemble $H \cap \mathbb{N}^*$ contient un élément minimum que nous notons n . Nous avons certainement $n\mathbb{Z} \subset H$ parce que H est un groupe (donc $n + n$ et $-n$ sont dans H dès que n est dans H). Nous devons prouver que $H \subset n\mathbb{Z}$.

Si $x \in H$, par le théorème de division euclidienne 1.177, il existe $q \in \mathbb{Z}$ et $r \in \mathbb{N}$, uniques, tels que $x = nq + r$ et $0 \leq r < n$. Nous savons déjà que $nq \in H$, donc $r = x - nq \in H$. Le nombre r est donc un élément de H strictement plus petit que n . Mais nous avons décidé que n serait le plus petit élément de $H \cap \mathbb{N}^*$. Par conséquent $r = 0$ et $x = nq \in n\mathbb{Z}$. □

Notons que si un sous-groupe H de $\mathbb{Z}$ est donné, alors le nombre n tel que $H = n\mathbb{Z}$ est unique. En effet si $n\mathbb{Z} = m\mathbb{Z}$ nous avons que n divise m (parce que $m \in m\mathbb{Z} \subset n\mathbb{Z}$) et que m divise n parce que $n \in m\mathbb{Z}$. Par conséquent $n = m$.

1.8.4 Résultats supplémentaires sur l'anneau des entiers**Corolaire 1.188.**

Les quotients de $\mathbb{Z}$ sont $\mathbb{Z}/n\mathbb{Z}$.

Démonstration. Tous les idéaux de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$. En effet en vertu de la proposition 1.187, les seuls sous-groupes de $\mathbb{Z}$ (en tant que groupe additif) sont les $n\mathbb{Z}$. Tous les idéaux sont donc de cette forme. De plus les $n\mathbb{Z}$ sont effectivement tous des idéaux : si $a \in n\mathbb{Z}$ et si $k \in \mathbb{Z}$ alors $ak \in n\mathbb{Z}$. Cela est donc un idéal. □

Proposition 1.189.

Soient $n \geq 2$ un entier et $\phi: \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ la surjection canonique. Nous noterons $\tilde{a} = \phi(a)$. Alors l'ensemble des inversibles de $\mathbb{Z}/n\mathbb{Z}$ est donné par

$$U(\mathbb{Z}/n\mathbb{Z}) = \phi(P_n) = \{\tilde{x} \text{ tel que } 0 \leq x \leq n \text{ tel que } \text{pgcd}(x, n) = 1\}. \quad (1.302)$$

où P_n est l'ensemble $P_n = \{x \in \{0, \dots, n-1\} \text{ tel que } \text{pgcd}(x, n) = 1\}$.

De plus,

$$\text{Card}(U(\mathbb{Z}/n\mathbb{Z})) = \varphi(n). \quad (1.303)$$

Démonstration. Soit $0 \leq x \leq n$ tel que $\text{pgcd}(x, n) = 1$. Il existe donc⁵⁵ $u, v \in \mathbb{Z}$ tels que $ux + vn = 1$. En passant aux classes,

$$\tilde{u}\tilde{x} = \tilde{1}, \quad (1.304)$$

55. Théorème de Bézout 1.181

donc $\tilde{u}$ est l'inverse de $\tilde{x}$. Cela prouve que $\phi(P_n) \subset U(\mathbb{Z}/n\mathbb{Z})$.

Nous prouvons maintenant l'inclusion inverse. Soient $\tilde{x}$ et $\tilde{y}$ inverses l'un de l'autre : $\tilde{x}\tilde{y} = \tilde{1}$. Il existe donc $q \in \mathbb{Z}$ tel que $xy - qn = 1$, ce qui prouve⁵⁶ que $\text{pgcd}(x, n) = 1$. $\square$

1.9 Corps

1.9.1 Définitions, morphismes

Définition 1.190 ([38]).

Un **corps** est une anneau⁵⁷ $(A, +, \times)$ dans lequel tout élément non nul est inversible pour l'opération $\times$ (pour l'opération $+$, tous les éléments sont inversibles parce que $(A, +)$ est un groupe).

Remarque 1.191.

Un anneau est ce qu'on appelle « *ring* » en anglais. Un corps est en anglais « *field* ». De plus le mot « *field* » comprend la commutativité. Donc certains utilisent le mot « corps » pour dire « corps commutatif » et parlent alors d'anneau à *division* pour parler de corps non commutatifs.

La proposition suivante donne une caractérisation d'un corps, en disant un tout petit peu plus que la définition 1.190.

Proposition 1.192.

L'anneau A est un corps si et seulement si $U(A) = A^*$.

Démonstration. En deux parties.

Sens direct Nous supposons que A est un corps. D'une part tous les éléments non nuls sont inversibles, c'est-à-dire $A^* \subset U(A)$.

Pour l'inclusion inverse, nous montrons qu'un élément inversible ne peut pas être nul. Cela n'est autre que le lemme 1.163 couplé à la proposition 1.164 : $a \cdot 0 = 0 \neq 1$ pour tout a .

Sens inverse Si $U(A) = A^*$, nous avons immédiatement que tous les éléments non nuls sont inversibles et donc que A est un corps. $\square$

Lemme 1.193.

Si $\mathbb{K}$ est un corps et si $a \in \mathbb{K}$ vérifie $a^2 = 1$, alors $a = \pm 1$.

Lemme 1.194.

Un corps non nul est un anneau intègre⁵⁸.

Démonstration. Soit un produit nul $ab = 0$. Si $a \neq 0$, alors il est inversible et nous multiplions $ab = 0$ par a^{-1} . Nous trouvons $b = 0$ parce que $0a^{-1} = 0$. $\square$

Conséquence : dans un corps nous avons toujours la règle du produit nul, et l'élément nul n'est jamais inversible.

Définition 1.195 (Morphisme de corps).

Un corps étant un anneau sans plus de structure, un **morphisme de corps** n'est qu'un morphisme des anneaux⁵⁹.

Le lemme suivant montre que définir un morphisme de corps comme étant simplement un morphisme des anneaux est une bonne idée.

Lemme 1.196.

Si $\phi: \mathbb{K} \rightarrow \mathbb{K}'$ est un morphisme de corps, alors

56. À nouveau avec le Théorème de Bézout.

57. Définition 1.30.

58. Définition 1.174.

59. Définition 1.31.

- (1) pour tout $a \in \mathbb{K}$ nous avons $\varphi(a^{-1}) = \varphi(a)^{-1}$;
 (2) le morphisme φ est injectif.

Démonstration. Vu que $\varphi(1) = 1$, nous avons aussi

$$1 = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1}). \quad (1.305)$$

Donc, par unicité de l'inverse⁶⁰, $\varphi(a^{-1}) = \varphi(a)^{-1}$.

Pour l'injectivité nous supposons $\varphi(a) = \varphi(b)$. Étant donné que $\mathbb{K}'$ est un corps, nous pouvons multiplier par $\varphi(b)^{-1}$:

$$\varphi(a)\varphi(b)^{-1} = 1. \quad (1.306)$$

En utilisant le premier point nous avons $1 = \varphi(a)\varphi(b^{-1})$, puis le morphisme d'anneaux : $1 = \varphi(ab^{-1})$, et encore le morphisme d'anneaux nous permet de déduire $ab^{-1} = 1$ et donc $a = b$. $\square$

1.10 Anneau intègre

La définition d'un anneau intègre est la définition 1.174.

Lemme 1.197.

Un corps⁶¹ est un anneau intègre.

Démonstration. En effet, soient un corps $\mathbb{K}$ et deux éléments $x, y \in \mathbb{K}$ tels que $xy = 0$. Si y est inversible, alors nous pouvons multiplier par y^{-1} pour trouver $x = 0$. Cela prouve que $\mathbb{K}$ est un anneau intègre. $\square$

Exemple 1.198.

L'ensemble $\mathbb{Z}$ avec les opérations usuelles est un anneau intègre⁶². $\triangle$

Exemple 1.199.

L'anneau $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre parce que $3 \cdot 2 = 0$ alors que ni 3 ni 2 ne sont nuls. $\triangle$

Nous verrons au théorème 3.121 que l'anneau A est intègre si et seulement si $A[X]$ est intègre.

Corolaire 1.200.

L'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier.

Démonstration. Supposons que n soit premier. La proposition 1.189 donne les inversibles de $\mathbb{Z}/n\mathbb{Z}$ par

$$U(\mathbb{Z}/n\mathbb{Z}) = \{\tilde{x} \text{ tel que } 0 \leq x \leq n \text{ tel que } \text{pgcd}(x, n) = 1\}. \quad (1.307)$$

Mais comme n est premier, $\text{pgcd}(x, n) = 1$ pour tout x , et donc tous les éléments de $\mathbb{Z}/n\mathbb{Z}$ sont inversibles. Donc $\mathbb{Z}/n\mathbb{Z}$ est intègre.

Si n n'est pas premier, alors $n = pq$ avec $1 < p \leq q < n$. Alors

$$[p]_n[q]_n = [pq]_n = [0]_n. \quad (1.308)$$

Donc lorsque n n'est pas premier, l'anneau $\mathbb{Z}/n\mathbb{Z}$ possède des diviseurs de zéro et n'est alors pas intègre. $\square$

1.10.1 Élément premier

Définition 1.201 ([39]).

Soit un anneau commutatif A . Un élément $p \in A$ est **premier** si il est

- (1) non nul,

60. Lemme 1.139 (2).

61. Définition 1.190.

62. Anneau intègre, définition 1.174.

- (2) non inversible,
 (3) si p divise un produit ab , alors il divise soit a soit b (ou le deux).

Le lemme suivant est souvent pris pour la définition d'un nombre premier lorsqu'on parle de $\mathbb{N}$ ou $\mathbb{Z}$.

Lemme 1.202 ([40, 1]).

Dans $\mathbb{N}$, un nombre est premier si et seulement si il admet exactement deux diviseurs entiers distincts.

Démonstration. En deux parties.

$\Rightarrow$ Soit un élément premier $p \in \mathbb{N}$. Il y a trois possibilités : $p = 0$, $p = 1$ et $p > 1$.

Le nombre $p = 0$ n'est pas premier parce qu'il est nul. Le nombre $p = 1$ n'est pas premier parce qu'il est inversible. Donc nous savons que si p est premier, alors $p > 1$.

Un élément $p > 1$ dans $\mathbb{N}$ a toujours au moins deux diviseurs distincts : 1 et p . Soit un diviseur k de p . Il existe $l \in \mathbb{N}$ tel que $p = kl$. Vu que p est premier et divise le produit kl , il divise k ou l . Disons que p divise k . De cette façon p divise k et k divise p .

Il existe donc $n \in \mathbb{N}$ tel que $k = np$. En y substituant $p = kl$, on trouve $k = np = nkl$. En simplifiant par k , il vient

$$1 = nl, \quad (1.309)$$

ce qui prouve que $n = l = 1$ et donc que $k = p$ et donc que p n'a pas d'autres diviseurs que 1 et p .

$\Leftarrow$ Nous supposons que $p \in \mathbb{N}$ ait exactement deux diviseurs entiers distincts. Nous vérifions que p vérifie les trois conditions de la définition 1.201.

- (1) $p \neq 0$ parce que 0 a nettement plus que deux diviseurs distincts.
- (2) $p \neq 1$ parce que 1 a exactement un diviseur. Donc p n'est pas inversible dans $\mathbb{N}$.
- (3) Soit p admettant exactement deux diviseurs distincts. Soit p divisant le produit ab' pour certains a et b' dans $\mathbb{N}$. Nous supposons que p ne divise pas a , et nous allons prouver que p divise b' en supposant d'abord que p ne divise pas b' .

Un ensemble Pour cela nous posons

$$E = \{x \in \mathbb{N} \text{ tel que } p \mid ax, p \nmid x\}. \quad (1.310)$$

Nous posons $b = \min(E)$. Nous avons pour hypothèse que E est non vide; en particulier $0 < b$.

$b < p$ On vérifie que si $p + k \in E$ alors $k \in E$. Donc b ne peut pas être plus grand que p . Vu que p lui-même n'est pas dans E , nous avons $b < p$.

Division euclidienne Nous effectuons la division euclidienne du théorème 1.177 :

$$p = mb + r. \quad (1.311)$$

En multipliant par a , $ar = ap - mab$. Vu que ab est un multiple de p $ap - mab$ est un multiple de p . En particulier ar est divisible en p .

La contradiction Nous avons donc $r \in E$, alors que $r < b$. Impossible.

□

Proposition 1.203 ([41]).

Dans un anneau intègre⁶³ tout élément premier est irréductible⁶⁴.

Démonstration. Soit p , un élément premier dans un anneau intègre A .

63. Si pas intègre, voir l'exemple 1.205.

64. Toutes les définitions dans le thème 55.

p n'est pas inversible Cela fait partie de la définition d'un élément premier.

p n'est pas un produit d'inversibles Soient $a, b \in A$ tels que $p = ab$. Par le point (3) de la définition 1.201, p divise soit a soit b . Supposons que p divise a . Alors il existe $x \in A$ tel que $a = px$. En remettant dans $p = ab$ nous avons :

$$p = pxb. \quad (1.312)$$

Mais l'anneau est intègre et permet donc des simplifications par tout élément non nul. La relation 1.312 donne donc

$$1 = xb, \quad (1.313)$$

ce qui signifie que b est inversible.

Un travail similaire montre que a est inversible si p divise b .

□

Exemple 1.204.

Si nous avons l'égalité $7 = ab$ dans $\mathbb{Z}$, alors soit a soit b vaut 1 et est donc inversible.

△

Sur un anneau non intègre, la notion d'élément premier n'est pas aussi intéressante que sur un anneau intègre. Par exemple la proposition 1.203 devient fausse.

Exemple 1.205.

Soit l'anneau $\mathbb{Z}^2$. L'élément $(1, 0)$ est premier mais pas irréductible.

$(1, 0)$ est premier L'élément $(1, 0)$ est non nul ; ça c'est pas cher. Pour qu'il soit inversible, il faudrait $(1, 0)(x, y) = (1, 1)$. Entre autres, $0 \times y = 1$, ce qui est impossible. Donc il n'est pas inversible.

Supposons que $(1, 0)$ divise le produit $(a, b)(c, d) = (ac, bd)$. Alors il existe (x, y) tel que $(1, 0)(x, y) = (ac, bd)$. Cela signifie que $x = ac$ et $0 \times y = bd$. En particulier, soit $b = 0$ soit $d = 0$. Si $b = 0$, nous avons $(a, b) = (a, 0)$ et effectivement, $(1, 0)$ le divise.

$(1, 0)$ n'est pas irréductible Nous avons $(1, 0) = (1, 0)(1, 0)$. Donc l'élément $(1, 0)$ est le produit de deux éléments non inversibles.

△

1.11 Symbole de sommation

1.11.1 Somme à valeurs dans un groupe abélien

Si S est un ensemble fini, nous savons de la proposition 1.103 qu'il existe un unique $N \in \mathbb{N}$ pour lequel il existe une bijection $\varphi: \{0, \dots, N\} \rightarrow S$. Cette bijection n'est à priori pas unique.

Lemme-Définition 1.206 ([1]).

Soient un groupe abélien $(G, +)$ ainsi qu'un ensemble fini I contenant n éléments. Soit une application $f: I \rightarrow G$. Si $\sigma_1, \sigma_2: \{1, \dots, n\} \rightarrow I$ sont deux bijections, alors⁶⁵

$$\sum_{i=1}^n f(\sigma_1(i)) = \sum_{i=1}^n f(\sigma_2(i)). \quad (1.314)$$

La valeur commune est notée

$$\sum_{i \in I} f(i) \quad (1.315)$$

65. Pour rappel, le symbole $\sum_{i=1}^n$ est défini par 1.68.

Démonstration. Nous commençons par considérer une transposition σ (qui permute k et l avec $k < l$). Nous avons

$$\sum_{i=1}^n f(i) = \sum_{i=1}^{k-1} f(i) + f(k) + \sum_{i=k+1}^{l-1} f(i) + f(l) + \sum_{i=l+1}^n f(i) \quad (1.316a)$$

$$= \sum_{i=1}^{k-1} f(i) + f(l) + \sum_{i=k+1}^{l-1} f(i) + f(k) + \sum_{i=l+1}^n f(i) \quad (1.316b)$$

$$= \sum_{i=1}^n f(\sigma(i)). \quad (1.316c)$$

Pour cela nous avons utilisé le fait que G est abélien pour permuter $f(l) \in G$ et $f(k) \in G$ avec $\sum_{i=k+1}^{l-1} f(i) \in G$.

Une permutation quelconque est un produit de telles transpositions (proposition 1.156). Donc pour toute permutation σ nous avons

$$\sum_{i=1}^n f(\sigma(i)) = \sum_{i=1}^n f(i). \quad (1.317)$$

□

La définition 1.206 donne lieu à un certain nombre de remarques.

- (1) Elle donne la somme sur un ensemble fini. Un problème avec les ensembles infinis (outre la convergence) est l'ordre de sommation. Si vous voulez sommer sur $\mathbb{Z}$, dans quel ordre le faire ?
- (2) Pour aller plus loin, et sommer sur des ensembles infinis, il faut regarder la définition 1.157.

Proposition 1.207.

Soient un groupe abélien $(G, +)$, un ensemble fini I est un ensemble fini, une application $f: I \rightarrow G$ et une bijection $\sigma: I \rightarrow I$. Alors

$$\sum_{i \in I} f(i) = \sum_{i \in I} f(\sigma(i)). \quad (1.318)$$

Si nous avons une application $L: S \rightarrow S$, nous notons

$$\sum_{s \in S} f(L(s)) = \sum_{s \in S} (f \circ L)(s). \quad (1.319)$$

Cette façon d'écrire donne une interprétation pour la notation $\sum_{g \in G} f(hg)$ qui arrive dans la proposition 1.209. Il s'agit de considérer l'application L_h du lemme 1.143, de considérer⁶⁶

$$\sum_{g \in G} f(hg) = \sum_{g \in G} (f \circ L_h)(g) \quad (1.320)$$

et de faire tourner la définition 1.206. La même chose tient pour définir $\sum_{g \in G} (gh)$ à l'aide de R_h .

Lemme 1.208.

Soit un ensemble A fini pouvant être écrit comme une union disjointe $A = \bigcup_{k=1}^n A_k$; nous supposons que les A_i sont non vides. Soient un groupe abélien $(G, +)$ et une application $f: A \rightarrow G$. Alors

$$\sum_{a \in A} f(a) = \sum_{k=1}^n \sum_{a \in A_k} f(a). \quad (1.321)$$

Démonstration. Le lemme 1.97 nous indique que les parties A_k sont des ensembles finis. Nous notons

66. Le fait que L_h soit une bijection n'a pas d'importance ici.

- (1) $N_0 = 0$, et $N_k = \text{Card}(A_k)$,
- (2) $S_k = \sum_{i=1}^k N_k$.
- (3) $\varphi_k: \{1, \dots, N_k\} \rightarrow A_k$, une bijection (l'existence est dans la proposition 1.103).

Nous avons que $\text{Card}(A) = S_n$ par le lemme 1.104(4). Nous définissons une belle bijection comme il faut :

$$\begin{aligned} \alpha: \{1, \dots, S_n\} &\rightarrow A \\ i &\mapsto \varphi_{k+1}(i - S_k) \end{aligned} \quad (1.322)$$

pour $i \in]S_k, S_{k+1}]$.

α est bien définie Vu que $i > S_k$ et $i \leq S_{k+1}$ nous avons $i - S_k \in \{1, \dots, N_{k+1}\}$, et donc φ_{k+1} s'applique bien à $i - S_k$.

α est injective Supposons que $\alpha(i) = \alpha(j)$. Si $i \in]S_k, S_{k+1}]$ et $j \in]S_l, S_{l+1}]$, alors $\alpha(i) = \varphi_{k+1}(i - S_k) \in A_{k+1}$ et $\alpha(j) = \varphi_{l+1}(j - S_l) \in A_{l+1}$. Vu que les A_i sont disjoints, nous avons $k = l$, et donc

$$\varphi_{k+1}(i - S_k) = \varphi_{k+1}(j - S_k). \quad (1.323)$$

Étant donné que φ_{k+1} est injective, nous avons $i - S_k = j - S_k$, ce qui montre que $i = j$.

α est surjective Soit $a \in A$. Il existe k tel que $a \in A_k$. Nous avons donc un $s \in \{1, \dots, N_k\}$ tel que $a = \varphi_k(s)$. En posant $i = s + S_k$, nous avons bien $a = \alpha(s + S_k)$ parce que $s + S_k \in]S_{k-1}, S_k]$.

Vu que α est une bijection, nous avons l'égalité

$$\sum_{a \in A} f(a) = \sum_{i=1}^{S_n} (f \circ \alpha)(i). \quad (1.324)$$

Nous avons encore besoin d'introduire une bijection. Nous posons

$$\begin{aligned} \beta_k:]S_{k-1}, S_k] &\rightarrow A_k \\ i &\mapsto \varphi_k(i - S_{k-1}). \end{aligned} \quad (1.325)$$

Cela est une bijection parce que φ_k en est une, et que $i \mapsto i - S_{k-1}$ est une bijection de $]S_{k-1}, S_k]$.

Nous pouvons maintenant terminer :

$$\sum_{a \in A} f(a) = \sum_{i=1}^{S_n} (f \circ \alpha)(i) \quad (1.326a)$$

$$= \sum_{k=1}^n \left(\sum_{i=S_{k-1}+1}^{S_k} (f \circ \alpha)(i) \right) \quad (1.326b)$$

$$= \sum_{k=1}^n \left(\sum_{i \in]S_{k-1}, S_k]} f(\varphi_k(i - S_{k-1})) \right) \quad (1.326c)$$

$$= \sum_{k=1}^n \left(\sum_{i \in]S_{k-1}, S_k]} f(\beta_k(i)) \right) \quad (1.326d)$$

$$= \sum_{i=1}^n \left(\sum_{a \in A_k} f(a) \right). \quad (1.326e)$$

Justifications :

— Pour (1.326b). Associativité de la somme.

□

Proposition 1.209 ([1]).

Soient un groupe fini G et une fonction $f: G \rightarrow A$ où A est un anneau commutatif. Alors

$$\sum_{g \in G} f(g) = \sum_{g \in G} f(gh) = \sum_{g \in G} f(hg) \quad (1.327)$$

pour tout $h \in G$.

Démonstration. Nous avons une bijection $\varphi: \{0, \dots, N\} \rightarrow G$ garantie par la proposition 1.103. La définition est que

$$\sum_{g \in G} f(g) = \sum_{i=0}^N f(\varphi(i)). \quad (1.328)$$

Par ailleurs, le lemme 1.143 donne une bijection $L_h: G \rightarrow G$ et permet de considérer la composée

$$\begin{aligned} \varphi': \{0, \dots, N\} &\rightarrow G \\ \varphi' &= L_h \circ \varphi. \end{aligned} \quad (1.329)$$

La proposition 1.206 nous permet d'utiliser la bijection φ' au lieu de φ pour exprimer la somme $\sum_{g \in G}$. Ensuite un jeu de notation utilisant (1.320) donne

$$\begin{aligned} \sum_{g \in G} f(g) &= \sum_{i=0}^N f(\varphi(i)) = \sum_{i=0}^N f(\varphi'(i)) = \sum_{i=0}^N (f \circ L_h \circ \varphi)(i) \\ &= \sum_{i=0}^N (f \circ L_h)(\varphi(i)) = \sum_{g \in G} (f \circ L_h)(g) = \sum_{g \in G} f(hg). \end{aligned} \quad (1.330)$$

En ce qui concerne $\sum_{g \in G} f(gh)$, c'est la même chose, en utilisant R_h au lieu de L_h . $\square$

Tout cela nous permet de faire une somme sympathique et bien connue.

Lemme 1.210.

Soit $n \in \mathbb{N}$. Nous avons

$$\sum_{k=0}^n k = \frac{n(n+1)}{2}. \quad (1.331)$$

Démonstration. La preuve est pratiquement immédiate par récurrence. Nous allons donner une preuve plus « constructive », qui formalise l'idée classique d'écrire la somme à l'endroit et à l'envers.

Nous notons S la somme $\sum_{k=0}^n k$. Le lemme 1.206 dit que si $\sigma_i: \{0, \dots, n\} \rightarrow \{0, \dots, n\}$ sont deux bijections, alors $\sum_{k=0}^n f(\sigma_1(k)) = \sum_{k=0}^n f(\sigma_2(k))$. Nous sommes intéressé au cas $f(i) = i$.

En prenant $\sigma_1(k) = k$ et $\sigma_2(k) = n - k$, nous avons

$$S = \sum_{k=0}^n k = \sum_{k=0}^n (n - k). \quad (1.332)$$

Donc

$$2S = \sum_{k=0}^n (k + (n - k)) = \sum_{k=0}^n n = n \sum_{k=0}^n 1 = n(n+1). \quad (1.333)$$

En divisant par deux, nous obtenons le résultat annoncé. $\square$

Proposition 1.211.

Si E est un ensemble fini et si G est un groupe abélien, alors pour toute fonction $f: E \rightarrow G$ et pour toute permutation⁶⁷ σ de E ,

$$\prod_{i \in E} f(i) = \prod_{i \in E} f(\sigma(i)) \quad (1.334)$$

Démonstration. C'est exactement la proposition 1.206, sauf qu'ici la loi de groupe est notée multiplicativement au lieu de additivement. $\square$

67. Une permutation est une bijection, définition 1.146.

1.12 Module sur un anneau

Définition 1.212 (module sur un anneau[42]).

Soit un anneau A . Un **module à gauche** sur A est la donnée d'un triple $(M, +, \cdot)$ où

(1) $+$ est une loi de composition interne à M , c'est-à-dire $+: M \times M \rightarrow M$,

(2) $\cdot$ est une loi de composition externe, c'est-à-dire $\cdot: A \times M \rightarrow M$

telles que

(1) $(M, +)$ est un groupe⁶⁸.

(2) $a \cdot (x + y) = a \cdot x + a \cdot y$,

(3) $(a + b) \cdot x = a \cdot x + b \cdot x$,

(4) $(ab) \cdot x = a \cdot (b \cdot x)$

(5) $1 \cdot x = x$.

pour tout $a, b \in A$ et $x, y \in M$.

Proposition 1.213.

Si M est un module sur un anneau, alors $(M, +)$ est un groupe commutatif.

Démonstration. Il suffit de calculer $(1 + 1) \cdot (x + y)$ de deux façons différentes :

$$(1 + 1) \cdot (x + y) = 1 \cdot (x + y) + 1 \cdot (x + y) = x + y + x + y \quad (1.335)$$

d'une part et

$$(1 + 1) \cdot (x + y) = (1 + 1) \cdot x + (1 + 1) \cdot y = x + x + y + y, \quad (1.336)$$

d'autre part. En égalant les deux expressions, il vient

$$x + y + x + y = x + x + y + y, \quad (1.337)$$

qui se simplifie (nous sommes dans un groupe) en $y + x = x + y$. $\square$

Définition 1.214.

Un **espace vectoriel** est un module⁶⁹ sur un corps commutatif⁷⁰.

Définition 1.215 ([43]).

Soient un A -module M et un ensemble I . Une famille $(m_i)_{i \in I}$ est **libre** si ils sont **linéairement indépendants**, c'est-à-dire si pour tout choix d'une partie finie J dans I et d'éléments $(a_j)_{j \in J}$ dans A , si nous avons

$$\sum_{j \in J} a_j m_j = 0, \quad (1.338)$$

alors $a_j = 0$ pour tout j .

Définition 1.216 ([44]).

Soit S , une partie du A -module M . Le **sous-module engendré** par S est l'ensemble des éléments de M qui sont des combinaisons linéaires finies d'éléments de S , c'est-à-dire de sommes de la forme

$$\sum_{t \in T} a_t t \quad (1.339)$$

où T est fini dans S et $a_t \in A$.

68. Nous verrons dans la proposition 1.213 qu'il est forcément commutatif.

69. Définition 1.212.

70. La condition de commutativité n'est pas indispensable, mais comme nous ne parlerons que de corps commutatifs...

1.12.1 Module produit

Lemme-Définition 1.217 ([43]).

Soient un anneau A et un ensemble I . Le A -**module produit** A^I est l'ensemble des applications $I \rightarrow A$.

En termes de notations, nous écrivons ceci :

$$A^I = \{(a_i)_{i \in I}, a_i \in A\}. \quad (1.340)$$

L'ensemble A^I devient un module par les définitions, pour $x, y \in A^I$ et $a \in A$:

$$ax = (ax_i)_{i \in I} \quad (1.341a)$$

$$x + y = (x_i + y_i)_{i \in I}. \quad (1.341b)$$

En d'autres termes, $A^I = \text{Fun}(I, A)$.

Lemme 1.218.

Pour chaque $i \in I$ nous considérons l'élément $e_i \in A^I$ donné par

$$e_i = (\delta_{ij})_{j \in I}. \quad (1.342)$$

La famille $\{e_i\}_{i \in I}$ est libre⁷¹ dans A^I .

Démonstration. Soient J fini dans I ainsi que des éléments $a_j \in A$ ($j \in J$). Nous supposons que⁷² $\sum_{j \in J} a_j e_j = 0$. Calculons un peu :

$$\sum_{j \in J} a_j e_j = \sum_{j \in J} (a_j \delta_{ji})_{i \in I} = \left(\sum_{j \in J} a_j \delta_{ji} \right)_{i \in I}. \quad (1.343)$$

Pour que le tout soit nul dans A^I , il faut que

$$\sum_{j \in J} a_j \delta_{ji} \quad (1.344)$$

soit nul pour tout $i \in I$. Si nous fixons $i \in I$, la somme sur j possède un seul terme non annulé par δ_{ji} , et c'est le terme $j = i$. Nous avons donc $a_i = 0$. $\square$

Définition 1.219.

Nous notons $A^{(I)}$ le sous-module de A^I engendré⁷³ par les e_i .

Théorème 1.220 (Propriété universelle de $A^{(I)}$ [43]).

Soient un anneau A ainsi qu'un A -module P . Pour $\phi \in \text{Hom}_A(A^{(I)}, P)$, nous considérons

$$\begin{aligned} \phi|_I: I &\rightarrow P \\ i &\mapsto \phi(e_i). \end{aligned} \quad (1.345)$$

(1) L'application

$$\begin{aligned} f: \text{Hom}_A(A^{(I)}, P) &\rightarrow \text{Fun}(I, P) \\ \phi &\mapsto \phi|_I \end{aligned} \quad (1.346)$$

est une bijection.

(2) L'application inverse est $g: \text{Fun}(I, P) \rightarrow \text{Hom}_A(A^{(I)}, P)$ donnée par

$$g(\psi)\left(\sum_{j \in J} a_j e_j\right) = \sum_{j \in J} a_j \psi(j) \quad (1.347)$$

pour tout J fini dans I et choix de $a_j \in A$.

71. Définition 1.215.

72. Pour rappel, les sommes finies sont définies par 1.206.

73. Définition 1.216.

Démonstration. Nous allons montrer que $g(f(\phi)) = \phi$ et que $f(g(\psi)) = \psi$ pour tout $\phi \in \text{Hom}_A(A^{(I)}, P)$ et pour tout $\psi \in \text{Fun}(I, P)$.

Dans un premier sens nous avons :

$$g(f(\phi))\left(\sum_j a_j e_j\right) = \sum_j a_j f(\phi)(j) \quad (1.348a)$$

$$= \sum_j a_j \phi(e_j) \quad (1.348b)$$

$$= \phi\left(\sum_j a_j e_j\right). \quad (1.348c)$$

Justifications :

- Pour (1.348b), nous avons utilisé le fait que $f(\phi)(i) = \phi|_I(i) = \phi(e_i)$.
- Pour (1.348c), nous utilisons le fait que ϕ est un morphisme de modules.

Et pour l'autre sens,

$$f(g(\psi))(i) = g(\psi)(e_i) = \psi(i). \quad (1.349)$$

□

1.12.2 Sous-module

Soient M un A -module et $x = (x_i)_{i \in I}$ une famille d'éléments de M paramétrée par l'ensemble I . Nous considérons l'application

$$\begin{aligned} \mu_x : A^{(I)} &\rightarrow M \\ (a_i)_{i \in I} &\mapsto \sum_{i \in I} a_i x_i. \end{aligned} \quad (1.350)$$

Ici $A^{(I)}$ désigne l'ensemble de toutes les applications $I \rightarrow A$ de support fini.

Définition 1.221.

À l'instar des espaces vectoriels, les modules ont une notion de partie libre, génératrice et de bases :

- (1) Si μ_x est surjective, nous disons que x est une partie **génératrice**.
- (2) Si μ_x est injective, nous disons que la partie x est **libre**.
- (3) Si μ_x est bijective, nous disons que la partie x est une **base**.

Définition 1.222.

Un sous-ensemble $N \subset M$ est un **sous-module** si $(N, +)$ est un sous-groupe de $(M, +)$ et si $a \cdot x \in N$ pour tout $x \in N$ et pour tout $a \in A$.

Exemple 1.223.

Un anneau A est lui-même un A -module et ses sous-modules sont les idéaux. △

Définition 1.224.

Soit M un module sur un anneau commutatif A . Un **projecteur** est une application linéaire $p : M \rightarrow M$ telle que $p^2 = p$.

Une famille $(p_i)_{i \in I}$ sur M est **orthogonale** si $p_i \circ p_j = 0$ pour tout $i \neq j$. La famille est **complète** si $\sum_{i \in I} p_i = \text{Id}$.

Théorème 1.225.

Soient des sous modules $M_1, \dots, M_n$ du module M tels que $M = M_1 \oplus \dots \oplus M_n$. Les applications p_i définies par

$$p_i(x_1 + \dots + x_n) = x_i \quad (1.351)$$

forment une famille orthogonale de projecteurs et $p_1 + \dots + p_n = \text{Id}$.

Inversement, si $(p_1, \dots, p_n)$ est une famille orthogonale de projecteurs dans un module $\mathcal{E}$ tel que $\sum_{i=1}^n p_i = \text{Id}$, alors

$$M = \bigoplus_{i=1}^n p_i(M). \quad (1.352)$$

Définition 1.226.

Un module est **simple** ou **irréductible** s'il n'a pas d'autres sous-modules que $\{0\}$ et lui-même. Un module est **indécomposable** s'il ne peut pas être écrit comme somme directe de sous-modules.

Un module simple est a fortiori indécomposable. L'inverse n'est pas vrai comme le montre l'exemple suivant.

Exemple 1.227.

Soit $\mathcal{E} = \mathbb{C}[X]/(X^2)$ vu comme $\mathbb{C}[X]$ -module. C'est le $\mathbb{C}[X]$ -module des polynômes de la forme $aX + b$ avec $a, b \in \mathbb{C}$. L'ensemble des polynômes de la forme aX est un sous-module. Le module $\mathcal{E}$ n'est donc pas simple. Il est cependant indécomposable parce que $\{aX\}$ est le seul sous-module non trivial. En effet si $\mathcal{F}$ est un sous-module de $\mathcal{E}$ contenant $aX + b$ avec $b \neq 0$, alors $\mathcal{F}$ contient $X(aX + b) = bX$ et donc contient tout $\mathcal{E}$. $\triangle$

Définition 1.228 (Algèbre[45]).

Si $\mathbb{K}$ est un corps commutatif⁷⁴, une $\mathbb{K}$ -**algèbre** A est un espace vectoriel⁷⁵ muni d'une opération bilinéaire $\times : A \times A \rightarrow A$, c'est-à-dire telle que pour tout $x, y, z \in A$ et pour tout $\alpha, \beta \in \mathbb{K}$,

- (1) $(x + y) \times z = x \times z + y \times z$
- (2) $x \times (y + z) = x \times y + x \times z$
- (3) $(\alpha x) \times (\beta y) = (\alpha\beta)(x \times y)$.

Si A et B sont deux $\mathbb{K}$ -algèbres, une application $f : A \rightarrow B$ est un **morphisme d'algèbres** entre A et B si pour tout $x, y \in A$ et pour tout $\alpha \in \mathbb{K}$,

- (1) $f(xy) = f(x)f(y)$
- (2) $f(x + \alpha y) = f(x) + \alpha f(y)$

où nous avons noté xy pour $x \times y$.

Lemme 1.229 ([1]).

Soient une algèbre A et une famille $(X_i)_{i \in I}$ de sous-algèbres de A (ici I est un ensemble quelconque). Alors la partie $X = \bigcap_{i \in I} X_i$ est une sous-algèbre de A .

Démonstration. Nous devons prouver que si x et y sont dans X et $\lambda \in \mathbb{K}$, alors xy , $x + y$ et λx sont dans X . Pour tout $i \in I$ nous avons $x, y \in X_i$ et donc $xy \in X_i$, $x + y \in X_i$ et $\lambda x \in X_i$ (parce que X_i est une algèbre). Donc $xy, x + y$ et λx sont dans X_i pour tout $i \in I$, et donc dans X . $\square$

Définition 1.230.

L'**algèbre engendrée** par X est l'intersection de toutes les sous-algèbres de A contenant X (qui est une algèbre par le lemme 1.229).

1.13 Caractéristique d'un anneau

Lemme-Définition 1.231.

Soit l'application

$$\begin{aligned} \mu : \mathbb{Z} &\rightarrow A \\ n &\mapsto n \cdot 1_A \end{aligned} \quad (1.353)$$

où $n \cdot 1_A$ signifie $\sum_{k=1}^n 1_A$.

- (1) C'est un morphisme d'anneaux.

⁷⁴. Définition 1.190

⁷⁵. Définition 1.214.

(2) Le noyau est un sous-groupe de $\mathbb{Z}$

(3) Il existe un unique $p \in \mathbb{Z}$ tel que $\ker(\mu) = p\mathbb{Z}$.

Ce p est la **caractéristique** de A .

Par exemple la caractéristique que $\mathbb{Q}$ est zéro parce qu'aucun multiple de l'unité n'est nul.

À propos de diagonalisation en caractéristique 2, voir l'exemple 9.133.

Lemme 1.232.

Si A est de caractéristique nulle, alors A est infini.

Démonstration. En effet, $\ker \mu = \{0\}$ implique que $n1_A \neq m1_A$ dès que $n \neq m$ et par conséquent A contient $\mathbb{Z}1_A$, et est infini. $\square$

Lemme 1.233.

Si p est la caractéristique de l'anneau A , alors nous avons l'isomorphisme d'anneaux

$$\mathbb{Z}1_A \simeq \mathbb{Z}/p\mathbb{Z}. \quad (1.354)$$

Démonstration. L'isomorphisme est donné par l'application $n1_A \mapsto \phi(n)$ si ϕ est la projection canonique $\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$. $\square$

Proposition 1.234.

La caractéristique d'un anneau fini divise son cardinal.

Démonstration. Si A est un anneau, le groupe $\mathbb{Z}$ agit sur A par

$$n \cdot a = a + n1_A. \quad (1.355)$$

Chaque orbite de cette action est de la forme

$$\mathcal{O}_a = \{a + n1_A \text{ tel que } n = 0, \dots, p-1\} \quad (1.356)$$

où p est la caractéristique de A . Les orbites ont p éléments et forment une partition de A , donc le cardinal de A est un multiple de p . $\square$

Lemme 1.235 ([46]).

Un anneau totalement ordonné est de caractéristique nulle.

Démonstration. Le morphisme $\mu: \mathbb{Z} \rightarrow A, n \mapsto n1_A$ est strictement croissant, en particulier $\mu(x) \neq \mu(y)$ dès que $x \neq y$. Donc $\ker(\mu) = \{0\}$. $\square$

L'ensemble typique de caractéristique p est $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Proposition 1.236.

Soit A un anneau commutatif unitaire de caractéristique p . L'application

$$\begin{aligned} \text{Frob}_A: A &\rightarrow A \\ x &\mapsto x^p \end{aligned} \quad (1.357)$$

est un automorphisme d'anneau unitaire.

Nous le nommons le **morphisme de Frobenius**. Nous utiliserons aussi les itérés du morphisme de Frobenius : $\text{Frob}^k: x \mapsto x^{p^k}$.

Exemple 1.237.

Soit à factoriser $X^p - 1$ dans $\mathbb{F}_p$. Grâce au morphisme de Frobenius, nous avons immédiatement

$$X^p - 1 = (X - 1)^p. \quad (1.358)$$

$\triangle$

Lemme 1.238.

La caractéristique⁷⁶ d'un anneau intègre est zéro ou un élément premier⁷⁷.

Démonstration. Si A est intègre, alors $\mathbb{Z}1_A$ est a fortiori intègre. Notons p la caractéristique de A . Si $p = 0$, la preuve est finie ; supposons donc que $p \neq 0$. Alors, l'anneau $\mathbb{Z}/p\mathbb{Z}$ est isomorphe à $\mathbb{Z}1_A$, et est donc intègre. Or, la proposition 1.200 dit que $\mathbb{Z}/p\mathbb{Z}$ est intègre si et seulement si p est premier, ce qui conclut la preuve. $\square$

Exemple 1.239.

Il existe des corps dont la caractéristique n'est pas égale au cardinal (contrairement à ce que laisserait penser l'exemple des $\mathbb{Z}/p\mathbb{Z}$). En effet les matrices $n \times n$ inversibles sur $\mathbb{F}_3$ forment un corps qui n'est pas de cardinal trois alors que la caractéristique est 3 :

$$\begin{pmatrix} 1 & \\ & 1 \end{pmatrix} + \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} + \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} = 0. \quad (1.359)$$

$\triangle$

1.13.1 Caractéristique deux

Beaucoup de résultats demandent une caractéristique différente de deux. Qu'a donc de particulier la caractéristique deux ?

Si $\mathbb{K}$ est un corps de caractéristique 2, alors l'égalité $x = -x$ n'implique pas $x = 0$, vu que $2x = 0$ est vérifiée pour tout x . Cela se répercute sur un certain nombre de résultats. Par exemple, en caractéristique deux, une forme antisymétrique n'est pas toujours alternée : voir le lemme 9.2.

1.14 Polynômes**1.14.1 Polynômes d'une variable**

Et voila la définition que tout le monde attendait ; la définition des anneaux de polynômes. Pour ne pas taper trop fort du premier coup, nous commençons par les polynômes d'une seule variable⁷⁸.

Nous allons définir et étudier ici l'anneau des polynômes sur un anneau A , c'est-à-dire ce qui sera noté $A[X]$. Pour $\mathbb{K}(X)$ lorsque $\mathbb{K}$ est un corps, voir 6.77.

L'ensemble des polynômes sur A sera simplement $A^{(\mathbb{N})}$. Vu que $\mathbb{N}$ est un ensemble bien particulier possédant plein de structure, nous allons pouvoir mettre sur $A^{(\mathbb{N})}$ une structure non seulement de A -module (ça c'est déjà fait), mais en plus d'anneau ainsi qu'une évaluation.

Définition 1.240.

L'ensemble des **polynômes** en une indéterminée sur l'anneau A est l'anneau $A^{(\mathbb{N})}$ que nous avons défini en 1.219. Il sera noté $\mathcal{P}(A)$.

En ce qui concerne la notation $A[X]$, voir 1.14.2.

Définition 1.241.

Soit $P \in \mathcal{P}$, $P \neq 0$. On appelle **degré** de P le plus grand nombre naturel n pour lequel le coefficient correspondant est non-nul. Ce naturel est noté $\deg(P)$. L'ensemble des polynômes de degré n sur A sera noté $\mathcal{P}_n(A)$.

Notez que nous n'avons pas encore donné la notation $A[X]$; nous verrons plus tard comment elle arrive.

Vu que $A^{(\mathbb{N})}$ est engendré par les e_i , tout polynôme sur A s'écrit $P = \sum_{i=1}^n a_i e_i$.

76. Définition 1.231.

77. Définition 1.201.

78. Les polynômes à plusieurs variables seront la définition 3.51.

Définition 1.242.

Nous ajoutons deux structures à $A^{(\mathbb{N})}$.

L'évaluation Si $\alpha \in A$ et si $P \in A^{(\mathbb{N})}$, nous définissons $P(\alpha)$ par

$$P(\alpha) = \left(\sum_{i=0}^n a_i e_i \right)(\alpha) = \sum_{i=0}^n a_i \alpha^i, \quad (1.360)$$

étant entendu que $\alpha^0 = 1$ dans A .

Cette définition s'étend immédiatement au cas où B est un anneau qui étend A . Dans ce cas nous pouvons définir $P(b)$ pour tout $P \in \mathbb{A}^{(\mathbb{N})}$ et $b \in B$ avec la même formule (1.360).

Le produit C'est ici que la structure particulière de $\mathbb{N}$ est utilisée. Nous définissons le produit $A^{\mathbb{N}} \times A^{(\mathbb{N})} \rightarrow A^{(\mathbb{N})}$ de la façon suivante. Si $(P_k)_{k \in \mathbb{N}}$ est la suite (presque partout nulle) d'éléments de A qui définit P et si $(Q_k)_{k \in \mathbb{N}}$ est celle de Q , nous notons

$$(PQ)_n = \sum_{k=0}^n P_k Q_{n-k}, \quad (1.361)$$

et donc $PQ = \sum_i (PQ)_i e_i$. Plus explicitement,

$$\left(\sum_{i=0}^n a_i e_i \right) \left(\sum_{j=0}^m b_j e_j \right) = \sum_{k=0}^{\infty} \left(\sum_{\substack{(i,j) \in \mathbb{N}^2 \\ i+j=k}} a_i b_j \right) e_k. \quad (1.362)$$

Notons qu'à droite, la somme sur k est une somme finie.

Proposition 1.243.

Soit un anneau A . À propos de structure sur $A^{(\mathbb{N})}$.

- (1) Avec le produit, l'ensemble $A^{(\mathbb{N})}$ devient un anneau.
- (2) L'application

$$\begin{aligned} g: A^{(\mathbb{N})} &\rightarrow A \\ P &\mapsto P(\alpha) \end{aligned} \quad (1.363)$$

est un morphisme d'anneaux⁷⁹. En particulier, $(PQ)(\alpha) = P(\alpha)Q(\alpha)$.

Démonstration. En plusieurs points

Anneau L'identité pour le produit dans $A^{(\mathbb{N})}$ est le polynôme donné par $a_0 = 1$ et $a_i = 0$ pour $i \neq 0$. Cela se vérifie en utilisant directement la définition (1.362). La distributivité aussi⁸⁰.

Le morphisme Nous notons P_k les éléments de la suite définissant P et Q_k ceux de Q . Alors nous avons

$$(P + Q)(\alpha) = \sum_k (P_k + Q_k) \alpha^k = \sum_k P_k \alpha^k + \sum_k Q_k \alpha^k = P(\alpha) + Q(\alpha). \quad (1.364)$$

Vous aurez noté que la première égalité était la définition (1.341b). De même,

$$P(\alpha)Q(\alpha) = \left(\sum_n P_n \alpha^n \right) \left(\sum_k Q_k \alpha^k \right) = \sum_k Q_k \left(\sum_n P_n \alpha^n \right) \alpha^k = \sum_k \sum_n Q_k P_n \alpha^{n+k} \quad (1.365a)$$

$$= \sum_m \left(\sum_{l=0}^m P_l Q_{m-l} \right) \alpha^m = \sum_m (PQ)_m \alpha^m = (PQ)(\alpha). \quad (1.365b)$$

□

⁷⁹. Définition 1.31.

⁸⁰. Je n'ai pas fait les calculs, écrivez-moi pour me dire si ça va facilement.

Lemme 1.244.

Si $\mathbb{A}$ est commutatif, alors $\mathbb{A}^{(\mathbb{N})}$ est commutatif.

Démonstration. Soient $P, Q \in \mathbb{A}^{(\mathbb{N})}$; pour rappel, le produit est donné par la définition 1.361. L'application

$$\begin{aligned} \varphi: \{0, \dots, n\} &\rightarrow \{0, \dots, n\} \\ k &\mapsto n - k \end{aligned} \quad (1.366)$$

est une bijection. Voici maintenant le calcul :

$$(PQ)_n = \sum_{k=0}^n P_k Q_{n-k} \quad (1.367a)$$

$$= \sum_{k=0}^n P_{\varphi(k)} Q_{n-\varphi(k)} \quad (1.367b)$$

$$= \sum_{k=0}^n P_{n-k} Q_k \quad (1.367c)$$

$$= \sum_{k=0}^n Q_k P_{n-k} \quad (1.367d)$$

$$= (QP)_n. \quad (1.367e)$$

Justifications

- Pour (1.367b). Lemme 1.206 et le fait que φ soit une bijection.
- Pour (1.367d). Commutativité de $\mathbb{A}$.

□

1.14.2 La notation $A[X]$

Si A est un anneau, nous avons déjà défini les polynômes en une indéterminée sur A comme étant le module $A^{(\mathbb{N})}$ qui est devenu un anneau par la proposition 1.243.

Le polynôme donné par la suite $(a_n)_{n \in \mathbb{N}}$ est souvent notée

$$\sum_k a_k X^k. \quad (1.368)$$

Par exemple avec $a = (4, 2, 8)$ nous avons $a = 8X^2 + 2X + 4$. Nous utiliserons souvent cette notation, qui est très pratique parce qu'elle s'adapte bien aux règles de multiplication et d'addition, en particulier la distributivité.

Il y a (au moins) deux façons de comprendre ce que signifie réellement « X » dans cette notation.

1.14.2.1 Première façon (qui botte en touche)

La première est de dire qu'il n'a pas de significations, et que X^2 est un simple abus de notations pour écrire $(0, 0, 1, 0, \dots)$. Avec cette façon de voir, nous notons l'anneau des polynômes sur A par « $A[X]$ » où le X n'a pas d'autres raisons d'être que d'avertir le lecteur que nous réservons la lettre « X » pour utiliser la notation pratique des polynômes.

1.14.2.2 Seconde façon (la bonne)

La seconde façon de voir le « X » est de nous rappeler que $A^{(\mathbb{N})}$ a une base en tant de module : les e_k dont nous avons parlé plus haut. Nous posons $X = e_1$, et nous prenons la convention $X^0 = 1$. Alors nous avons $e_k = X^k$ et nous notons $A[X]$ l'anneau $A^{(\mathbb{N})}$ exprimé avec X .

Dans les deux cas, il n'est pas vraiment légitime d'écrire des égalités comme « $P(X) = X^2 + 2X - 3$ », et encore moins de dire « Le polynôme P , évalué en X vaut $X^2 + 2X - 3$ » : il est plus correct d'écrire « $P = X^2 + 2X - 3$ ».

Le lemme suivant montre que ces notations tombent vraiment à point. La véritable difficulté de l'énoncé est de comprendre qu'il n'est pas trivial.

Nous avons vu dans la définition 1.242 que si B est un anneau qui étend A , et si $P \in A[X]$, alors nous avons une définition de $P(b)$ pour tout $b \in B$. Nous appliquons cela à $B = A[X]$, qui est un anneau qui étend A . Autrement dit, si P et Q sont des polynômes, ça a un sens d'écrire $P(Q)$ et le résultat sera un élément de $A[X]$.

Dans le cas particulier $Q = X$, nous avons une chouette formule.

Lemme 1.245.

Nous avons

$$P(X) = P \quad (1.369)$$

pour tout $P \in A[X]$.

Démonstration. Si $P = (a_k)_{k \in \mathbb{N}}$ alors par définition $P(\alpha) = \sum_k a_k \alpha^k$ dès que α est dans un anneau B qui étend A . Nous considérons le cas particulier $B = A[X]$ et $\alpha = X$, c'est-à-dire $Q = (0, 1, 0, \dots)$, l'élément $P(X)$ de $A[X]$ vaut

$$\sum_k a_k X^k, \quad (1.370)$$

qui est exactement P lui-même. □

Mais il faut bien comprendre que si P est le polynôme $(-3, 2, 1, 0, \dots)$, noté $X^2 + 2X - 3$, écrire $P(X) = X^2 + 2X - 3$ est une pirouette de notations que rien ne justifie par rapport à simplement écrire $P = X^2 + 2X - 3$.

1.14.3 Action du groupe symétrique

Définition 1.246 (Thème 65).

Une **action de groupe** G sur un ensemble E est la donnée, pour chaque élément $g \in G$, d'une fonction $\phi_g : E \rightarrow E$, de telle sorte que :

$$\begin{aligned} \phi_e(x) &= x, & \forall x \in E; \\ \phi_{gh}(x) &= \phi_g(\phi_h(x)), & \forall g, h \in G, \forall x \in E. \end{aligned}$$

On dit dans ce cas que G **agit** sur E .

Par souci de notations, nous notons $\mathcal{P}_n(A)$ l'anneau des polynômes de n variables sur A . La propriété universelle de $\mathcal{P}_n(A) = A^{(\mathbb{N}^n)}$ du théorème 1.220 nous donne une application

$$g : \text{Fun}(\mathbb{N}^n, \mathcal{P}_n(A)) \rightarrow \text{Hom}_A(\mathcal{P}_n(A), \mathcal{P}_n(A)) \quad (1.371)$$

Avec cela nous pouvons énoncer et démontrer le lemme qui donne l'action de S_n ⁸¹ sur $\mathcal{P}_n(A)$.

Lemme 1.247 ([47]).

Pour $\sigma \in S_n$ nous définissons

$$\begin{aligned} \phi_\sigma : \mathbb{N}^n &\rightarrow \mathcal{P}_n(A) \\ m &\mapsto e_{\sigma(m)}. \end{aligned} \quad (1.372)$$

Alors l'application

$$\begin{aligned} \rho : S_n &\rightarrow \text{Hom}_A(\mathcal{P}_n(A), \mathcal{P}_n(A)) \\ \sigma &\mapsto g(\phi_\sigma) \end{aligned} \quad (1.373)$$

est une action⁸².

81. Définition du groupe symétrique S_n en 1.146.

82. Définition 1.246.

Démonstration. Nous commençons par donner une expression à notre ρ . Un élément de $\mathcal{P}_n(A)$ est de la forme $\sum_{m \in \mathbb{N}^n} a_m e_m$, et nous avons ⁸³

$$\rho(\sigma) \left(\sum_{m \in \mathbb{N}^n} a_m e_m \right) = \sum_m a_m \phi_\sigma(m) = \sum_m a_m e_{\sigma(m)}. \quad (1.374)$$

Nous avons tout de suite $\rho(\text{Id}) = \text{Id}$.

En ce qui concerne la composition, nous avons d'une part

$$\rho(\sigma_1 \sigma_2) \left(\sum_m a_m e_m \right) = g(\phi_{\sigma_1 \sigma_2}) \left(\sum_m a_m e_m \right) = \sum_m a_m e_{\sigma_1 \sigma_2(m)}, \quad (1.375)$$

et d'autre part,

$$\rho(\sigma_1) \rho(\sigma_2) \left(\sum_m a_m e_m \right) = \rho(\sigma_1) \left(\sum_m a_m e_{\sigma_2(m)} \right) \quad (1.376a)$$

$$= \rho(\sigma_1) \left(\sum_m a_{\sigma_2^{-1}(m)} e_m \right) \quad (1.376b)$$

$$= \sum_m a_{\sigma_2^{-1}(m)} e_{\sigma_1(m)} \quad (1.376c)$$

$$= \sum_m a_m e_{\sigma_1 \sigma_2(m)} \quad (1.376d)$$

La proposition 1.207 est utilisée pour (1.376b) et pour (1.376d). $\square$

1.14.4 Corps des fractions

Définition 1.248 ([48]).

Soit un anneau commutatif et intègre ⁸⁴ A . Nous posons $E = A \times A \setminus \{0\}$, et nous définissons les deux opérations suivantes sur E :

$$(1) (a, b) + (c, d) = (ad + cb, bd);$$

$$(2) (a, b)(c, d) = (ac, bd).$$

Et aussi la relation d'équivalence $(a, b) \sim (c, d)$ si et seulement si $ad = bc$.

Le **corps des fractions** de A est le quotient

$$\text{Frac}(A) = (A \times A \setminus \{0\}) / \sim. \quad (1.377)$$

Nous notons a/b la classe de (a, b) .

Lorsque A est un anneau de polynômes ⁸⁵, alors les éléments de $\text{Frac}(A)$ sont des **fractions rationnelles**.

Le fait que A soit intègre est important pour être certain que $bd \neq 0$ sous l'hypothèse que $b, d \neq 0$.

La proposition suivante montre encore que le corps des fractions est le plus petit corps que l'on puisse imaginer à partir d'un anneau.

Proposition 1.249 ([13, 1]).

Soit un anneau commutatif A . Tout corps commutatif contenant un sous-anneau isomorphe ⁸⁶ à A contient un sous-corps isomorphe à $\text{Frac}(A)$.

Démonstration. Soit un corps $\mathbb{K}$ contenant un sous-anneau A' isomorphe à A . Nous notons $\sigma: A' \rightarrow A$ un isomorphisme d'anneaux entre A' et A .

⁸³. La somme est définie par 1.206, et ça va être important. Ah oui, en réalité partout, les sommes sont finies parce que les a_m ($m \in \mathbb{N}^n$) sont presque tous nuls. Il faudrait écrire sur la somme sur $\{m \in \mathbb{N}^n \text{ tel que } a_m \neq 0\}$, mais vous vous imaginez la complication dans la notation.

⁸⁴. Définition 1.174.

⁸⁵. Définition 1.240.

⁸⁶. Morphisme d'anneaux, définition 1.31.

Une partie bien choisie Nous considérons la partie suivante de $\mathbb{K}$:

$$S = \{ab^{-1} \text{ tel que } a, b \in A'\}. \quad (1.378)$$

S est un corps Deux éléments arbitraires de S sont ab^{-1} et xy^{-1} . Nous devons prouver plusieurs choses.

Neutres En prenant $a = b = 1$ nous avons $ab^{-1} = 1 \in S$. En prenant $a = 0$ et $b = 1$ nous avons $ab^{-1} = 0 \in S$.

Somme Il faut remarquer que $ab^{-1} + xy^{-1} = (ay + xb)(by)^{-1}$. En effet,

$$(ay + xb)(xb)^{-1} = (ay + xb)y^{-1}b^{-1} \quad (1.379a)$$

$$= ayy^{-1}b^{-1} + xby^{-1}b^{-1} \quad (1.379b)$$

$$= ab^{-1} + xy^{-1} \quad (1.379c)$$

Justifications :

- Pour (1.379b). Distributivité.
- Pour (1.379c). Commutativité dans A .

Produit Il s'agit du même genre de calculs en utilisant les mêmes propriétés. Nous avons que

$$(ab^{-1})(xy^{-1}) = (ax)(by)^{-1}. \quad (1.380)$$

Ce qui va être notre isomorphisme Ensuite nous montrons que l'application

$$\begin{aligned} \varphi: S &\rightarrow \text{Frac}(A) \\ ab^{-1} &\mapsto \sigma(a)/\sigma(b) \end{aligned} \quad (1.381)$$

est bien définie et est un isomorphisme de corps.

Bien définie Si $ab^{-1} = xy^{-1}$ alors $ay = xb$. Vu que σ est un isomorphisme nous avons aussi $\sigma(a)\sigma(y) = \sigma(x)\sigma(b)$ et donc $\sigma(a)/\sigma(b) = \sigma(x)/\sigma(y)$ par définition des classes de $\text{Frac}(A)$.

Morphisme Deux éléments arbitraires de S sont ab^{-1} et xy^{-1} . Calculons un peu :

$$\varphi((ab^{-1})(xy^{-1})) = \varphi(axy^{-1}b^{-1}) \quad (1.382a)$$

$$= \varphi((ax)(by)^{-1}) \quad (1.382b)$$

$$= \sigma(ax)/\sigma(by) \quad (1.382c)$$

$$= (\sigma(a)/\sigma(b))(\sigma(x)/\sigma(y)) \quad (1.382d)$$

$$= \varphi(ab^{-1})\varphi(xy^{-1}). \quad (1.382e)$$

Justifications :

- Pour (1.382a). Commutativité dans A .
- Pour (1.382b). Associativité dans A .
- Pour (1.382d). Définition 1.248(2) de la multiplication de fractions.

Surjectif Tout élément de $\text{Frac}(A)$ est de la forme a'/b' avec $a', b' \in A$, et donc de la forme $\sigma(a)/\sigma(b)$ avec $a, b \in A'$. Un tel élément est l'image par φ de $ab^{-1} \in S$.

Injectif Si $\varphi(ab^{-1}) = \varphi(xy^{-1})$ alors $\sigma(a)/\sigma(b) = \sigma(x)/\sigma(y)$, et par définition des classes nous avons $\sigma(a)\sigma(y) = \sigma(b)\sigma(x)$. De là nous avons $\sigma(ay) = \sigma(bx)$ et donc $ay = bx$ (parce que σ est un isomorphisme). Nous en déduisons que $ab^{-1} = xy^{-1}$.

□

1.250.

Soit un anneau A et son anneau des polynômes $\mathcal{P}(A)$. Si $\alpha \in A$, nous avons la définition 1.242 qui donne l'évaluation $P(\alpha)$.

Si par contre P et Q sont des polynômes sur A , nous n'avons pas encore défini ce que serait l'évaluation de la fraction rationnelle P/Q en α . Nous comblons à présent ce manque.

Définition 1.251 (Évaluation d'une fraction rationnelle).

Soit un corps $\mathbb{K}$ contenant l'anneau A . Si $R = P/Q \in \text{Frac}(A)$ et si $\alpha \in \mathbb{K}$ nous définissons⁸⁷

$$R(\alpha) = (P/Q)(\alpha) = P(\alpha)Q^{-1}(\alpha). \quad (1.383)$$

Dans cette formule, les polynômes, l'inverse et le produit sont calculés dans $\mathbb{K}$ et non dans A .

Théorème-Définition 1.252.

Soit A un anneau commutatif intègre.

- (1) Il existe un couple $(\mathbb{K}, \epsilon)$ où $\mathbb{K}$ est un corps commutatif et $\epsilon: A \rightarrow \mathbb{K}$ est un morphisme injectif d'anneaux tels que pour tout $\lambda \in \mathbb{K}$, il existe $(a, b) \in A \times A^*$ tels que

$$\lambda = \epsilon(a)(\epsilon(b))^{-1} \quad (1.384)$$

- (2) Si $(\mathbb{K}', \epsilon')$ est un autre couple qui vérifie la propriété, les corps $\mathbb{K}$ et $\mathbb{K}'$ sont isomorphes. Le corps $\mathbb{K}$ associé à l'anneau A est le **corps des fractions** de A , et sera noté $\text{Frac}(A)$.

- (3) Nous posons

$$\begin{aligned} \sigma: A \times A^* &\rightarrow \mathbb{K} \\ (a, b) &\mapsto \epsilon(a)(\epsilon(b))^{-1}. \end{aligned} \quad (1.385)$$

Nous avons

$$\sigma(xa, xb) = \sigma(a, b) \quad (1.386)$$

pour tout $a, b, x \in A$.

1.14.5 Corps totalement ordonné

Définition 1.253.

Ordre et choses reliées dans un corps.

- (1) Un corps $\mathbb{K}$ est **totalement ordonné** s'il existe une relation d'ordre total⁸⁸ tel que
- (1a) $x \leq y$ implique $x + z \leq y + z$ pour tout $x, y, z \in \mathbb{K}$
- (1b) $x \geq 0$ et $y \geq 0$ implique $xy \geq 0$.
- (2) Si $\mathbb{K}$ est un corps totalement ordonné, nous y définissons la valeur absolue par

$$|x| = \begin{cases} x & \text{si } x \geq 0 \\ -x & \text{si } x \leq 0. \end{cases} \quad (1.387)$$

- (3) La suite (x_n) dans le corps totalement ordonné $\mathbb{K}$ est **de Cauchy** si pour tout $\epsilon \in \mathbb{K}^+$, il existe $N \in \mathbb{N}$ tel que si $p, q \geq N$ alors $|x_p - x_q| \leq \epsilon$.
- (4) La suite (x_n) dans le corps totalement ordonné $\mathbb{K}$ est **convergente** s'il existe $q \in \mathbb{K}$ tel que pour tout $\epsilon \in \mathbb{K}^+$, il existe N tel que si $k \geq N$ alors $|x_k - q| \leq \epsilon$.
- (5) Un corps totalement ordonné est **complet** si toute suite de Cauchy y est convergente.
- (6) Si $a, \epsilon \in \mathbb{K}$ avec $\epsilon > 0$ alors nous définissons la **boule ouverte** de centre a et de rayon ϵ par

$$B(a, \epsilon) = \{x \in \mathbb{K} \text{ tel que } |a - x| < \epsilon\}, \quad (1.388)$$

et la **boule fermée** par

$$\overline{B(a, \epsilon)} = \{x \in \mathbb{K} \text{ tel que } |a - x| \leq \epsilon\}. \quad (1.389)$$

Lemme 1.254.

Une suite (x_k) converge vers q si et seulement si pour tout $\epsilon > 0$, il existe $N > 0$ tel que $x_k \in B(q, \epsilon)$ pour tout $k \geq N$.

⁸⁷. Les fractions rationnelles, définition 1.248.

⁸⁸. Définition 1.10.

Démonstration. Il s'agit de mettre côte à côte les points (4) et (6) de la définition 1.253. $\square$

1.255.

Ces boules prendront une nouvelle force avec le super-théorème 7.99.

Parmi ces définitions, celles de suite convergente, de Cauchy et de corps complet seront utilisées dans le cas de $\mathbb{Q}$ (et de $\mathbb{R}$ pour la complétude). Elles seront prouvées être équivalentes aux définitions topologiques dans le cas particulier de $\mathbb{R}$ et $\mathbb{Q}$ lorsque la topologie métrique sera définie. Dans cet état d'esprit nous n'allons pas démontrer tout de suite que $\mathbb{R}$ est un corps complet. Nous allons directement démontrer que c'est un espace topologique complet.

Lemme 1.256 (Règle des signes[49]).

Soit un corps totalement ordonné $\mathbb{K}$ ainsi que $x, y \in \mathbb{K}$. Nous avons :

- (1) Si $x \leq 0$ et $y \leq 0$ alors $xy \geq 0$.
- (2) Si $x \leq 0$ et $y \geq 0$ alors $xy \leq 0$.
- (3) Si $x \geq 0$ et $y \leq 0$ alors $xy \leq 0$.
- (4) $0 \leq 1$.
- (5) Si $x \geq 0$ alors $x^{-1} \geq 0$.

Lemme 1.257 (Propriétés de la valeur absolue).

Soit $\mathbb{K}$ un corps totalement ordonné. Si $x, y \in \mathbb{K}$ alors⁸⁹

- (1) Si $x \geq 0$ alors $-x \leq 0$.
- (2) Si $x \leq 0$ alors $-x \geq 0$.
- (3) $|x| \geq 0$
- (4) $|x| = 0$ si et seulement si $x = 0$
- (5) $|-x| = |x|$.
- (6) $|x + y| \leq |x| + |y|$.

Démonstration. Point par point

- (1) Nous partons de $x \geq 0$ et nous ajoutons $-x$ des deux côtés en profitant de la définition d'un corps totalement ordonné : $x - x \geq -x$ et donc $0 \geq -x$, c'est-à-dire $-x \leq 0$.
- (2) Nous partons de $x \leq 0$ et nous ajoutons $-x$ des deux côtés.
- (3) Si $x \geq 0$ alors c'est vrai. Sinon, $x \leq 0$ et $|x| = -x \geq 0$ par le point (1).
- (4) Si $x = 0$ alors $x = -x$ et $|x| = 0$. Au contraire si $x \neq 0$ alors $-x \neq 0$ et que x soit positif ou négatif, nous aurons toujours $\pm x \neq 0$.
- (5) Il faut décomposer en deux cas selon que $x \geq 0$ et $x \leq 0$. Supposons $x \geq 0$. Alors d'une part $|x| = x$. D'autre part $-x \leq 0$ par le point (1), de telle sorte que

$$|-x| = -(-x) = x. \quad (1.390)$$

Nous avons donc $|x| = |-x| = x$.

Le même raisonnement tient avec $x \leq 0$.

- (6) Nous supposons que $x \leq y$ et nous distinguons divers cas suivant la positivité de x et y .

- (1) Si $x, y \geq 0$. Dans ce cas, $x + y \geq y \geq 0$, donc $|x + y| = x + y = |x| + |y|$.
- (2) Si $x, y \leq 0$. Dans ce cas, $x + y \leq 0$ et nous avons $|x + y| = -x - y = |x| + |y|$.
- (3) Si $x \leq 0$ et $y \geq 0$. Nous subdivisons encore en deux cas suivant que $x + y$ est positif ou négatif. Si $x + y \geq 0$, alors nous écrivons successivement

$$x \leq 0 \quad (1.391a)$$

$$x + y \leq y \leq y + |x| = |x| + |y| \quad (1.391b)$$

89. La « valeur absolue » est définie en (1.253)(2).

et donc $|x + y| = x + y \leq |x| + |y|$.

Nous supposons à présent que $x \leq 0$, $y \geq 0$ et $x + y \leq 0$. Dans ce cas il suffit d'écrire $|x + y| = |(-x) + (-y)|$ pour retomber dans le cas précédent à inversion près de x et y .

□

Remarque 1.258.

La partie (6) est très importante parce que c'est elle qui fera presque toutes les majorations dont nous aurons besoin en analyse. En effet elle donne l'inégalité triangulaire de la façon suivante : si $x, y, z \in \mathbb{K}$ nous avons

$$|x - y| = |(x - z) + (z - y)| \leq |x - z| + |z - y|. \quad (1.392)$$

Lemme 1.259 (À propos de boules).

Soient un corps totalement ordonné $\mathbb{K}$ et des éléments $x, y \in \mathbb{K}$. Soit aussi $\epsilon > 0$ dans $\mathbb{K}$. Nous avons :

(1) Nous avons $y \in B(x, \epsilon)$ si et seulement si $x - \epsilon < y < x + \epsilon$.

(2) Si $y \in \overline{B(x, \epsilon)}$ alors $y \in B(x, \epsilon')$ pour tout $\epsilon' > \epsilon$.

Démonstration. Pour rappel,

$$|x - y| = \begin{cases} x - y & \text{si } x - y \geq 0 \\ y - x & \text{si } x - y \leq 0. \end{cases} \quad (1.393)$$

Nous pouvons maintenant démontrer nos choses.

(1) En deux parties.

$\Rightarrow$ Nous supposons que $|x - y| < \epsilon$.

Si $x - y \geq 0$ alors l'hypothèse signifie $x - y < \epsilon$, ce qui donne $y > x - \epsilon$. Mais l'inégalité $x - y \geq 0$ donne également $x \geq y$ et donc $x + \epsilon \geq y + \epsilon > y$. Notez le jeu de l'inégalité non stricte qui se change en inégalité stricte.

Si $x - y \leq 0$ nous pouvons faire le même raisonnement.

$\Leftarrow$ Des inégalités $x - \epsilon < y$ et $y < x + \epsilon$ nous tirons $x - y < \epsilon$ et $y - x < \epsilon$. Donc quel que soit le signe de $x - y$ nous avons toujours $|x - y| < \epsilon$.

(2) C'est immédiat parce que

$$|x - y| \leq \epsilon < \epsilon'. \quad (1.394)$$

□

Lemme 1.260.

Tout corps totalement ordonné est de caractéristique nulle.

1.15 Les rationnels

Une construction très explicite est faite dans [12]. Ici nous allons prendre plus court :

Définition 1.261.

Le corps des fractions de $\mathbb{Z}$ (définition 1.248) est noté $\mathbb{Q}$ et ses éléments sont les **rationnels**.

1.262.

Les résultats énoncés ici sont utilisés plus bas et servent de guide à une éventuelle contributrice qui voudrait écrire une partie dédiée à $\mathbb{Q}$ et ses propriétés de base⁹⁰. Nous espérons que des preuves se trouvent dans [12]. En tout cas, chère lectrice, je t'invite à ne rien prendre pour évident.

90. Par exemple, définir une relation d'ordre sur $\mathbb{Q}$ et expliciter l'inclusion de $\mathbb{Z}$ dans $\mathbb{Q}$.

Proposition 1.263.*L'application*

$$\begin{aligned} f: \mathbb{Z} &\rightarrow \mathbb{Q} \\ z &\mapsto z/1 \end{aligned} \tag{1.395}$$

est une injection.

Démonstration. Supposons que $f(a) = f(b)$, c'est à dire que $a/1 = b/1$. En vertu de la relation d'équivalence donnée en 1.248, nous avons $a1 = b1$, c'est à dire $a = b$. $\square$

1.264.

À partir de maintenant, nous allons identifier la partie $f(\mathbb{Z})$ à $\mathbb{Z}$. Nous nous autorisons donc à dire que $4 \in \mathbb{Q}$ ou que $-7 \in \mathbb{Q}$, et même que $0 \in \mathbb{Q}$.

Proposition 1.265.*L'ensemble des rationnels est infini dénombrable⁹¹.*

Démonstration. L'ensemble $\mathbb{Z}$ est infini⁹² et la proposition 1.263 donne une injection $f: \mathbb{Z} \rightarrow \mathbb{Q}$. Donc $f(\mathbb{Z})$ est infini.

L'ensemble $\mathbb{Q}$ contient une partie infinie. Il est donc infini par le lemme 1.97.

L'application

$$\begin{aligned} g: \mathbb{Z}^2 &\rightarrow \mathbb{Q} \\ a, b &\mapsto a/b \end{aligned} \tag{1.396}$$

est surjective alors que $\mathbb{Z}^2$ est dénombrable. Le lemme 1.106 dit alors que $\mathbb{Q}$ est fini ou dénombrable. Vu que nous avons déjà prouvé que $\mathbb{Q}$ était infini, nous déduisons que $\mathbb{Q}$ est infini dénombrable. $\square$

1.15.1 Relation d'ordre**Proposition-Définition 1.266.***Pour $a, b, c, d \in \mathbb{Z}$ nous disons que*

$$\frac{a}{b} \geq \frac{c}{d} \tag{1.397}$$

*si et seulement si $ad \geq bc$ dans $\mathbb{Z}$.**Cela est une relation d'ordre total sur $\mathbb{Z}$.***Lemme 1.267.***Tout rationnel est majoré par un naturel.***Proposition 1.268.***Si $q < 1$ dans $\mathbb{Q}$, alors $qx < x$ pour tout $x \in \mathbb{Q}^+$.***Proposition 1.269.***Le corps $\mathbb{Q}$ est archimédien⁹³.***1.15.2 Caractéristique****Lemme 1.270.***Le corps $\mathbb{Q}$ est de caractéristique⁹⁴ nulle.*

91. Ouais, je sais, dans les définitions prises ici, un ensemble dénombrable est toujours infini. Mais l'excès de précision ne tue pas, loin s'en faut.

92. Lemme 1.92.

93. Définition 1.58.

94. Définition 1.231.

1.16 Suite de Cauchy dans un corps totalement ordonné

Lemme 1.271 ([46, 1]).

Tout corps commutatif de caractéristique nulle contient un sous-corps isomorphe à $\mathbb{Q}$.

Démonstration. Soit un corps $\mathbb{K}$ de caractéristique nulle. Nous savons du lemme 1.231 que

$$\begin{aligned}\mu: \mathbb{Z} &\rightarrow \mathbb{K} \\ n &\mapsto n1_{\mathbb{K}}\end{aligned}\tag{1.398}$$

est un morphisme d'anneaux vérifiant $\ker(\mu) = \{0\}$. Nous posons $Z = \mu(\mathbb{Z})$. L'application $\mu: \mathbb{Z} \rightarrow Z$ est un isomorphisme d'anneaux. Prouvons cela :

Morphisme L'application μ est un morphisme par le lemme 1.231.

Surjectif Par définition les éléments de Z sont dans l'image de $\mathbb{Z}$.

Injectif Si $x, y \in \mathbb{Z}$ vérifient $\mu(x) = \mu(y)$, alors $\mu(x - y) = 0$ parce que μ est un morphisme. Mais $\mathbb{K}$ est de caractéristique nulle, c'est à dire $\ker(\mu) = \{0\}$. Donc $x - y = 0$.

Le corps $\mathbb{K}$ contient donc un sous-anneau isomorphe à $\mathbb{Z}$. Vu que $\mathbb{Z}$ et $\mathbb{K}$ sont commutatifs, la proposition 1.249 s'applique et $\mathbb{K}$ contient un sous-corps isomorphe à $\text{Frac}(\mathbb{Z}) = \mathbb{Q}$. $\square$

La proposition suivante donne des précisions à propos du lemme 1.271.

Proposition 1.272 ([1]).

Soit un corps totalement ordonné $\mathbb{K}$. Nous considérons l'application

$$\begin{aligned}\mu: \mathbb{Z} &\rightarrow \mathbb{K} \\ n &\mapsto n \cdot 1_{\mathbb{K}}\end{aligned}\tag{1.399}$$

et ensuite

$$\begin{aligned}\sigma: \mathbb{Q} &\rightarrow \mathbb{K} \\ a/b &\mapsto \mu(a)\mu(b)^{-1}.\end{aligned}\tag{1.400}$$

Alors

- (1) *L'application σ est bien définie.*
- (2) *L'application σ est un morphisme de corps.*
- (3) *Si $q \leq q'$ dans $\mathbb{Q}$, alors $\sigma(q) \leq \sigma(q')$.*

Démonstration. En plusieurs morceaux.

σ est bien définie Montrons que σ est bien définie. Pour cela nous considérons $a, b, x, y \in \mathbb{Z}$ tels que $a/b = x/y$ dans $\mathbb{Q}$. Par définition des classes (définition 1.248 du corps des fractions), nous avons $ay = bx$ dans $\mathbb{Q}$. Vu que μ est un morphisme nous avons alors

$$\mu(a)\mu(y) = \mu(b)\mu(x)\tag{1.401}$$

et donc $\mu(a)\mu(b)^{-1} = \mu(x)\mu(y)^{-1}$, c'est à dire $\sigma(a/b) = \sigma(x/y)$. L'application σ est donc bien définie.

Morphisme pour la somme L'application μ est un morphisme d'anneaux, comme déjà dit depuis le lemme 1.231. Notons aussi que, parce que $\mathbb{K}$ est commutatif,

$$\mu(qy)^{-1} = \mu(q)^{-1}\mu(y)^{-1}.\tag{1.402}$$

En utilisant la définition 1.248(1) de la somme nous avons

$$\sigma(p/q + x/y) = \sigma((py + qx)/qy)\tag{1.403a}$$

$$= [\mu(py) + \mu(qx)]\mu(qy)^{-1}\tag{1.403b}$$

$$= \mu(py)\mu(qy)^{-1} + \mu(qx)\mu(qy)^{-1}\tag{1.403c}$$

$$= \mu(p)\mu(q)^{-1} + \mu(x)\mu(y)^{-1}\tag{1.403d}$$

$$= \sigma(p/q) + \sigma(x/y).\tag{1.403e}$$

Morphisme pour le produit Même genre de calculs que pour la somme.

Croissante Nous savons aussi par lemme 1.256(4) que $1 \geq 0$. Vu que μ est un morphisme d'anneaux,

$$\mu(n+1) = \mu(n) + \mu(1) = \mu(n) + 1 \quad (1.404)$$

La définition 1.253(1a) dit alors que $\mu(n) \geq 0$ pour tout $n \in \mathbb{N}$. Nous avons pour la même raison que si $m \geq n$ dans $\mathbb{N}$, alors $\mu(m) \geq \mu(n)$ dans $\mathbb{K}$.

Soient maintenant $p, q \in \mathbb{N}$, et prouvons que $\sigma(p/q) \geq 0$. D'abord

$$\sigma(p/q) = \mu(p)\mu(q)^{-1} \quad (1.405)$$

où $\mu(p) \geq 0$ et $\mu(q) \geq 0$. Ensuite le lemme 1.256(5) nous indique que $\mu(q)^{-1} \geq 0$. Enfin la condition 1.253(1b) nous permet de conclure que $\sigma(p/q) \geq 0$.

Finalement, si $q_1 \geq q_2$ dans $\mathbb{Q}$, alors $q_1 - q_2 \geq 0$, et nous avons

$$\sigma(q_1) = \sigma(q_2 + q_1 - q_2) = \sigma(q_2) + \sigma(q_1 - q_2) \geq \sigma(q_2) \quad (1.406)$$

par la condition 1.253(1a).

□

1.273.

Si $\mathbb{K}$ est un corps totalement ordonné, la proposition 1.272 nous donne un morphisme de corps $\sigma: \mathbb{Q} \rightarrow \mathbb{K}$ qui respecte l'ordre. Pour $q \in \mathbb{Q}$ et $k \in \mathbb{K}$ nous notons

$$qk = \sigma(q)k. \quad (1.407)$$

Nous pourrions donc écrire $\frac{k}{2}$ pour $\sigma(1/2)k$.

Le lemme suivant explique que la notation (1.407) n'est pas complètement idiote.

Lemme 1.274.

Soit un corps commutatif totalement ordonné $\mathbb{K}$. Soit $k \in \mathbb{K}$. Nous avons

$$k + k = 2k. \quad (1.408)$$

Démonstration. Vu que $\sigma: \mathbb{Q} \rightarrow \mathbb{K}$ est un morphisme, il vérifie $\sigma(1) = 1$, donc

$$k + k = \sigma(1)k + \sigma(1)k \quad (1.409a)$$

$$= (\sigma(1) + \sigma(1))k \quad (1.409b)$$

$$= \sigma(2)k \quad (1.409c)$$

$$= 2k. \quad (1.409d)$$

□

Proposition 1.275.

Toute suite convergente dans un corps totalement ordonné est de Cauchy.

Démonstration. Soit un corps totalement ordonné $\mathbb{K}$ et une suite $x_n \xrightarrow{\mathbb{K}} x$. Soit $\epsilon > 0$. Il est important de se rendre compte que $\epsilon \in \mathbb{K}$ et que l'inégalité est au sens de l'ordre dans $\mathbb{K}$; en particulier ce n'est pas $\epsilon \in \mathbb{R}$ ni $\epsilon \in \mathbb{Q}$. D'ailleurs nous n'avons pas encore défini $\mathbb{R}$.

Vu que (x_n) converge vers x , il existe $N \in \mathbb{N}$ tel que pour tout $k > N$,

$$|x_k - x| < \epsilon. \quad (1.410)$$

Soient $p, q > N$. Alors en utilisant la majoration du lemme 1.257(6),

$$|x_p - x_q| = |(x_p - x) + (x - x_q)| \leq |x_p - x| + |x - x_q| \leq 2\epsilon. \quad (1.411)$$

En analyse en général, on s'arrête là et on dit que (x_n) est de Cauchy parce qu'il n'y a pas vraiment de différence entre réaliser une majoration avec ϵ ou avec 2ϵ . Détaillons toutefois comment ça se passe dans le cas où ϵ est un élément d'un corps totalement ordonné.

Le 2ϵ arrivant à la fin de (1.411) est en réalité $\epsilon + \epsilon = \sigma(2)\epsilon$ en vertu de ce qui est raconté en 1.273 et en vertu du lemme 1.274.

Considérons $\epsilon' = \sigma(1/2)\epsilon$, que nous pouvons noter $\epsilon' = \epsilon/2$. Vu que $\epsilon' > 0$, il existe un N' tel que pour tout $p, q > N'$ nous ayons

$$|x_p - x_q| \leq 2\epsilon' = \sigma(2)\sigma(1/2)\epsilon = \sigma(1)\epsilon = \epsilon. \quad (1.412)$$

Ce dernier ϵ étant bien celui fixé au début de la preuve, nous en déduisons que (x_n) est de Cauchy. $\square$

1.16.1 Suites de Cauchy dans les rationnels

Proposition 1.276 ([12]).

Principales propriétés des suites de Cauchy dans $\mathbb{Q}$.

- (1) Toute suite convergente est de Cauchy⁹⁵.
- (2) Toute suite de Cauchy est bornée.
- (3) Si $x_n \rightarrow 0$ et si (y_n) est bornée, alors $x_n y_n \rightarrow 0$
- (4) Si (x_n) et (y_n) sont de Cauchy alors $(x_n + y_n)$, $(x_n - y_n)$ et $(x_n y_n)$ sont également de Cauchy.
- (5) Si il existe $a, b \in \mathbb{Q}$ tels que $x_n \rightarrow a$ et $y_n \rightarrow b$ alors $x_n + y_n \rightarrow a + b$, $x_n - y_n \rightarrow a - b$ et $x_n y_n \rightarrow ab$.
- (6) Soit (x_n) une suite de Cauchy qui ne converge pas vers zéro. Alors il existe n_0 tel que la suite $\left(\frac{1}{x_n}\right)_{n \geq n_0}$ soit de Cauchy.

Démonstration. Point par point.

- (1) C'est la proposition 1.275.
- (2) Soit (x_n) une suite de Cauchy dans $\mathbb{Q}$. Avec $\epsilon = 1$ dans la définition, si $q > N_1$, nous avons

$$|x_q - x_{N_1}| \leq 1. \quad (1.413)$$

Et donc pour tout q plus grand que N_1 , $x_N - 1 \leq x_q \leq x_N + 1$, ou encore, pour tout n :

$$|x_n| \leq \max\{|x_1|, |x_2|, \dots, |x_N|, |x_N + 1|\}. \quad (1.414)$$

La suite est donc bornée.

- (3) Soit $\epsilon > 0$. Les hypothèses disent qu'il existe un N tel que $|x_n| \leq \epsilon$ dès que $n \geq N$. Et il existe aussi $M \geq 0$ tel que $|y_n| \leq M$ pour tout n . Du coup, lorsque $n \geq N$ nous avons $|x_n y_n| \leq M\epsilon$.
- (4) En ce qui concerne la somme,

$$|x_p + y_p - x_q - y_q| \leq |x_p - x_q| + |y_p - y_q|. \quad (1.415)$$

Soit N_1 tel que si $p, q \geq N_1$ alors $|x_p - x_q| \leq \epsilon$ et N_2 de même pour la suite (y_n) . En prenant $N = \max\{N_1, N_2\}$, la somme (1.415) est plus petite que 2ϵ dès que $p, q \geq N$.

Passons à la démonstration du fait que le produit de deux suites de Cauchy est de Cauchy. Les suites (x_n) et (y_n) sont bornées et quitte à prendre le maximum, nous disons qu'elles sont toutes les deux bornées par le nombre M : pour tout n nous avons $|x_n| \leq M$ et $|y_n| \leq M$. Nous avons :

$$|x_p y_p - x_q y_q| \leq |x_p y_p - x_q y_p| + |x_q y_p - x_q y_q| \leq |y_p| |x_p - x_q| + |x_q| |y_p - y_q|. \quad (1.416)$$

95. Et non la réciproque, qui sera justement la grande innovation des nombres réels.

Vu que (x_n) et (y_n) sont de Cauchy, si p et q sont assez grands, les deux différences sont majorées par ϵ et nous avons

$$|x_p y_p - x_q y_q| \leq M\epsilon + M\epsilon = 2M\epsilon, \quad (1.417)$$

ce qui prouve que $(x_n y_n)$ est de Cauchy.

- (5) En ce qui concerne la somme, nous pouvons tout de suite calculer

$$|x_n + y_n - (a + b)| \leq |x_n - a| + |y_n - b|. \quad (1.418)$$

Il existe une valeur de n à partir de laquelle le premier terme est plus petit que ϵ et une à partir de laquelle le second terme est plus petit que ϵ . En prenant le maximum des deux, la somme est plus petite que 2ϵ .

En ce qui concerne le produit,

$$|x_n y_n - ab| \leq |x_n y_n - a y_n| + |a y_n - ab| \leq |y_n| |x_n - a| + |a| |y_n - b|. \quad (1.419)$$

Les suites $|x_n - a|$ et $|y_n - b|$ convergent vers zéro ; la suite (y_n) est bornée parce que convergente (combinaison des points (1) et (2)) et a (la suite constante) est également bornée. Donc par le point (3), nous avons

$$y_n |x_n - a| + a |y_n - b| \rightarrow 0. \quad (1.420)$$

Au passage nous avons également utilisé la propriété de la somme que nous venons de démontrer.

- (6) Soit (x_n) une suite de Cauchy dans $\mathbb{Q}$ ne convergeant pas vers zéro : il existe $\alpha > 0$ tel que pour tout $N \in \mathbb{N}$, il existe $n \geq N$ tel que $|x_n| > \alpha$. Mais notre suite est de Cauchy, donc il existe $n_0 \in \mathbb{N}$ tel que si $p, q \geq n_0$ alors

$$|x_p - x_q| \leq \frac{\alpha}{2}. \quad (1.421)$$

En fixant $N = n_0$, on obtient un naturel $n \geq n_0$ tel que $|x_n| \geq \alpha$. De plus, comme la suite est de Cauchy, si $p > n$ nous avons aussi $|x_n - x_p| \leq \frac{\alpha}{2}$. Cela implique $|x_p| \geq \frac{\alpha}{2}$ et en particulier $x_p \neq 0$.

Nous venons de prouver que la suite ne s'annule plus à partir de l'indice n , et même que $|x_k| \geq \alpha/2$ pour tout $k \geq n$. La suite $(1/x_k)_{k \geq n}$ est donc bien définie.

Soit $\epsilon > 0$. Soit n_0 tel que $|x_p - x_q| < \epsilon$ pour tout $p, q > n_0$. Soit K plus grand que n_0 et que n . En prenant $p, q \geq K$, nous avons $|x_p| > \frac{\alpha}{2}$ et $|x_q| > \frac{\alpha}{2}$. Nous en déduisons que

$$\left| \frac{1}{x_p} - \frac{1}{x_q} \right| \leq \frac{|x_q - x_p|}{|x_p x_q|} \leq \frac{4}{\alpha^2} |x_q - x_p| \leq \frac{4}{\alpha^2} \epsilon. \quad (1.422)$$

Donc $\left(\frac{1}{x_n} \right)$ est de Cauchy.

□

1.17 Insuffisance des rationnels

Nous allons voir qu'il n'existe pas de nombres rationnels x tels que $x^2 = 2$, mais que pourtant il existe une infinité de suites de rationnels (x_n) tels que $x_n^2 \rightarrow 2$.

Lemme 1.277.

Un entier x est pair si et seulement si l'entier x^2 est pair.

Démonstration. Si x est un nombre pair, alors il existe un entier a tel que $x = 2a$ alors $x^2 = 4a^2$ est pair.

Inversement, si x est impair alors il existe un entier a tel que $x = 2a + 1$ et alors $x^2 = 4a^2 + 4a + 1 = 2(2a^2 + 2a) + 1$ est impair. □

Le théorème 3.35 nous dira que tous les $\sqrt{n}$ sont irrationnels dès que n n'est pas un carré parfait. Voici déjà le résultat pour $n = 2$. Le fait que $\sqrt{2}$ existe dans $\mathbb{R}$ sera la proposition 1.333.

Proposition 1.278 (Irrationalité de $\sqrt{2}$).

Il n'existe pas de fractions d'entiers dont le carré soit égal à 2.

Démonstration. Nous supposons que la fraction d'entiers a/b est telle que $a^2/b^2 = 2$, et nous allons construire une suite d'entiers strictement décroissante et strictement positive, ce qui est impossible.

Grâce au lemme 1.277 nous avons successivement les affirmations suivantes :

- $\frac{a^2}{b^2} = 2$ avec $a \neq 0$ et $b \neq 0$.
- $a^2 = 2b^2$, donc a^2 est pair.
- a est alors pair et a^2 est divisible par 4. Soit $a^2 = 4k$.
- $4k/b^2 = 2$, donc $4k = 2b^2$, donc $b^2 = 2k$ et b^2 est pair.
- Nous déduisons que b est pair.

La fraction $\frac{a/2}{b/2}$ est alors une nouvelle fraction d'entiers dont le carré vaut 2. En procédant de la même façon, en remplaçant a par $a/2$ et b par $b/2$, on obtient que la fraction d'entiers $\frac{a/4}{b/4}$ a la même propriété.

En particulier, tous les nombres de la forme $a/2^n$ sont des entiers. Ils forment une suite strictement décroissante d'entiers strictement positifs. Impossible, me diriez-vous ? Et vous auriez bien raison : toute partie non vide de $\mathbb{N}$ admet un plus petit élément⁹⁶. Il n'y a donc pas de fractions d'entiers dont le carré vaut 2. $\square$

Lemme 1.279 (Série géométrique).

Si $q \neq 1$ dans $\mathbb{Q}$ et $p \in \mathbb{N}$ nous avons

$$\sum_{k=0}^p q^k = \frac{1 - q^{p+1}}{1 - q}. \quad (1.423)$$

Démonstration. En posant $S_p = 1 + q + q^2 + \cdots + q^p$, nous avons $S_p - qS_p = 1 - q^{p+1}$ et donc

$$S_p = \sum_{k=0}^p q^k = \frac{1 - q^{p+1}}{1 - q}. \quad (1.424)$$

$\square$

Proposition 1.280.

La suite donnée par

$$x_n = 1 + \frac{1}{1!} + \cdots + \frac{1}{n!} \quad (1.425)$$

est de Cauchy et ne converge pas dans $\mathbb{Q}$.

96. Voir [12], et attention : ce n'est pas tout à fait évident.

Démonstration. Si $p > q > 0$ nous avons

$$x_p - x_q = \sum_{k=q+1}^p \frac{1}{k!} \quad (1.426a)$$

$$\leq \sum_{k=q+1}^p \frac{1}{(q+1)!} \frac{1}{(q+1)^{k-q-1}} \quad (1.426b)$$

$$\leq \frac{1}{(q+1)!} \lim_{p \rightarrow \infty} \sum_{k=0}^p \frac{1}{(q+1)^k} \quad (1.426c)$$

$$= \frac{1}{(q+1)!} \frac{1}{1 - \frac{1}{q+1}} \quad (1.426d)$$

$$= \frac{1}{(q+1)!} \frac{q+1}{q} \quad (1.426e)$$

$$= \frac{1}{q!q}. \quad (1.426f)$$

Justifications :

- Pour (1.426b), il s'agit de remplacer dans $k!$ tous les facteurs plus grands que $(q+1)$ par $q+1$. Cela rend le dénominateur plus petit.
- Pour (1.426c), il y a une inégalité parce que la suite $p \mapsto \sum_{k=0}^p 1/(q+1)^k$ est une suite strictement croissante.
- Pour (1.426d), le lemme 1.279 donne la valeur de la somme finie. En ce qui concerne la limite, nous avons demandé $p > q > 0$ et donc $q+1 > 1$. Dans ce cas la limite fonctionne.

Cette inégalité une fois établie nous permet de prouver les assertions. La suite (x_n) est de Cauchy car, pour tout $\epsilon \in \mathbb{Q}$ s'écrivant $\epsilon = \frac{a}{b}$ avec $a, b \in \mathbb{N}$, en prenant $p, q > b$, nous avons

$$x_p - x_q \leq \frac{1}{b!b} < \frac{1}{b} < \frac{a}{b} = \epsilon. \quad (1.427)$$

Montrons par l'absurde que cette suite ne converge pas dans $\mathbb{Q}$. Pour cela, nous supposons que $\lim_{n \rightarrow \infty} x_n = \frac{a}{b} \in \mathbb{Q}$. Pour tout $p > q$ nous avons établi

$$0 < x_p - x_q < \frac{1}{qq!}. \quad (1.428)$$

Prenons la limite $p \rightarrow \infty$; par stricte croissance de la suite, les inégalités restent strictes :

$$0 < \frac{a}{b} - x_q < \frac{1}{qq!}. \quad (1.429)$$

Si $n > b$ alors nous pouvons écrire

$$\frac{a}{b} - x_n = \frac{\alpha}{n!} \quad (1.430)$$

avec $\alpha \in \mathbb{Z}$ parce que le dénominateur commun entre $\frac{a}{b}$ et x_n est dans $n!$. En prenant donc $q > n$ dans (1.429) nous pouvons écrire

$$0 < \frac{\alpha}{q!} < \frac{1}{qq!}, \quad (1.431)$$

c'est-à-dire $0 < \alpha < \frac{1}{q}$, ce qui est impossible pour $\alpha \in \mathbb{Z}$. □

Lemme 1.281.

Soit $A > 0$ dans $\mathbb{Q}$. Il existe un rationnel $q > 0$ tel que $q^2 < A$.

Démonstration. Vu que $\mathbb{Q}$ est archimédien (proposition 1.269), il existe $n \in \mathbb{N}$ tel que $1 < nA$. Pour ce n , nous avons

$$\left(\frac{1}{n}\right)^2 < \frac{1}{n} < A. \quad (1.432)$$

□

La proposition suivante donne une suite de rationnels qui convergerait dans $\mathbb{R}$ vers $\sqrt{A}$ (non encore défini à ce stade). Il est expliqué dans [50] que la suite peut être vue comme une forme de méthode de Newton 34.54; voir l'exemple 34.57. Si vous aimez les dessins et les approches géométriques, il y a une explication sur Wikipédia[51].

Proposition 1.282 ([50]).

Soient $A > 0$ dans $\mathbb{Q}$ et $x_0 \in \mathbb{Q}$. La suite (x_k) définie par

$$x_{k+1} = \frac{1}{2} \left(x_k + \frac{A}{x_k} \right) \quad (1.433)$$

a les propriétés suivantes :

- (1) La suite $y_k = x_k^2$ converge dans $\mathbb{Q}$ vers A .
- (2) La suite (x_k) est de Cauchy dans $\mathbb{Q}$.
- (3) La suite (x_k) ne converge pas dans $\mathbb{Q}$ dans le cas de $A = 2$.

Démonstration. En plusieurs points.

La suite s_k En posant $y_k = x_k^2$ nous calculons que

$$y_{k+1} - A = \frac{(y_k - A)^2}{4y_k}. \quad (1.434)$$

Autrement dit, la suite $s_k = y_k - A$ vérifie

$$s_{k+1} = \frac{s_k^2}{4(A + s_k)}. \quad (1.435)$$

Quelle que soit la valeur de $s_0 = x_0^2 - A$, nous avons

$$s_1 = \frac{s_0^2}{4(A + s_0)} = \frac{(x_0^2 - A)^2}{4(A + x_0^2 - A)} = \frac{(x_0^2 - A)^2}{4x_0^2} > 0. \quad (1.436)$$

Donc à partir de s_1 , tous les éléments sont positifs. Vu que $A > 0$ nous avons aussi

$$s_{k+1} < \frac{s_k^2}{4s_k} = \frac{s_k}{4} \quad (1.437)$$

et donc $s_k < s_0/4^k$. Donc $s_k \rightarrow 0$.

La suite (y_k) Nous venons de prouver que si $y_k = A + s_k$, alors $s_k \rightarrow 0$. Autrement dit, la suite y_k converge vers A dans $\mathbb{Q}$.

La suite (y_k) est donc de Cauchy par la proposition 1.276(1).

La suite (x_k) est de Cauchy Soit $\epsilon > 0$ dans $\mathbb{Q}$. Vu que (y_k) est de Cauchy, il existe $n_0 \in \mathbb{N}$ tel que

$$|x_r^2 - x_s^2| < \epsilon \quad (1.438)$$

pour tout $r, s \geq n_0$.

Soit par ailleurs $q \neq 0$ dans $\mathbb{Q}$ tel que $q^2 < A$, assuré par le lemme 1.281. Quitte augmenter la valeur de n_0 , nous supposons que $x_r, x_s > q$, et en particulier que $x_r + x_s \neq 0$. Cela permet d'écrire d'abord

$$x_r^2 - x_s^2 = (x_r + x_s)(x_r - x_s) \quad (1.439)$$

et ensuite de prendre la valeur absolue et de diviser par $|x_r + x_s|$:

$$|x_r - x_s| = \frac{|x_r^2 - x_s^2|}{|x_r + x_s|} < \frac{\epsilon}{2q}. \quad (1.440)$$

Donc (x_k) est une suite de Cauchy.

Pas de convergence pour $A = 2$ Supposons que $x_k \rightarrow a \in \mathbb{Q}$. Dans ce cas nous aurions $x_k^2 \rightarrow a^2 = A = 2$ (proposition 1.276(5)). Mais nous savons par la proposition 1.278 que $a^2 = 2$ est impossible dans $\mathbb{Q}$.

□

Notons que cette proposition ne présume en rien de l'existence ou de la non-existence dans $\mathbb{Q}$ d'un élément qui pourrait décemment être nommé $\sqrt{A}$. Il se fait que le théorème 3.35 dira que $\sqrt{n}$ est soit entier soit irrationnel.

1.283.

Un petit programme en python explorer la suite de la proposition 1.282.

```

1 #!/usr/bin/python3
2
3 def rec(A,x):
4     return ((x**2+A)/x)/2
5
6 A = 3          # Compute square root of 3
7 x = 1000       # Initial guess: 1000
8
9 for i in range(1,100):
10    print(i, x, x**2, x**2-A)
11    x = rec(A, x)

```

tex/frido/codeSnip_4.py

1.18 Les réels

Une construction des réels via les coupures de Dedekind est donnée dans [52].

1.284.

La construction des réels va nécessiter un petit « bootstrap » au niveau de la topologie. En effet la notion de suite de Cauchy est une notion topologique (définition 7.169) alors que la topologie métrique (celle entre autres de $\mathbb{Q}$) ne sera définie que par le théorème 7.99. Nous avons donc dû définir en la définition 1.253 *ex nihilo* les notions de

- suite de Cauchy
- suite convergente
- complétude

Nous allons ensuite construire $\mathbb{R}$ comme ensemble de classes d'équivalence de suites de Cauchy dans $\mathbb{Q}$. Ce ne sera que plus tard, après avoir défini la notion d'espace métrique que nous allons voir que sur $\mathbb{R}$, ces trois notions coïncident avec celles topologiques⁹⁷. Et par conséquent que $\mathbb{R}$ sera un espace métrique complet⁹⁸.

Dans cette optique, il est intéressant de lire ce que dit Wikipédia à propos des suites de Cauchy dans l'article consacré à la construction des nombres réels[53].

1.18.1 L'ensemble

Soit $\mathcal{E}$ l'ensemble des suites de Cauchy⁹⁹ dans $\mathbb{Q}$. Soit aussi l'ensemble $\mathcal{E}_0$ constituée des suites qui convergent vers zéro¹⁰⁰.

97. Proposition 7.176.

98. Théorème 1.319 pour la complétude en tant que corps et théorème 1.275 pour la complétude en tant que espace métrique.

99. Définition 1.253(3)

100. Nous rappelons qu'à ce niveau nous n'avons pas encore prouvé que toutes les suites de Cauchy convergent.

En posant

$$x + y = (x_n + y_n) \quad (1.441)$$

et

$$xy = (x_n y_n), \quad (1.442)$$

l'ensemble $\mathcal{E}$ devient un anneau¹⁰¹ commutatif dont le neutre de l'addition est la suite constante $x_n = 0$ et le neutre pour la multiplication est la suite constante $x_n = 1$.

Proposition 1.285.

La partie $\mathcal{E}_0$ est un idéal¹⁰² de l'anneau $\mathcal{E}$.

Démonstration. Nous savons par la proposition 1.276(1) que les suites convergentes sont de Cauchy ; par conséquent $\mathcal{E}_0 \subset \mathcal{E}$.

L'ensemble structuré $(\mathcal{E}_0, +)$ est un sous-groupe de $\mathcal{E}$ par les propriétés de la proposition 1.276 (il s'agit du fait que la somme de deux suites convergent vers zéro est une suite convergente vers zéro).

En ce qui concerne la propriété fondamentale des idéaux, si $x \in \mathcal{E}_0$ et $y \in \mathcal{E}$ nous devons prouver que $xy \in \mathcal{E}_0$. Vu que $(\mathcal{E}_0, \cdot)$ est commutatif, cela suffira pour être un idéal bilatère. Vu que y est une suite de Cauchy, elle est bornée ; et étant donné que $x \rightarrow 0$ nous avons alors $xy \rightarrow 0$ (par la proposition 1.276(3)). $\square$

Théorème-Définition 1.286 (L'anneau des réels[12]).

Sur l'ensemble quotient $\mathcal{E}/\mathcal{E}_0$, les opérations

$$(1) \quad \bar{u} + \bar{v} = \overline{u + v}$$

$$(2) \quad \bar{u} \cdot \bar{v} = \overline{uv}$$

sont bien définies et donnent à $\mathcal{E}/\mathcal{E}_0$ une structure de corps commutatif appelé **corps des réels** et noté $\mathbb{R}$

Démonstration. Nous divisons la preuve en plusieurs parties.

Les opérations sont bien définies La partie $\mathcal{E}_0$ est un idéal par la proposition 1.285. Le quotient est donc bien défini et est un anneau par la proposition 1.168(2).

Caractérisation des classes Soit $q \in \mathbb{Q}$ et une suite x convergente vers q . Cette suite est de Cauchy comme toute suite convergente. Montrons que

$$\bar{x} = \{\text{suites qui convergent vers } q\}. \quad (1.443)$$

Si $y \in \bar{x}$ alors $y = x + h$ avec $h \in \mathcal{E}_0$, et comme $h_n \rightarrow 0$, on a $y_n \rightarrow q$. Réciproquement, si $y_n \rightarrow q$ alors pour chaque n nous avons

$$y_n = x_n + (y_n - x_n), \quad (1.444)$$

mais $y_n - x_n \rightarrow 0$. Donc la suite $y - x \in \mathcal{E}_0$ ce qui signifie que $y \in \bar{x}$.

Neutre et unité Il est vite vérifié que $\bar{0}$, la classe de la suite constante égale à zéro est neutre pour l'addition. De même, $\bar{1}$, est un neutre pour la multiplication.

Corps Nous devons prouver que tout élément non nul est inversible. C'est-à-dire que si $x \in \mathcal{E}$ ne converge pas vers zéro¹⁰³ alors il existe $y \in \mathcal{E}$ tel que $xy \in \bar{1}$.

Nous savons par la proposition 1.276(6) que x étant une suite de Cauchy dans $\mathbb{Q}$, il existe $n_0 \in \mathbb{N}$ tel que $\left(\frac{1}{x_n}\right)_{n \geq n_0}$ est une suite de Cauchy. Nous posons alors

$$y_n = \begin{cases} 0 & \text{si } n \leq n_0 \\ \frac{1}{x_n} & \text{si } n > n_0. \end{cases} \quad (1.445)$$

101. Définition 1.30.

102. Définition 1.167.

103. $x \in \mathcal{E}$ peut soit ne pas converger du tout, soit converger vers autre chose que zéro.

Nous avons alors

$$(xy)_n = \begin{cases} 0 & \text{si } n \leq n_0 \\ 1 & \text{si } n > n_0 \end{cases} \quad (1.446)$$

et donc $xy \in \bar{1}$.

□

1.287 (Quelques notations entre $\mathbb{Q}$ et $\mathbb{R}$).

Si $k \mapsto x_k$ est une suite, nous notons (x_k) avec des parenthèses la suite elle-même. Le k dans (x_k) est un indice muet, et dans les cas où il peut y avoir une ambiguïté, nous pouvons noter $(x_k)_{k \in \mathbb{N}}$. Cette dernière notation est plus lourde, mais plus exacte.

Le mieux est d'écrire simplement x la suite, mais alors il faut être prudent et ne pas noter x la limite. Nous éviterons donc d'écrire $x_k \rightarrow x$.

Si (x_k) est une suite de Cauchy dans $\mathbb{Q}$, nous notons $\bar{x}$ l'élément de $\mathbb{R}$ qui lui correspond. En fait $\bar{x} = (x_k) : \bar{x}$ est la suite-elle-même, mais pour nous souvenir de l'origine nous allons adopter cette notation.

D'autre part nous définissons

$$\begin{aligned} \varphi: \mathbb{Q} &\rightarrow \mathbb{R} \\ q &\mapsto \overline{[k \mapsto q]}, \end{aligned} \quad (1.447)$$

c'est-à-dire que $\varphi(q)$ est la classe de la suite constante $x_k = q$.

Proposition 1.288.

Soit l'application

$$\begin{aligned} \varphi: \mathbb{Q} &\rightarrow \mathbb{R} \\ q &\mapsto \bar{q}. \end{aligned} \quad (1.448)$$

où par $\bar{q}$ nous entendons la classe de la suite constante égale à q (qui est de Cauchy).

- (1) C'est un homomorphisme de corps injectif.
- (2) Image(φ) est un sous-corps de $\mathbb{R}$
- (3) $\varphi: \mathbb{Q} \rightarrow \text{Image}(\varphi)$ est un isomorphisme de corps.

Démonstration. Le fait que ce soit un homomorphisme est simplement

$$\begin{aligned} \text{— } \varphi(q + q') &= \overline{q + q'} = \bar{q} + \bar{q}' \\ \text{— } \varphi(qq') &= \overline{qq'} = \bar{q}\bar{q}'. \end{aligned}$$

En ce qui concerne l'injectivité, si q est tel que $\varphi(q) = \bar{0} = \mathcal{E}_0$, c'est que

$$\varphi(q) = \{\text{suites de Cauchy qui convergent vers zéro}\} \quad (1.449)$$

Mais nous savons aussi que ¹⁰⁴

$$\varphi(q) = \bar{q} = \{\text{suites de Cauchy qui convergent vers } q\} \quad (1.450)$$

Nous en déduisons que $q = 0$.

□

Lorsque dans la suite nous parlerons d'un élément de $\mathbb{Q}$ comme étant un réel, nous aurons en tête l'image de cet élément par φ .

Lemme 1.289.

Soient $q, l \in \mathbb{Q}$ tels que $\bar{q} = \bar{l}$. Alors $q = l$ dans $\mathbb{Q}$.

104. Voir dans la démonstration du théorème 1.286.

Démonstration. La suite constante $x_n = q$ est un représentant de $\bar{q}$, et la suite constante $y_n = l$ est représentant de $\bar{l}$. Dire que $\bar{l} = \bar{q}$ signifie qu'il existe une suite $z \in \mathcal{E}_0$ tel que

$$x = y + z. \quad (1.451)$$

Pour tout n nous avons donc $x_n = y_n + z_n$, ou encore

$$z_n = q - l \quad (1.452)$$

pour tout n . Vu que z est une suite constante, elle en peut appartenir à $\mathcal{E}_0$ que si elle est la suite constante nulle, c'est à dire si $q = l$. $\square$

1.18.2 Relation d'ordre

Définition 1.290.

Nous définissons les parties $\mathcal{E}^+$ et $\mathcal{E}^-$ de $\mathcal{E}$ par

- (1) $x \in \mathcal{E}^+$ si et seulement si pour tout $\epsilon > 0$ (ϵ est dans $\mathbb{Q}$), il existe N_ϵ tel que $n > N_\epsilon$ implique $x_n > -\epsilon$.
- (2) $x \in \mathcal{E}^-$ si et seulement si pour tout $\epsilon > 0$, il existe N_ϵ tel que $n > N_\epsilon$ implique $x_n < \epsilon$.

Nous notons aussi $\mathcal{E}^{++} = \mathcal{E}^+ \setminus \mathcal{E}_0$.

Dans le lemme suivant, le point (2) peut sembler perturbant. Il s'agit de dire que si x est la classe de la suite constante 0, alors il est le neutre pour l'addition dans $\mathbb{R}$.

Lemme 1.291 (À propos du zéro).

Nous avons

- (1) $\mathcal{E}^+ \cap \mathcal{E}^- = \{\bar{0}\}$.
- (2) Si $x = \bar{0}$ alors $x = 0$.

Lemme 1.292.

Les parties $\mathcal{E}^+$ et $\mathcal{E}^-$ partitionnent $\mathcal{E}$ de la façon suivante :

- (1) $\mathcal{E}^+ \cap \mathcal{E}^- = \mathcal{E}_0$
- (2) $\mathcal{E}^+ \cup \mathcal{E}^- = \mathcal{E}$

Démonstration. On prouve d'abord que $\mathcal{E}^+ \cap \mathcal{E}^- \subset \mathcal{E}_0$, l'inclusion inverse est évidente. Soit $\epsilon > 0$ et $x \in \mathcal{E}^+ \cap \mathcal{E}^-$. Il existe un $N \in \mathbb{N}$ tel que $x_n > -\epsilon$ et $x_n < \epsilon$ pour tout $n \geq N$. Par conséquent, $|x_n| \leq \epsilon$ pour tout $n \geq N$ et la suite x converge vers zéro, c'est-à-dire $x \in \mathcal{E}_0$.

Pour prouver le second point, soit $x \in \mathcal{E} \setminus \mathcal{E}^-$, et prouvons que $x \in \mathcal{E}^+$. La condition $x \notin \mathcal{E}^-$ donne qu'il existe un $\alpha > 0$ (dans $\mathbb{Q}$) tel que pour tout n , il existe $p > n$ avec $x_p > \alpha$. Mais x est une suite de Cauchy, donc nous avons un n_0 tel que si $n, p \geq n_0$ alors $|x_n - x_p| \leq \frac{\alpha}{2}$. En particulier, si $n \geq n_0$, et si $p > n$ est tel que $x_p > \alpha$, on obtient

$$x_n > \frac{\alpha}{2} > 0 \quad (1.453)$$

Par conséquent $x \in \mathcal{E}^+$ parce que $x \in \mathcal{E}$ et les x_n sont tous positifs à partir d'un certain rang. $\square$

Lemme 1.293 ([1]).

Si $x \in \mathcal{E}^{++}$, alors il existe N tel que $x_n > 0$ pour tout $n > N$.

Démonstration. La suite x ne tend pas vers zéro. Donc il existe $\delta > 0$ tel que pour tout $N > 0$ il existe $n > N$ vérifiant $x_n > \delta$.

Mais la suite x est également de Cauchy. Écrivons cette condition pour $\delta/2$. Il existe $N_2 > 0$ tel que $p, q > N_2$ implique $|x_p - x_q| < \delta/2$.

Nous fixons $n > N_2$ tel que $x_n > \delta$. Alors pour tout $p > N_2$ nous avons aussi

$$|x_p - x_n| < \frac{\delta}{2}. \quad (1.454)$$

Cela implique que $x_p > \delta/2 > 0$ pour tout $p > N_2$. $\square$

La proposition suivante est une version plus précise du lemme 1.293.

Proposition 1.294 ([13]).

Soit $x \in \mathcal{E}^{++}$. Il existe $q \in \mathbb{Q}^+ \setminus \{0\}$ et $N \in \mathbb{N}$ tel que $x_n \geq q$ pour tout $n \geq N$.

Démonstration. Fixons $\epsilon \in \mathbb{Q}^+ \setminus \{0\}$, et procédons par l'absurde. Du coup nous savons trois choses sur la suite (x_n) .

- (1) Hypothèse absurde : pour tout $q \in \mathbb{Q}^+ \setminus \{0\}$ et pour tout $N \in \mathbb{N}$, il existe $p \geq N$ vérifiant $x_p < q$.
- (2) Vu que $x \in \mathcal{E}^{++} \subset \mathcal{E}^+$, il existe $P_1 \in \mathbb{N}$ tel que $x_n > -\epsilon$ pour tout $n \geq P_1$.
- (3) La suite x est de Cauchy. Donc il existe $P_2 \in \mathbb{N}$ tel que si $m, n \geq P_2$, nous avons $|x_m - x_n| < \epsilon/2$.

Nous considérons $P \geq \max\{P_1, P_2\}$ et nous prenons $q = \epsilon/2$, $N = P$ dans la propriété (1). Il existe donc $p > P$ tel que $x_p < \epsilon/2$.

Prenons aussi $n > p$ et écrivons les deux autres propriétés :

- (1) $x_n > -\epsilon$ parce que $n > p > P > P_1$.
- (2) $|x_n - x_p| < \epsilon/2$ parce que $n, p > P > P_2$.

Du coup nous avons

$$x_n < x_p + \frac{\epsilon}{2} < \epsilon, \quad (1.455)$$

et donc $-\epsilon < x_n < \epsilon$.

Au final, nous avons prouvé que pour tout $\epsilon \in \mathbb{Q}^+ \setminus \{0\}$, il existe P tel que $n > P$ implique $|x_n| < \epsilon$. Cela signifie que

$$x_n \xrightarrow{\mathbb{Q}} 0, \quad (1.456)$$

c'est à dire $x \in \mathcal{E}_0$, ce qui est contraire à l'hypothèse. $\square$

Lemme 1.295 ([12]).

Quelques propriétés du partitionnement.

- (1) $x \in \mathcal{E}^-$ si et seulement si $(-x) \in \mathcal{E}^+$
- (2) $x \in \mathcal{E}^+$ et $y \in \mathcal{E}^+$ implique $x + y \in \mathcal{E}^+$
- (3) $x \in \mathcal{E}^+$ et $y \in \mathcal{E}^+$ implique $xy \in \mathcal{E}^+$
- (4) Si $x, y \in \mathcal{E}$ sont tels que $x - y \in \mathcal{E}_0$ alors soit $x, y \in \mathcal{E}^+$ soit $x, y \in \mathcal{E}^-$.

Démonstration. Point par point.

- (1) Définition de $\mathcal{E}^+$ et $\mathcal{E}^-$.
- (2) Pour $n \geq N_{\epsilon/2}$ nous avons $x_n > -\epsilon/2$ et $y_n > -\epsilon/2$. Donc $x_n + y_n > -\epsilon$.
- (3) Si x ou y est dans $\mathcal{E}_0$ alors $xy \in \mathcal{E}_0$ et c'est bon. Si par contre $x, y \in \mathcal{E}^{++}$ alors le lemme 1.293 nous indique que pour n suffisamment grand, $x_n > 0$ et $y_n > 0$. Et dans ce cas, $(xy)_n > 0$, c'est-à-dire $xy \in \mathcal{E}^+$.
- (4) Supposons que $x - y \in \mathcal{E}_0$ avec $x \in \mathcal{E}^+$ et prouvons qu'alors $y \in \mathcal{E}^+$. Soit donc $\epsilon > 0$; il existe n_1 tel que $x_n > -\frac{\epsilon}{2}$ dès que $n \geq n_1$. Mais $x - y \in \mathcal{E}_0$, donc il existe n_2 tel que $|x_n - y_n| < \frac{\epsilon}{2}$ dès que $n \geq n_2$. En prenant n plus grand que n_1 et n_2 , nous avons en même temps

$$\left\{ \begin{array}{l} x_n > -\frac{\epsilon}{2} \\ |x_n - y_n| < \frac{\epsilon}{2} \end{array} \right. \quad (1.457a)$$

$$\left\{ \begin{array}{l} x_n > -\frac{\epsilon}{2} \\ |x_n - y_n| < \frac{\epsilon}{2} \end{array} \right. \quad (1.457b)$$

Cela implique que $y_n > -\epsilon$ et donc que $y \in \mathcal{E}^+$.

Nous pouvons de même prouver que si $x \in \mathcal{E}^-$ alors $y \in \mathcal{E}^-$. $\square$

Définition 1.296 (Positivité dans $\mathbb{R}$).

Vocabulaire et notations.

- (1) Nous notons $\mathbb{R} = \mathcal{E}/\mathcal{E}_0$.
- (2) Nous notons $\mathbb{R}^+ = \bar{\mathcal{E}}^+$.
- (3) Nous notons $\mathbb{R}^- = \bar{\mathcal{E}}^-$.
- (4) Un élément de $\mathbb{R}$ est **positif** s'il est la classe d'une suite de Cauchy appartenant à $\mathcal{E}^+$.
- (5) Un élément de $\mathbb{R}$ est **négatif** s'il est la classe d'une suite de Cauchy appartenant à $\mathcal{E}^-$.
- (6) Lorsque nous parlons de nombres réels, le symbole « 0 » signifie $\mathcal{E}_0$ ou plus précisément la classe d'un élément de $\mathcal{E}_0$ modulo $\mathcal{E}_0$.

1.297.

Avec les conventions de la définition 1.296, et en anticipant sur nos connaissances à propos des réels,

- (1) zéro est positif et négatif.
 - (2) L'intersection entre $\mathbb{R}^+$ et $\mathbb{R}^-$ est le singleton $\{0\}$.
 - (3) L'ensemble des nombres *strictement* positifs est noté $(\mathbb{R}^+)^*$ ou $\mathbb{R}^+ \setminus \{0\}$.
 - (4) Le mot « positif » signifie « positif ou nul » ; le mot « négatif » signifie « négatif ou nul ».
- Cela sont des conventions qui sont également celles de Wikipédia[54].

Définition 1.298 (Ordre sur $\mathbb{R}$).

Si $a, b \in \mathbb{R}$ nous notons $a \leq b$ si et seulement si $b - a \in \bar{\mathcal{E}}^+$.

Proposition 1.299.

Le couple $(\mathbb{R}, \leq)$ est un corps totalement ordonné¹⁰⁵

Démonstration. Il s'agit de vérifier, dans l'ordre, les définitions 1.9, 1.10 et 1.253(1). Pour la suite nous considérons $x, y, z \in \mathbb{R}$ et des suites de Cauchy a, b, c telles que $x = \bar{a}$, $y = \bar{b}$ et $z = \bar{c}$.

Réflexivité Pour savoir si $x \geq x$, nous devons nous demander si $x - x \in \bar{\mathcal{E}}^+$. Nous avons $x - x = \bar{a} - \bar{a} = \bar{0} = 0$.

antisymétrie Nous supposons que $x \geq y$ et $y \geq x$. Du côté des suites de Cauchy, cela signifie que $a - b \in \mathcal{E}^+$ et $b - a \in \mathcal{E}^+$. Le lemme 1.295(1) nous indique alors que $a - b = -(b - a) \in \mathcal{E}^-$. Donc

$$a - b \in \mathcal{E}^+ \cap \mathcal{E}^- = \{\bar{0}\}. \quad (1.458)$$

Donc le réel $x - y$ est la classe de la suite constante 0. Le lemme 1.291(2) dit alors que $x - y = 0$ ou encore que $x = y$.

transitivité Nous supposons que $x \leq y$ et $y \leq z$. Alors nous avons

$$c - a = c - b + b - a \quad (1.459a)$$

$$= (c - b) + (b - a) \quad (1.459b)$$

$$\in \mathcal{E}^+ + \mathcal{E}^+ \quad (1.459c)$$

$$\subset \mathcal{E}^+ \quad (1.459d)$$

où nous avons utilisé le lemme 1.295(2). Vu que $c - a \in \mathcal{E}^+$, nous avons $z - x = \overline{c - a} \geq 0$.

Ordre total Nous devons prouver que pour $x, y \in \mathbb{R}$ nous avons toujours $x \leq y$ ou $y \leq x$. Supposons que nous n'ayons pas $x \leq y$, c'est à dire $\overline{b - a} \notin \mathcal{E}^+$. Vu le lemme 1.292(2) nous avons $\overline{b - a} \in \mathcal{E}^-$, ce qui donne, par le lemme 1.295(1) que $\overline{a - b} \in \mathcal{E}^+$, c'est à dire $y \leq x$.

Corps ordonné Enfin nous devons vérifier les deux conditions de la définition 1.253(1).

Pour la première condition, nous supposons $x \leq y$, c'est à dire $b - a \in \mathcal{E}^+$. Nous avons donc

$$(b + c) - (a + c) = b + x - a - c = b - a \in \mathcal{E}^+, \quad (1.460)$$

105. Corps totalement ordonné, définition 1.253.

donc $\overline{a+c} \leq \overline{b+c}$, c'est à dire $x+z \leq y+z$.

Pour la seconde condition, c'est le lemme 1.295(3).

□

Définition 1.300.

Vu que $\mathbb{R}$ est un corps totalement ordonné (proposition 1.299), si $x \in \mathbb{R}$, nous définissons $|x|$ conformément à 1.253(2).

Lemme 1.301.

L'application

$$\begin{aligned} \varphi: \mathbb{Q} &\rightarrow \mathbb{R} \\ q &\mapsto \bar{q} \end{aligned} \tag{1.461}$$

dont nous avons déjà parlé dans la proposition 1.288 est strictement croissante.

Démonstration. Nous supposons $q < l$ dans $\mathbb{Q}$. Nous devons montrer que $\bar{q} \leq \bar{l}$ dans $\mathbb{R}$, c'est à dire que $\bar{q} \leq \bar{l}$ et $\bar{q} \neq \bar{l}$.

Considérons la suite constante $x_n = l - q \in \mathbb{Q}$. Pour tout $\epsilon > 0$ dans $\mathbb{Q}$ nous avons

$$x_n = l - q > 0 > -\epsilon, \tag{1.462}$$

et donc $x_n \in \mathcal{E}^+$. Donc $\overline{l-q} \geq 0$. Cela signifie $\bar{q} \leq \bar{l}$.

D'autre part le lemme 1.289 dit que $\bar{q} = \bar{l}$ que si $q = l$, ce qui est exclu parce que $q < l$. Donc $\bar{q} \neq \bar{l}$. □

Remarque 1.302.

Comme déjà mentionné plus haut, à chaque fois que nous parlerons d'un élément de $\mathbb{Q}$ comme étant un élément de $\mathbb{R}$, nous considérons la classe de la suite constante.

Lemme 1.303.

Si $x, y, z \in \mathbb{R}$ avec $x > 0$ sont tels que $z > y/x$ alors $zx > y$.

Démonstration. Nous savons que

$$z - \frac{y}{x} \in \mathcal{E}^+ \setminus \{0\} = \mathcal{E}^{++}. \tag{1.463}$$

Vu que $x \in \mathcal{E}^{++}$, multiplier par x fait rester dans $\mathcal{E}^{++}$:

$$zx - x \frac{y}{x} \in \mathcal{E}^{++}. \tag{1.464}$$

Un représentant de $x \frac{y}{x}$ est la suite $n \mapsto x_n \frac{y_n}{x_n} = y_n$. Donc $x \frac{y}{x} = y$. Cela signifie que $zx - y \in \mathcal{E}^{++}$ et donc que $zx > y$. □

Lemme 1.304.

Pour tout $a \in \mathbb{R}$, il existe $p \in \mathbb{N}$ tel que $p > a$.

Démonstration. Nous allons donner deux preuves différentes de ce lemme.

Première façon L'élément a de $\mathbb{R}$ admet un représentant (a_n) qui est une suite de Cauchy dans $\mathbb{Q}$. C'est donc une suite bornée, c'est-à-dire qu'il existe $m, q \in \mathbb{N}$ tels que $|a_n| \leq m/q$ pour tout n (proposition 1.276(2)). Soit M un naturel strictement plus grand que m/q ¹⁰⁶.

La suite de Cauchy $(M - a_n)_{n \in \mathbb{N}}$ est constituée de rationnels positifs et est donc dans $\mathcal{E}^+$.

La classe de $M - a$ est donc un réel positif¹⁰⁷. Par définition de la relation d'ordre, $M \geq a$.

¹⁰⁶. Lemme 1.267.

¹⁰⁷. Et nous allons d'ailleurs arrêter de toujours préciser « la classe de » lorsque ce n'est pas nécessaire.

Seconde façon La suite (a_n) est majorée par $\frac{m}{q}$, donc on a dans $\mathbb{Q}$ et pour tout n :

$$a_n \leq \frac{m}{q} = M \leq qM. \quad (1.465)$$

L'application $\varphi: \mathbb{Q} \rightarrow \mathbb{R}$ est croissante, donc

$$\varphi((a_n)) \leq \varphi(qM). \quad (1.466)$$

□

En corolaire, nous avons

Lemme 1.305.

Pour tout $x \in \mathbb{R}$, il existe $q \in \mathbb{Z}$ tel que $q < x$.

Démonstration. Utilisation du lemme précédent avec $a = -x$: on prend $q = -p$. □

Théorème 1.306 ([12]).

Le corps $\mathbb{R}$ est archimédien¹⁰⁸.

Démonstration. La proposition 1.299 dit que $\mathbb{R}$ est totalement ordonné. Soient $x, y \in \mathbb{R}$ avec $x > 0$; posons $a = \frac{y}{x}$. Le lemme 1.304 nous donne un $p \in \mathbb{N}$ tel que $p > a$. Nous concluons alors avec le lemme 1.303 :

$$px > ax = \frac{y}{x}x = y. \quad (1.467)$$

□

Le lemme suivant n'est pas loin de dire que $\mathbb{Q}$ est dense dans $\mathbb{R}$, à part que nous n'avons pas encore donné de topologie sur $\mathbb{R}$.

Lemme 1.307.

Si $x, y \in \mathbb{R}$ sont tels que $x < y$, alors il existe $s \in \mathbb{Q}$ tel que $x < s < y$.

Démonstration. Nous avons par hypothèse que $y - x > 0$ et donc le fait que $\mathbb{R}$ soit archimédien (théorème 1.306) nous donne $q \in \mathbb{N}$ tel que $q(y - x) > 1$. Soit

$$E = \{n \in \mathbb{Z} \text{ tel que } \frac{n}{q} \leq x\}. \quad (1.468)$$

Cet ensemble n'est pas vide à cause du lemme 1.305 ; de plus, comme $|x|q \leq n_0$ pour un certain n_0 (à cause du lemme 1.304), l'ensemble E est majoré par n_0 . Donc E possède un plus grand élément¹⁰⁹ p qui vérifie

$$\frac{p}{q} \leq x < \frac{p+1}{q}. \quad (1.469)$$

De plus $(p+1)/q < y$. En effet nous avons

$$\frac{p+1}{q} = \frac{p}{q} + \frac{1}{q} \leq x + \frac{1}{q} < x + y - x = y \quad (1.470)$$

où nous avons utilisé l'inégalité stricte $y - x > \frac{1}{q}$.

Nous avons donc

$$x < \frac{p+1}{q} < y, \quad (1.471)$$

et le nombre $(p+1)/q$ convient comme s . □

¹⁰⁸. Définition 1.58.

¹⁰⁹. Lemme 1.90.

Remarque 1.308.

Le lemme 1.307 a également pour conséquence que des ensembles comme $[-1, 1]$ ne sont pas bien ordonnés (définition 1.10). En effet la partie $]0, 1[$ ne possède pas de minimum parce que si $x \in]0, 1[$ alors $0 < x$ et il existe $s \in \mathbb{Q}$ (a fortiori $s \in \mathbb{R}$) tel que $0 < s < x$, c'est-à-dire que x n'est pas un minimum de $]0, 1[$.

Tant que nous y sommes dans les encadrements de réels...

1.309.

Soit $q_0 \in \mathbb{Q}$ tel que $0 \leq q_0 < 1$. On définit alors $d_1 \in \{0, 1\}$ comme valant 1 si $2q_0 \geq 1$ et 0 sinon. Puis on pose $q_1 = 2q_0 - d_1$.

Poursuivant de la sorte, on crée une suite $(d_n)_{n \geq 1}$: c'est le **développement dyadique** de q_0 .

Lemme 1.310 ([1]).

Soit q, q' deux rationnels tels que $0 \leq q < q' < 1$. Il existe deux entiers naturels a et N tels que $q < \frac{a}{2^N} < q'$.

Démonstration. On crée les développements dyadiques de q et q' , que l'on note respectivement $(d_n)_{n \geq 1}$ et $(d'_n)_{n \geq 1}$. Notons

$$E = \{n \in \mathbb{N} \text{ tel que } d_n \neq d'_n\}. \quad (1.472)$$

Comme $q \neq q'$, les développements dyadiques sont différents¹¹⁰, l'ensemble E est non-vide, et il admet un plus petit élément N . Or, $q < q'$, et donc nécessairement $d_N < d'_N$. On construit alors $a = \sum_{i=1}^N d_i 2^i$. $\square$

Corolaire 1.311.

Pour tous réels x, y tels que $0 \leq x < y \leq 1$, il existe un nombre de la forme $d = a/2^n$, avec $n \in \mathbb{N}$ et $a \in \mathbb{N}$, $a \leq 2^n$, tel que $x < d < y$.

Lemme 1.312 ([1]).

Soient des réels a, b, x, y tels que

$$a \leq x \leq b \quad (1.473)$$

et

$$a \leq y \leq b, \quad (1.474)$$

alors $|x - y| \leq |b - a|$.

Lemme 1.313.

Soient deux réels a, b tels que

$$(1) \ a \geq 0,$$

$$(2) \ b \geq 0$$

$$(3) \ a + b = 0.$$

Alors $a = 0$ et $b = 0$.

Lemme 1.314.

Si $a \in \mathbb{R}$, alors $a^2 \geq 0$ et $a^2 = 0$ si et seulement si $a = 0$.

1.18.3 Complétude

Le théorème 17.127 donne une complétion de tout espace métrique en un espace complet. Il serait tentant de l'utiliser ici pour définir $\mathbb{R}$ à partir de $\mathbb{Q}$. Cette méthode ne fonctionne cependant pas parce que la démonstration de 17.127 utilise le fait que $\mathbb{R}$ est complet.

110. À vérifier tout de même...

Lemme 1.315.

Nous avons

$$|\varphi(q)| = |\varphi(q)| \quad (1.475)$$

pour tout $q \in \mathbb{Q}$.

Démonstration. Soit $q \in \mathbb{Q}$. Si $q \geq 0$ alors nous avons d'une part $|q| = q$ dans $\mathbb{Q}$, et d'autre part $\varphi(q) \geq 0$ dans $\mathbb{R}$. Donc au final

$$|\varphi(q)| = \varphi(q) = \varphi(|q|). \quad (1.476)$$

Supposons au contraire que $q < 0$. Alors $|q| = -q$ dans $\mathbb{Q}$, mais aussi $\varphi(q) \leq 0$. Donc

$$|\varphi(q)| = -\varphi(q) = \varphi(-q) = \varphi(|q|). \quad (1.477)$$

□

Lemme 1.316 ([12, 1]).

Toute suite de Cauchy dans $\mathbb{Q}$ converge dans $\mathbb{R}$ vers le réel qu'elle représente.

Plus précisément, en suivant les notations de 1.287, si (x_k) est une suite de Cauchy dans $\mathbb{Q}$, alors

(1) $\varphi(x_k)$ est une suite de Cauchy dans $\mathbb{R}$.

(2) $\varphi(x_k) \xrightarrow{\mathbb{R}} \bar{x}$.

Ici $\bar{x}$ est la classe de la suite x . C'est donc un élément de $\mathbb{R}$.

Démonstration. Soit (x_n) une suite de Cauchy de $\mathbb{Q}$, c'est-à-dire que $x_k \in \mathbb{Q}$ pour tout k et qu'elle est de Cauchy. Elle représente un réel $\bar{x} \in \mathbb{R}$, et nous voulons prouver que pour la topologie de $\mathbb{R}$ nous avons $\lim_{n \rightarrow \infty} \varphi(x_n) = \bar{x}$.

$\varphi(x_k)$ est de Cauchy Soit $\epsilon > 0$ dans $\mathbb{R}$. Nous considérons $\epsilon' \in \mathbb{Q}$ tel que $0 < \epsilon' < \epsilon$. Plus précisément tel que

$$0 < \varphi(\epsilon') < \epsilon. \quad (1.478)$$

Soit $N > 0$ tel que $|x_p - x_q| < \epsilon'$ pour tout $p, q \geq N$. Cela existe parce que (x_k) est dans Cauchy dans $\mathbb{Q}$. Nous avons alors

$$|\varphi(x_p) - \varphi(x_q)| = |\varphi(x_p - x_q)| \quad (1.479a)$$

$$= \varphi(|x_p - x_q|) \quad (1.479b)$$

$$\leq \varphi(\epsilon') \quad (1.479c)$$

$$\leq \epsilon. \quad (1.479d)$$

Justifications :

— Pour (1.479b). C'est le lemme 1.315.

— Pour (1.479c). L'application φ est croissante, lemme 1.301.

Donc la suite $\varphi(x_k)$ est de Cauchy.

$\varphi(x_k) \xrightarrow{\mathbb{R}} \bar{x}$ Nous devons prouver que pour tout $\epsilon \in \mathbb{R}$, il existe N tel que $n > N$ implique $\varphi(x_n) \in B(\bar{x}, \epsilon)$. Nous allons faire ça en deux parties. D'abord $\epsilon \in \mathbb{Q}$ et ensuite $\epsilon \in \mathbb{R}$.

Avec $\epsilon \in \mathbb{Q}$ Soit $\epsilon \in \mathbb{Q}$. Vu que x est une suite de Cauchy dans $\mathbb{Q}$, il existe N tel que si $p, n > N$ nous avons

$$x_p - \epsilon < x_n < x_p + \epsilon. \quad (1.480)$$

Ces inégalités sont dans $\mathbb{Q}$. Nous fixons p et nous commençons par écrire plus en détail la première inéquation :

$$x_p - \epsilon - x_n < 0. \quad (1.481)$$

Autrement dit, pour tout n nous avons

$$(\overline{x_p - \epsilon})_n < x_n. \quad (1.482)$$

Pour rappel, la suite $\overline{x_p - \epsilon}$ est la suite constante dans $\mathbb{Q}$. La suite

$$n \mapsto x_n - (\overline{x_p - \epsilon})_n \quad (1.483)$$

est dans $\mathcal{E}^+$. Donc, en vertu de la définition 1.298 nous avons

$$\bar{x} - \overline{x_p - \epsilon} \geq 0. \quad (1.484)$$

Nous pouvons aussi bien écrire

$$\bar{x} \geq \varphi(x_p) - \varphi(\epsilon). \quad (1.485)$$

En prenant l'autre inégalité de (1.480) nous trouvons de la même manière que

$$\bar{x} \leq \varphi(x_p) + \varphi(\epsilon). \quad (1.486)$$

Ces deux inégalités ensemble montrent que

$$\varphi(x_p) \in B(\bar{x}, \varphi(\epsilon)). \quad (1.487)$$

Avec $\epsilon \in \mathbb{R}$ Nous considérons $\epsilon \in \mathbb{R}$ et $\epsilon' \in \mathbb{Q}$ tel que $\varphi(\epsilon') < \epsilon$. Par le point précédent, il existe N tel que $p > N$ implique

$$\varphi(x_p) \in B(\bar{x}, \varphi(\epsilon')). \quad (1.488)$$

Étant donné que $\varphi(\epsilon') < \epsilon$ nous avons

$$\varphi(x_p) \in B(\bar{x}, \varphi(\epsilon')) \subset B(\bar{x}, \epsilon). \quad (1.489)$$

□

Proposition 1.317.

Soit une suite convergente $x_k \xrightarrow{\mathbb{Q}} q$. Alors

$$\varphi(x_k) \xrightarrow{\mathbb{R}} \varphi(q) \quad (1.490)$$

où φ est la fonction qui à un rationnel fait correspondre la classe de la suite constante correspondante ¹¹¹.

Démonstration. Le fait d'avoir une convergence $x_k \rightarrow q$ dans $\mathbb{Q}$ implique que la suite (x_k) est de Cauchy, par la proposition 1.276(1).

Le lemme 1.316 nous indique que $\varphi(x_k)$ est une suite dans $\mathbb{R}$ qui converge vers $\bar{q}$, la classe de la suite (x_k) .

À prouver : $\varphi(x) = \bar{q}$. Autrement dit, nous devons prouver que la classe de la suite constante $a_k = q$ et la classe de la suite x sont les mêmes.

La suite $(x_k - q)$ est de Cauchy dans $\mathbb{Q}$ et converge vers zéro par hypothèse. Donc les suites x et (q) sont dans la même classe. □

Proposition 1.318 ([1]).

Deux choses à propos de suites de rationnels convergeant vers un réel.

- (1) Soit un réel x . Il existe une suite de rationnels strictement croissante qui converge vers x .
- (2) Si de plus $x > 0$, alors la suite (toujours strictement croissante) peut être choisie parmi les rationnels strictement positifs.

Démonstration. Le lemme 1.307 nous sera d'une grande aide. Soit $x \in \mathbb{R}$. Il existe $q_0 \in \mathbb{Q}$ tel que $x - 1 < q_0 < x$. Ensuite nous construisons la suite par récurrence : q_k est choisi tel que $q_{k-1} < q_k < x$. Cela règle le point (1).

Pour (2). Il suffit de faire la même chose, en partant de $0 < q_0 < x$. □

¹¹¹. Voir les notations en 1.287.

Théorème 1.319 (Complétude de $\mathbb{R}$, critère de Cauchy[12]).

Nous avons :

- (1) Le corps $\mathbb{R}$ est un corps complet (définition 1.253(5))
- (2) Une suite dans $\mathbb{R}$ est convergente (définition 1.253(4)) si et seulement si elle est de Cauchy (définition 1.253(3)).

Notez la grande similitude entre ce théorème et le théorème 7.198. Ils ne sont pas équivalents, ne parlent pas exactement du même objet « $\mathbb{R}$ », ni des mêmes notions de suites de Cauchy et de complétude.

Démonstration. Soit (x_n) une suite de Cauchy dans $\mathbb{R}$. Pour chaque n , il existe par le lemme 1.307 un $y_n \in \mathbb{Q}$ tel que

$$x_n - \frac{1}{n} < y_n < x_n + \frac{1}{n}. \quad (1.491)$$

(y_n) est une suite de Cauchy dans $\mathbb{Q}$ Nous prouvons que (y_n) est une suite de Cauchy dans $\mathbb{Q}$ (définition 1.253(3)). Vu que (x_n) est de Cauchy pour le corps $\mathbb{R}$, si $\epsilon > 0$ dans $\mathbb{R}$ est donné, il existe n_ϵ tel que si $p, q \geq n_\epsilon$, alors $|x_p - x_q| < \epsilon$.

Nous avons :

$$|y_p - y_q| \leq |y_p - x_p| + |x_p - x_q| + |x_q - y_q| < \frac{1}{p} + \epsilon + \frac{1}{q}. \quad (1.492)$$

En choisissant $N_\epsilon > \max\{n_\epsilon, \frac{1}{\epsilon}\}$ (ce qui est possible par le lemme 1.304), et en prenant $p, q > N_\epsilon$, nous avons

$$|y_p - y_q| \leq 3\epsilon, \quad (1.493)$$

ce qui prouve que (y_p) est une suite de Cauchy dans $\mathbb{Q}$, pour la notion de suite de Cauchy dans $\mathbb{Q}$.

Le réel représenté Vu que (y_p) est de Cauchy dans $\mathbb{Q}$, elle représente un réel que nous notons $\bar{y}$.

Convergence de (x_n) Nous prouvons que $x_n \xrightarrow{\mathbb{R}} \bar{y}$.

Nous savons qu'une suite de Cauchy de rationnels converge dans $\mathbb{R}$ vers le réel qu'elle représente, c'est-à-dire : $y_n \xrightarrow{\mathbb{R}} \bar{y}$ où chaque $y_n \in \mathbb{Q}$ est vu comme la suite constante (cela est le lemme 1.316). Autrement dit, pour $\epsilon > 0$, il existe un $N_\epsilon \in \mathbb{N}$ tel que si $p > N_\epsilon$ alors $|\bar{y} - y_p| < \epsilon$. Pour un tel p nous avons

$$|\bar{y} - x_p| \leq |\bar{y} - y_p| + |y_p - x_p| \leq \epsilon + \frac{1}{p}. \quad (1.494)$$

Donc dès que p est plus grand que $\max\{N_\epsilon, \frac{1}{\epsilon}\}$, nous avons $|\bar{y} - x_p| < 2\epsilon$, ce qui signifie que la suite (x_n) converge vers $\bar{y}$ dans $\mathbb{R}$.

Ceci achève de prouver que $\mathbb{R}$ est un corps complet.

En ce qui concerne l'équivalence entre les suites convergentes et de Cauchy, nous venons de prouver que toute suite de Cauchy dans $\mathbb{R}$ est convergente. La réciproque est la proposition 1.275. $\square$

Nous avons terminé avec la construction des réels. Les propriétés topologiques arrivent en la section 10.3. En particulier le théorème 7.198 pour la complétude de $\mathbb{R}$ en tant qu'espace métrique.

1.18.4 Intervalles

Nous avons déjà défini la notion d'intervalle pour un espace totalement ordonné en 1.15. Nous posons quelques notations dans $\mathbb{R}$.

Définition 1.320.

Soient $a \neq b$ dans $\mathbb{R}$. Nous définissons les parties suivantes de $\mathbb{R}$:

- (1) $]a, b[= \{x \in \mathbb{R} \text{ tel que } a < x < b\}$
- (2) $[a, b[= \{x \in \mathbb{R} \text{ tel que } a \leq x < b\}$
- (3) $]a, b] = \{x \in \mathbb{R} \text{ tel que } a < x \leq b\}$
- (4) $[a, b] = \{x \in \mathbb{R} \text{ tel que } a \leq x \leq b\}$
- (5) $] -\infty, a] = \{x \in \mathbb{R} \text{ tel que } x \leq a\}$
- (6) $] -\infty, a[= \{x \in \mathbb{R} \text{ tel que } x < a\}$
- (7) $]a, \infty[= \{x \in \mathbb{R} \text{ tel que } x > a\}$
- (8) $[a, \infty[= \{x \in \mathbb{R} \text{ tel que } x \geq a\}$.
- (9) $] -\infty, \infty[= \mathbb{R}$.

La proposition 1.325 nous dira que tous les intervalles de $\mathbb{R}$ sont d'une de ces formes.

1.18.5 Maximum, supremum et compagnie

Ce n'est un secret pour personne que $\mathbb{R}$ est un ensemble totalement ordonné¹¹² : il y a des éléments plus grands que d'autres, et mieux : à chaque fois que je prends deux éléments différents dans $\mathbb{R}$, il y en a un des deux qui est plus grand que l'autre. Il n'y a pas d'*ex æquo* dans $\mathbb{R}$.

Définition 1.321.

Soit A , une partie de $\mathbb{R}$.

- (1) Un nombre M est un **majorant** de A si M est plus grand que tous les éléments de A : pour tout $x \in A$, $M \geq x$.
- (2) Un nombre m est un **minorant** de A si m est plus petit que tous les éléments de A : pour tout $x \in A$, $m \leq x$.

Nous parlons de majorant ou de minorants stricts lorsque les inégalités sont strictes.

Nous insistons sur le fait que l'inégalité n'est pas stricte. Ainsi, 1 est un majorant de $[0, 1]$. Dès qu'un ensemble a un majorant, il en a plein. Si s majore l'ensemble A , alors $s + 1$, $s + 4$, et $s + \frac{3}{7}$ majorent également A .

Exemple 1.322.

Une petite galerie d'exemples de majorants.

- L'intervalle fermé $[4, 8]$ admet entre autres 8 et 130 comme majorants,
- l'intervalle ouvert $]4, 8[$ admet également 8 et 130 comme majorants,
- 7 n'est pas un majorant de $[1, 5] \cup]8, 32]$,
- 10/10 majore les notes qu'on peut obtenir à un devoir.
- l'intervalle $[4, \infty[$ n'a pas de majorants.

△

Proposition-Définition 1.323 (Least-upper-bound property[55]).

Soit A une partie majorée de $\mathbb{R}$. Il existe un unique élément $M \in \mathbb{R}$ tel que

- (1) $M \geq x$ pour tout $x \in A$,
- (2) pour tout ε , le nombre $M - \varepsilon$ n'est pas un majorant de A , c'est-à-dire qu'il existe un élément $x \in A$ tel que $x > M - \varepsilon$.

Cet élément est nommé **supremum** de A et est noté $\sup(A)$. De la même façon, **l'infimum** de A , noté $\inf A$, est le plus grand de ses minorants.

Par convention, si la partie n'est pas bornée vers le haut, nous dirons que son supremum n'existe pas, ou bien qu'il est égal à $+\infty$, suivant les contextes. Pour votre culture générale, sachez toutefois que $\infty \notin \mathbb{R}$.

112. Proposition 1.299.

Démonstration. Nous faisons la preuve pour l'infimum.

Unicité En ce qui concerne l'unicité, soient m_1 et m_2 , deux infimums de A . Supposons $m_1 > m_2$. Alors il existe $\epsilon > 0$ tel que $m_2 < m_2 + \epsilon < m_1$ (c'est le lemme 1.307). Cela prouve que $m_2 + \epsilon$ est un minorant de A et donc que m_2 n'est pas un infimum.

Existence Soit A , une partie de $\mathbb{R}$. Nous allons trouver son infimum en suivant une méthode de dichotomie. Pour cela nous allons construire trois suites en même temps de la façon suivante. D'abord nous choisissons un point x_0 de A et un point x_1 qui minore A (qui existe par hypothèse) :

$$\begin{aligned} x_0 &\text{ est un élément de } A, \\ x_1 &\text{ est un minorant de } A, \\ a_0 &= x_0 \\ b_0 &= x_1 \\ b_1 &= x_1. \end{aligned} \tag{1.495}$$

Ensuite, nous faisons la récurrence suivante :

$$\begin{aligned} x_{n+1} &= \frac{a_n + b_n}{2}, \\ a_{n+1} &= \begin{cases} a_n & \text{si } x_{n+1} \text{ minore } A \\ x_{n+1} & \text{sinon,} \end{cases} \\ b_{n+1} &= \begin{cases} x_{n+1} & \text{si } x_{n+1} \text{ minore } A \\ b_n & \text{sinon.} \end{cases} \end{aligned} \tag{1.496}$$

Nous allons montrer que (a_n) et (b_n) sont des suites convergentes de même limite et que cette limite est l'infimum de A .

Soit $n \in \mathbb{N}$; il y a deux possibilités. Soit $a_n = a_{n-1}$ et $b_n = x_n$, soit $a_n = x_n$ et $b_n = b_{n-1}$. Supposons que nous soyons dans le premier cas (le second se traite de façon similaire). Alors nous avons

$$\begin{aligned} |a_n - b_n| &= |a_{n-1} - x_n| \\ &= \left| a_{n-1} - \frac{a_{n-1} + b_{n-1}}{2} \right| \\ &= \frac{1}{2} |a_{n-1} - b_{n-1}|, \end{aligned} \tag{1.497}$$

ce qui prouve que $|a_n - b_n| \rightarrow 0$. Nous montrons maintenant que la suite (a_n) est de Cauchy. En effet nous avons

$$|a_n - a_{n-1}| = \begin{cases} 0 \\ \left| \frac{a_n - b_n}{2} \right| \end{cases} \leq \frac{1}{2n}. \tag{1.498}$$

Il en est de même pour la suite (b_n) . Ce sont deux suites de Cauchy (donc convergentes par la proposition 1.275) qui convergent vers la même limite. Soit ℓ cette limite.

Le nombre ℓ minore A . En effet si $a \in A$ est plus petit que ℓ , les éléments b_n tels que $|b_n - \ell| < |a - \ell|$ ne peuvent pas minorer A . D'autre part, pour tout ϵ , le nombre $\ell + \epsilon$ ne peut pas minorer A . En effet, ℓ est la limite de la suite décroissante (a_n) , donc il existe a_n entre ℓ et $\ell + \epsilon$. Mais a_n ne minore pas A , donc $\ell + \epsilon$ ne minore pas non plus A .

Nous avons prouvé que toute partie minorée de $\mathbb{R}$ possède un infimum.

La preuve que toute partie majorée possède un supremum se fait de la même façon. □

Lemme 1.324.

Soit une partie A de $\mathbb{R}$. Si M est un majorant de A , alors $M \geq \sup(A)$.

Démonstration. Si $M < \sup(A)$, alors en posant $\epsilon = \sup(A) - M$, le nombre $\sup(A) - \epsilon$ est encore un majorant de A , ce qui est impossible par définition d'un supremum. □

1.18.5.1 Intervalles

Proposition 1.325.

Tous les intervalles de $\mathbb{R}$ sont d'une des formes listées dans la définition 1.320.

1.18.5.2 Quelques exemples

En matière de notations, le maximum de l'ensemble A est noté $\max A$, le supremum est noté $\sup A$. Le minimum et l'infimum sont notés $\min A$ et $\inf A$.

Exemple 1.326.

Exemples de différence entre majorant, supremum et maximum.

- Le nombre 10 est un supremum, majorant et maximum de l'intervalle fermé $[0, 10]$,
- Le nombre 10 est un majorant et un supremum, mais pas un maximum de l'intervalle ouvert $]0, 10[$,
- Le nombre 136 est un majorant, mais ni un maximum ni un supremum de l'intervalle $[0, 10]$.

△

En utilisant les notations concises, ces différents cas s'écrivent ainsi :

$$10 = \max[0, 10] = \sup[0, 10] \quad 10 = \sup[0, 10[\quad (1.499)$$

Exemple 1.327.

Si on dit que un pont s'effondre à partir d'une charge de 10 tonnes, alors 10 tonnes est un *supremum* des charges que le pont peut supporter : si on met 9,999999 tonnes dessus, il tient encore le coup, mais si on ajoute un gramme, alors il s'effondre (on sort de l'ensemble des charges acceptables). △

Exemple 1.328.

Si on dit qu'un pont résiste jusqu'à 10 tonnes, alors 10 tonnes est un *maximum* de la charge acceptable. Sur ce pont-ci, on peut ajouter le dernier gramme. Mais à partir de là, le moindre truc qu'on ajoute, il s'effondre. △

Lemme 1.329.

À propos de bornes d'un intervalle.

- (1) La borne inférieure d'un intervalle est son *infimum*,
- (2) la borne supérieure est le *supremum*.
- (3) Si de plus l'intervalle est fermé, l'infimum est un *minimum* et le supremum est un *maximum*.

Exemple 1.330.

Quelques exemples dans les intervalles.

- (1) $A = [1, 2]$. Tous les nombres plus petits ou égaux à 1 sont minorants, 1 est infimum et minimum. Le nombre 2 est un majorant, le maximum et le supremum.
- (2) $B =]3, \pi[$. Le nombre π est le supremum et est un majorant, mais n'est pas le maximum (parce que $\pi \notin B$). L'ensemble B n'a pas de maximum. Bien entendu, -1000 est un minorant.

Dans les deux cas, le nombre 53 est un majorant. △

Il existe évidemment de nombreux exemples plus vicieux.

Exemple 1.331.

Prenons $E = \{\frac{1}{n} \text{ tel que } n \in \mathbb{N}_0\}$, dont les premiers points sont indiqués sur la figure 1.1. Cet ensemble est constitué des nombres $1, \frac{1}{2}, \frac{1}{3}, \dots$. Le plus grand d'entre eux est 1 parce que tous les nombres de la forme $\frac{1}{n}$ avec $n \geq 1$ sont plus petits ou égaux à 1. Le nombre 1 est donc maximum de E .

L'ensemble E n'a par contre pas de minimum parce que tout élément de E s'écrit $\frac{1}{n}$ pour un certain n et est plus grand que $\frac{1}{n+1}$ qui est également dans E .

Prouvons que zéro est l'infimum de E . D'abord, tous les éléments de E sont strictement positifs, donc zéro est certainement un minorant de E . Ensuite, nous savons que pour tout $\varepsilon > 0$, il existe un n tel que $\frac{1}{n}$ est plus petit que ε . L'ensemble E possède donc un élément plus petit que $0 + \varepsilon$, et zéro est bien l'infimum. $\triangle$

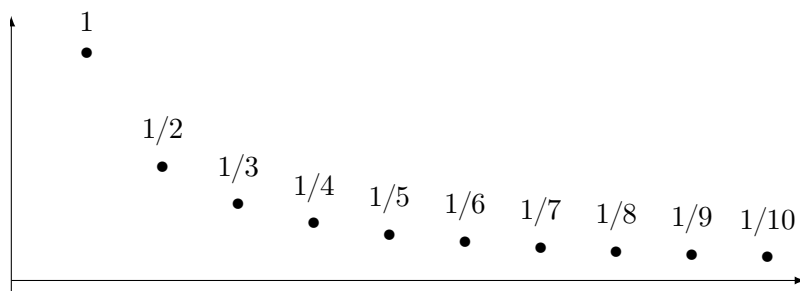


FIGURE 1.1 – Les premiers points du type $x_n = 1/n$.

L'exemple suivant est une source classique d'erreurs en ce qui concerne l'infimum. Il sera à relire après avoir vu la définition de limite (définition 10.22).

Exemple 1.332.

Les premiers points de l'ensemble $F = \{\frac{(-1)^n}{n} \text{ tel que } n \in \mathbb{N}_0\}$ sont représentés à la figure 1.2. Bien que (comme nous le verrons plus tard) la limite de la suite $x_n = (-1)^n/n$ soit zéro, il n'est pas correct de dire que zéro est l'infimum de l'ensemble F . Le dessin, au contraire, montre bien que -1 est le minimum (aucun point est plus bas que -1), tandis que le maximum est $1/2$.

Nous reviendrons avec cet exemple dans la suite. Pour l'instant, ayez bien en tête que zéro n'est rien de spécial pour l'ensemble F en ce qui concerne les notions de maximum, minimum et compagnie. $\triangle$

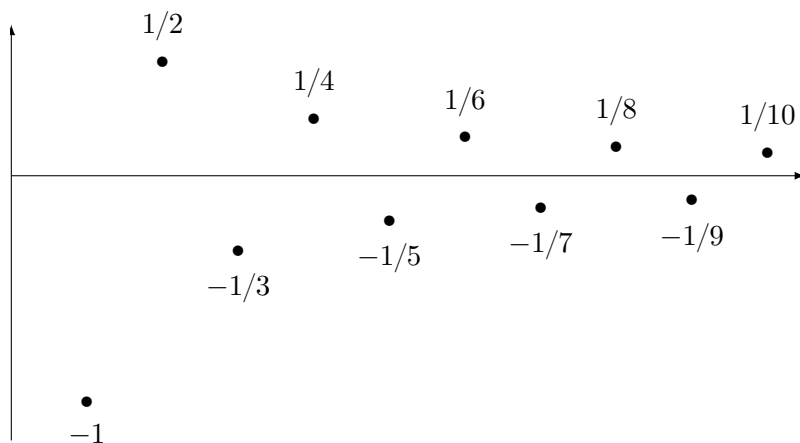


FIGURE 1.2 – Les quelques premiers points du type $(-1)^n/n$.

1.18.6 Racines

Dans cette section, nous définissons $\sqrt[n]{x}$ pour $x \in \mathbb{Q}^+$. Vous notez que c'est fait de façon assez algébrique¹¹³, ou en tout cas, en restant proche des définitions. Des définitions plus technologiques utilisant la continuité de $x \mapsto x^n$ et qui prouvent que c'est bijectif sur un domaine choisi avec prudence existent, et c'est fait dans la définition 12.344. Il est même expliqué dans [50] que la méthode décrite ici permet de définir $\sqrt[n]{x}$ pour tout n entier, et pas seulement pour $n = 2$.

113. Discutable parce que des limites sont utilisées.

Proposition 1.333.

Soit $q \in \mathbb{Q}^+$. Il existe un unique $r \in \mathbb{R}$ tel que $r^2 = q$.

Plus précisément, en termes des notations de 1.287, pour tout $q \in \mathbb{Q}^+$, il existe un unique $r \in \mathbb{R}^2$ tel que $r^2 = \varphi(q)$.

Démonstration. En deux parties : d'abord l'existence et ensuite l'unicité.

Existence Si $q = 0$, c'est $r = 0$. Nous supposons $q > 0$. La suite (x_k) de la proposition 1.282 a la propriété d'être de Cauchy dans $\mathbb{Q}$. Donc il existe un réel r qui est la classe de cette suite. Nous posons donc

$$r = \bar{x}. \quad (1.500)$$

En ce qui concerne r^2 , nous avons, par définition du produit dans $\mathbb{R}$,

$$r^2 = \bar{x}^2 = \overline{(x_k^2)}, \quad (1.501)$$

c'est la classe de la suite de Cauchy donnée par les x_k^2 . Posons $y_k = x_k^2$; la relation (1.501) s'écrit

$$r^2 = \bar{y}. \quad (1.502)$$

La proposition 1.282 nous dit également que y est une suite de Cauchy et que

$$y_k \xrightarrow{\mathbb{Q}} q \quad (1.503)$$

La proposition 1.317 donne alors $\bar{y} = \bar{q}$, et finalement

$$r^2 = \bar{q} = \varphi(q). \quad (1.504)$$

Ici tout n'est pas encore terminé avec l'existence parce qu'il faut nous assurer que $r \geq 0$. Ce n'est pas très compliqué : si $r < 0$, alors nous pouvons faire le choix $-r$ qui convient tout aussi bien : $(-r)^2 = r^2$.

Unicité Supposons $r_1, r_2 \in \mathbb{R}$ tels que $r_1^2 = r_2^2$. La proposition 1.299 dit que $\mathbb{R}$ est totalement ordonné; disons pour fixer les idées que $r_1 \leq r_2$. Cela signifie, par définition de l'ordre sur $\mathbb{R}$, que $r_2 - r_1 \geq 0$. En posant $s = r_2 - r_1$ nous avons $r_2 = r_1 + s$. Passons au carré; la distribution dans le calcul suivant provient du fait que $\mathbb{R}$ est un corps :

$$r_2^2 = (r_1 + s)^2 = r_1^2 + 2r_1s + s^2. \quad (1.505)$$

Vu que $r_1^2 = q = r_2^2$, nous avons $2r_1s + s^2 = 0$ ou encore

$$s(2r_1 + s) = 0. \quad (1.506)$$

Vu que $\mathbb{R}$ est un corps, il est un anneau intègre¹¹⁴ et la règle du produit nul s'applique : soit $s = 0$, soit $2r_1 + s = 0$. Vu que $r_2 > 0$ et que $s \geq 0$, nous avons $2r_1 + s > 0$ et donc $s = 0$.

Nous en déduisons que $r_1 = r_2$.

□

1.18.7 Corps valué

Définition 1.334 (Valeur absolue, corps valué[56, 57]).

Soit un corps $\mathbb{K}$. Une **valeur absolue** sur $\mathbb{K}$ est une application $|\cdot|: \mathbb{K} \rightarrow \mathbb{R}^+$ telle que

- (1) $|x| = 0$ si et seulement si $x = 0$,
- (2) $|x + y| \leq |x| + |y|$
- (3) $|xy| \leq |x||y|$.

Un corps muni d'une valeur absolue est un **corps valué**.

114. Lemme 1.194.

1.18.8 Partie entière, partie fractionnaire

Lemme-Définition 1.335 ([58]).

Pour tout réel x , il existe un unique entier n vérifiant

$$n \leq x < n + 1. \quad (1.507)$$

Dans ce cas nous avons $x - n \in [0, 1[$.

Ce n est la **partie entière** de x , et il sera noté $\text{int}(x)$. Le nombre $x - \text{int}(x)$ est la **partie fractionnaire** de x que nous notons $\text{frac}(x)$.

Il est toutefois à noter que la partie fractionnaire de x n'est pas garantie d'être une fraction ; cette dénomination est donc un peu trompeuse.

1.19 Les complexes

Définition 1.336 (Nombres complexes[59]).

L'ensemble des **nombres complexes** $\mathbb{C}$ est l'ensemble $\mathbb{R}^2$ muni des opérations suivantes :

(1)

$$\begin{aligned} \times_{\mathbb{C}} : \mathbb{C} \times \mathbb{C} &\rightarrow \mathbb{C} \\ ((x, y), (x', y')) &\mapsto (xx' - yy', xy' + yx') \end{aligned} \quad (1.508)$$

(2)

$$\begin{aligned} +_{\mathbb{C}} : \mathbb{C} \times \mathbb{C} &\rightarrow \mathbb{C} \\ ((x, y), (x', y')) &\mapsto (x + x', y + y') \end{aligned} \quad (1.509)$$

(3)

$$\begin{aligned} \cdot : \mathbb{R} \times \mathbb{C} &\rightarrow \mathbb{C} \\ (\lambda, (x, y)) &\mapsto (\lambda x, \lambda y). \end{aligned} \quad (1.510)$$

Lemme 1.337.

Le triple $(\mathbb{C}, +_{\mathbb{C}}, \times_{\mathbb{C}})$ est un anneau¹¹⁵ commutatif dont le neutre pour l'addition est $(0, 0)$ et le neutre pour la multiplication est $(1, 0)$.

Démonstration. Ce ne sont que des calculs. Juste pour vous montrer, voici la première partie pour l'associativité :

$$((a, b)(x, y))(s, t) = (ax - by, ay + bx)(s, t) \quad (1.511a)$$

$$= (axs - bys - ayt - bxt, axt - byt + ays + bxs). \quad (1.511b)$$

Nous avons utilisé la distributivité sur $\mathbb{R}$, provenant du fait que $\mathbb{R}$ est un corps par le théorème 1.286. $\square$

Lemme 1.338.

L'anneau $\mathbb{C}$ est un corps.

Démonstration. Il suffit de trouver un inverse pour chaque élément non nul. Soit un élément non nul $(a, b) \in \mathbb{C}$. En combinant les lemmes 1.313 et 1.314 nous savons que $a^2 + b^2 > 0$. En particulier, cet élément est inversible dans $\mathbb{R}$, et nous pouvons considérer l'élément suivant de $\mathbb{C}$:

$$z = \left(\frac{a}{a^2 + b^2}, -\frac{b}{a^2 + b^2} \right). \quad (1.512)$$

Prouver que $z(a, b) = (1, 0)$ est maintenant juste un calcul. $\square$

115. Définition 1.30.

Lemme 1.339.*L'application*

$$\begin{aligned}\varphi: \mathbb{R} &\rightarrow \mathbb{C} \\ x &\mapsto (x, 0)\end{aligned}\tag{1.513}$$

*est un morphisme d'anneaux*¹¹⁶.*Démonstration.* Simples calculs. Par exemple

$$\varphi(xx') = (xx', 0) = (x, 0)(x', 0) = \varphi(x)\varphi(x').\tag{1.514}$$

□

1.340.

Admirez ...

- Un nombre complexe est un couple de réels.
- Un réel est une classe d'équivalence de suites de Cauchy de rationnels.
- Une suite de Cauchy de rationnels est une application $\mathbb{N} \rightarrow \mathbb{Q}$ vérifiant certaines propriétés.
- Un rationnel est une classe d'équivalences d'éléments de $\mathbb{Z}$.
- Un élément de $\mathbb{Z}$ est une classe d'équivalence de couples de naturels.
- Un naturel sera ... là c'est plus compliqué. Une construction vraiment rigoureuse des naturels risque d'être en dehors du cadre du Frido.

Bref, les objets que nous manipulons sont d'une effroyable complexité.

1.341.À partir de maintenant, lorsque nous parlons de $\mathbb{R}$, nous parons en réalité de $\varphi(\mathbb{R}) \subset \mathbb{C}$.**Lemme 1.342.***Nous avons $(0, 1)^2 = (-1, 0)$. Nous notons $i = (0, 1)$.**Démonstration.* Calcul direct à partir de la définition 1.508.

□

Proposition 1.343 ([1]).*L'application*

$$\begin{aligned}f: \mathbb{R}^2 &\rightarrow \mathbb{C} \\ (a, b) &\mapsto a\varphi(1) + bi\end{aligned}\tag{1.515}$$

*est un isomorphisme de $\mathbb{R}$ -module*¹¹⁷.Cette proposition permet d'écrire tout nombre complexe sous la forme $a + bi$ pour des réels a et b .**Définition 1.344.***Si $z = a + bi$ est un nombre complexe (avec $a, b \in \mathbb{R}$), son **complexe conjugué** est le nombre $a - bi$.*

L'étude de la série géométrique est reportée à (beaucoup) plus tard, à la proposition 11.126. Dans l'immédiat il nous est possible de calculer la somme partielle.

Lemme 1.345 (Somme partielle de la série géométrique).*Soit $q \in \mathbb{C}$. Nous avons*

$$\sum_{n=0}^N q^n = \frac{1 - q^{N+1}}{1 - q}.\tag{1.516}$$

¹¹⁶. Définition 1.31.¹¹⁷. Module, définition 1.212.

Démonstration. Posons $S_N = 1 + q + \dots + q^N$. Nous avons évidemment $S_N - qS_N = 1 - q^{N+1}$ et donc

$$S_N = \sum_{n=0}^N q^n = \frac{1 - q^{N+1}}{1 - q}. \quad (1.517)$$

□

Chapitre 2

Théorie des groupes

Pour rappel, la notion de groupe est définie en 1.28.

2.1 Groupes

Définition 2.1 (centralisateur[60]).

Soient un groupe G , un sous-groupe H et un élément $h \in H$. Le **centralisateur** de h dans G est l'ensemble des éléments de G qui commutent avec h :

$$Z_G(h) = \{z \in G \text{ tel que } hz = zh\}. \quad (2.1)$$

Le centralisateur de H dans G est l'ensemble des éléments de G qui commutent avec tous les éléments de H :

$$Z_G(H) = \bigcap_{h \in H} Z_G(h). \quad (2.2)$$

Le **centre** d'un groupe G est l'ensemble des éléments de G qui commutent avec tous les autres :

$$Z_G = Z_G(G) = \{z \in G \text{ tel que } gz = zg \forall g \in G\}. \quad (2.3)$$

Définition 2.2 (normalisateur[60]).

Soient un groupe G et un sous-groupe H . Le **normalisateur** de H dans G est

$$\mathcal{N}_G(H) = \{g \in G \text{ tel que } gH = Hg\}. \quad (2.4)$$

Définition 2.3 (Sous-groupe normal).

Un sous-groupe N de G est **normal** ou **distingué** si pour tout $g \in G$ et pour tout $n \in N$, $gng^{-1} \in N$. Autrement dit lorsque $gNg^{-1} \subset N$.

Lorsque N est normal dans G il est parfois noté $N \triangleleft G$.

Définition 2.4.

Un sous-groupe H de G est un sous-groupe **caractéristique** si $\alpha(H) \subset H$ pour tout automorphismes¹ α de G .

Lemme 2.5 ([61]).

Si H est un sous-groupe caractéristique de G , alors $\alpha(H) = H$ pour tout automorphismes α de G .

Démonstration. Si α est un automorphisme de G , alors α^{-1} est encore un automorphisme de G . En particulier $\alpha^{-1}(H) \subset H$.

Soit $h \in H$. Nous devons prouver que $h \in \alpha(H)$. Pour cela :

$$h = \alpha(\alpha^{-1}(h)) \in \alpha(\alpha^{-1}(H)) \subset \alpha(H). \quad (2.5)$$

□

1. Automorphisme de groupe, définition 1.29.

Définition 2.6 (Groupe simple).

Un groupe est dit **simple** si il est non trivial et si les seuls sous-groupes normaux qu'il admet sont lui-même et le sous-groupe réduit à l'identité.

Définition 2.7 (Sous-groupe engendré).

Soit A une partie du groupe G . Le sous-groupe **engendré** par A est l'intersection de tous les sous-groupes de G contenant A . Nous notons ce groupe $\text{gr}_G(A)$.

Lorsque A est fini (disons $A = \{a_1, \dots, a_n\}$), on note aussi le sous-groupe engendré $\langle a_1, \dots, a_n \rangle$.

2.8.

Un sous-groupe engendré n'est jamais vide parce qu'il contient toujours au moins le neutre (parce que c'est un sous-groupe). Si G est un groupe, le sous-groupe $\text{gr}_G(\emptyset)$ lui-même contient e ².

2.9.

Dans de nombreux cas, le groupe « ambiant » G est entendu par le contexte et nous noterons $\text{gr}(A)$ au lieu de $\text{gr}_G(A)$.

Si par exemple A est la matrice $\begin{pmatrix} 4 & 5 \\ 6 & 7 \end{pmatrix}$, le groupe $\text{gr}(A)$ est à comprendre dans $\text{GL}(2, \mathbb{R})$. Il faudrait être fou pour avoir en tête un autre groupe que $\text{GL}(2, \mathbb{R})$ sans le préciser.

D'ailleurs, connaissez-vous un groupe contenant la matrice A et n'étant pas un sous-groupe de $\text{GL}(2, \mathbb{C})$?

Lemme 2.10.

Si G est un groupe et A une partie de G , alors $\text{gr}(A)$ est un sous-groupe de G .

Le sous-groupe engendré par A est le plus petit (pour l'inclusion) groupe de G contenant A . Plus formellement, nous avons le résultat suivant.

Lemme 2.11.

Tout sous-groupe de G contenant A contient $\text{gr}(A)$.

Démonstration. Si H est un sous-groupe de G contenant A , alors $\text{gr}(A)$ est l'intersection de H avec tous les autres sous-groupes de G contenant A . Il contient donc $\text{gr}(A)$. $\square$

Lemme 2.12 ([62]).

Si A est une partie du groupe G , alors le sous-groupe $\text{gr}(A)$ engendré³ par A est l'ensemble de tous les produits finis d'éléments de A et de A^{-1} (l'identité est le produit à zéro éléments).

C'est-à-dire que tout élément de $\text{gr}(A)$ peut être écrit sous la forme⁴

$$\prod_{i=1}^n g_i^{a_i} \quad (2.6)$$

où $a_i \in \mathbb{Z}$ et $g: \mathbb{N} \rightarrow A$ n'est pas spécialement injective : il peut arriver que $g_i = g_j$.

Démonstration. Vu qu'un produit vide est égal à l'identité, le lemme est vrai (un peu trivialement) dans le cas où $A = \emptyset$. À partir de maintenant nous supposons que A est non vide.

Nous nommons $\text{gr}(A)$ le groupe engendré par A et par H l'ensemble

$$H = \{g_1 \dots g_n \text{ tel que } g_i \in A \cup A^{-1}\}. \quad (2.7)$$

Nous commençons par prouver que H est un groupe.

- Vu que A est non vide, nous considérons $a \in A$. Dans ce cas, $e = aa^{-1} \in H$. Donc $e \in H$.
- L'inverse de $g_1 \dots g_n$ est $g_n^{-1} \dots g_1^{-1}$ qui est également dans H .

2. Demandez-vous si il est possible que $\text{gr}(\emptyset)$ contienne d'autres éléments que e .

3. Définition 2.7.

4. Les a_i négatifs correspondent aux inverses. Notons que si $g \in A$, il n'y a pas de garanties que g^{-1} soit également dans A .

— Le produit de $g_1 \dots g_n$ par $h_1 \dots h_n$ est également dans H ⁵.

Vu que H est un groupe contenant A , nous avons $\text{gr}(A) \subset H$ parce que $\text{gr}(A)$ est une intersection dont un des éléments est H .

Par ailleurs tout groupe contenant A doit contenir les inverses et les produits finis, donc $H \subset \text{gr}(A)$.

Au final, $H = \text{gr}(A)$, ce qu'il fallait. $\square$

Lemme 2.13.

Soit un groupe G et un sous-groupe $H = \text{gr}(h_1, \dots, h_n)$. Si $\alpha \in G$, alors

$$\alpha H \alpha^{-1} = \text{gr}(\alpha h_1 \alpha^{-1}, \dots, \alpha h_n \alpha^{-1}). \quad (2.8)$$

Démonstration. Il s'agit d'une conséquence du lemme 2.12. Un élément de $\text{gr}(\alpha h_1 \alpha^{-1}, \dots, \alpha h_n \alpha^{-1})$ est un produit d'éléments de G de la forme $\alpha h_i \alpha^{-1}$ ou $(\alpha h_j \alpha^{-1})^{-1} = \alpha h_j^{-1} \alpha^{-1}$. Or nous avons

$$\alpha h_i \alpha^{-1} \alpha h_j \alpha^{-1} = \alpha h_i h_j \alpha^{-1} \in \alpha H \alpha^{-1}. \quad (2.9)$$

Donc

$$\text{gr}(\alpha h_1 \alpha^{-1}, \dots, \alpha h_n \alpha^{-1}) \subset \alpha H \alpha^{-1}. \quad (2.10)$$

L'inclusion dans l'autre sens est du même tonneau. $\square$

Définition 2.14 (Partie génératrice, groupe monogène).

Soit G , un groupe et A une partie de G . Si $\text{gr}(A) = G$, alors nous disons que A est une **partie génératrice** le groupe G .

Un groupe est **monogène** s'il a une partie génératrice réduite à un seul élément.

Définition 2.15 (Groupe cyclique).

Un élément $a \in G$ est un **générateur** de G si tous les éléments de G s'écrivent sous la forme a^n pour un certain $n \in \mathbb{Z}$. Un groupe fini et monogène est dit **cyclique**.

Exemple 2.16.

Soit le groupe $(\mathbb{Z}/10\mathbb{Z}, +)$. L'élément $[2]_{10}$ n'est pas générateur parce que ses puissances⁶ sont

$$\text{gr}([2]_{10}) = \{[2]_{10}, [4]_{10}, [6]_{10}, [8]_{10}, [0]_{10}\}. \quad (2.11)$$

Par contre l'élément $[3]_{10}$ est générateur : ses puissances sont dans l'ordre

$$[3]_{10}, [6]_{10}, [9]_{10}, [2]_{10}, [5]_{10}, [8]_{10}, [1]_{10}, [4]_{10}, [7]_{10}, [0]_{10}. \quad (2.12)$$

$\triangle$

Un exemple presque identique, mais un peu masqué sera l'exemple 18.158.

2.2 Sous-groupe normal

Proposition 2.17.

Soit N un sous-groupe de G . Les propriétés suivantes sont équivalentes :

- (1) N est normal⁷ dans G .
- (2) N est une union de classes de conjugaison⁸ de G ,
- (3) $gNg^{-1} \subseteq N$ pour tout $g \in G$,

5. Et c'est ici qu'on se rend compte que la décomposition n'est probablement que rarement unique.

6. Attention aux notations ; en général on écrit la loi de groupe de façon multiplicative et on parle des puissances d'un élément, mais ici on écrit la loi de groupe additivement, donc les « puissances » sont en réalité les multiples.

7. Définition 2.3.

8. Définition 1.144.

- (4) $gNg^{-1} = N$ pour tout $g \in G$,
 (5) $gN = Ng$ pour tout $g \in G$,
 (6) Le normalisateur⁹ de N est $G : \mathcal{N}_G(N) = G$.

Démonstration. En plusieurs parties.

(1) implique (3) C'est la définition de sous-groupe normal.

(3) implique (4) Soit $g \in G$. Nous avons $gNg^{-1} \subset N$, mais aussi (en appliquant l'hypothèse à g^{-1}) $g^{-1}Ng \subset N$. En combinant nous avons

$$N \subset g(g^{-1}Ng)g^{-1} \subset gNg^{-1}. \quad (2.13)$$

Nous avons l'inclusion dans les deux sens. Donc l'égalité.

(4) implique (5) Soit $g \in G$. Un élément général de gN est de la forme gn avec $n \in N$. Nous devons trouver un $n' \in N$ tel que $gn = n'g$. En posant $n' = gng^{-1}$ nous avons

$$n' = gng^{-1} \in gNg^{-1} \subset N. \quad (2.14)$$

Il est immédiat de prouver que $gn = n'g$. Cela prouve que $gN \subset Ng$.

Le même raisonnement donne $Ng \subset gN$.

(5) implique (3) Un élément de gNg^{-1} est $a = gng^{-1}$ avec $n \in N$. Nous devons prouver que $a \in N$. Vu que $gn \in gN$, par hypothèse il existe n' tel que $gn = n'g$. En remplaçant dans la définition de a ,

$$a = gng^{-1} = n'gg^{-1} = n' \in N. \quad (2.15)$$

(5) implique (2) Pour chaque $a \in G$ nous notons C_a la classe de conjugaison de a dans G :

$$C_a = \{gag^{-1} \text{ tel que } g \in G\}. \quad (2.16)$$

Vu que $a \in C_a$ (prendre $g = e$ dans (2.16).) nous avons forcément

$$N \subset \bigcup_{n \in N} C_n. \quad (2.17)$$

Prouvons maintenant l'inclusion inverse. Nous avons déjà prouvé que (5) implique (3). Donc si $n \in N$, alors $gng^{-1} \in N$. Nous avons alors

$$C_n = \{gng^{-1} \text{ tel que } g \in G\} \subset N. \quad (2.18)$$

Donc il est vrai que $N = \bigcup_{n \in N} C_n$.

(2) implique (1) Nous supposons que $N \subset G$ est un sous-groupe de la forme

$$N = \bigcup_{a \in I} C_a \quad (2.19)$$

où I est une partie de G . Nous devons montrer que pour tout $g \in G$ et pour tout $n \in N$ nous avons $gng^{-1} \in N$. Vu que $n \in N$, il existe $a \in I$ tel que $n \in C_a$ et donc il existe $k \in G$ tel que $n = kak^{-1}$. Nous avons donc

$$gng^{-1} = g(kak^{-1})g^{-1} = (gk)a(gk)^{-1} \in C_a \subset N. \quad (2.20)$$

Le lecteur attentif aura remarqué l'utilisation de l'axiome du choix. La prudence l'incitera à ne pas le faire remarquer au jury.

(6) si et seulement si (5) C'est la définition du normalisateur.

□

9. Définition 2.2.

Définition 2.18.

Soit $g \in G$ et $n \in \mathbb{Z}$. Nous définissons g^n par

- (1) $g^0 = e$ et $g^n = gg^{n-1}$ si n est positif.
- (2) si $n < 0$, nous posons $g^n = (g^{-1})^{-n}$.

Définition 2.19 (Ordre d'un groupe et d'un élément).

Ce sont deux choses différentes.

- (1) Si G est un groupe, l'**ordre** est la cardinalité de G et est noté $|G|$.
- (2) L'**ordre** d'un élément g de G est le naturel

$$\min\{n \in \mathbb{N} \setminus \{0\} \text{ tel que } g^n = e\}, \quad (2.21)$$

s'il existe ; dans le cas contraire, nous disons que l'ordre de g est infini.

Nous verrons que le corolaire 2.36 au théorème de Lagrange dira que l'ordre d'un élément divise l'ordre du groupe.

Lemme 2.20 ([34, 13]).

Soient un groupe G et deux sous-groupes normaux¹⁰ H et K tels que $H \cap K = \{e\}$. Alors :

- (1) Tout élément de H commute avec tout élément de K .
- (2) HK est un sous-groupe de G .
- (3) L'application

$$\begin{aligned} \varphi: H \times K &\rightarrow HK \\ (h, k) &\mapsto hk \end{aligned} \quad (2.22)$$

est un isomorphisme de groupes.

Démonstration. Point par point.

- (1) Soient $h \in H$ et $k \in K$. Nous voulons montrer que $hk = kh$. Pour cela nous considérons l'élément $a = hkh^{-1}k^{-1}$. Vu que H est normal dans G , nous avons

$$kh^{-1}k^{-1} \in H \quad (2.23)$$

et donc $a \in H$. De même K étant normal dans G , nous avons $hkh^{-1} \in K$ et donc $a \in K$. Au final $a \in H \cap K = \{e\}$. Nous avons prouvé que

$$hkh^{-1}k^{-1} = e, \quad (2.24)$$

et donc que $hk = kh$.

- (2) Vu que H et K sont des sous-groupes, $\{e\}$ est dans les deux, de telle sorte que $e \in HK$. De plus si $h_i \in H$ et $k_i \in K$, la commutativité du point (1) donne

$$(h_1k_1)(h_2k_2) = h_1h_2k_1k_2 \in HK. \quad (2.25)$$

Donc le produit de deux éléments de HK est dans HK .

- (3) En trois sous-parties.

Homomorphisme Soient $h_i \in H$ et $k_i \in K$. En utilisant la commutativité du point (1) nous avons

$$\varphi((h_1, k_1)(h_2, k_2)) = \varphi(h_1h_2, k_1k_2) \quad (2.26a)$$

$$= (h_1h_2)(k_1k_2) \quad (2.26b)$$

$$= (h_1k_1)(h_2k_2) \quad (2.26c)$$

$$= \varphi(h_1, k_1)\varphi(h_2, k_2). \quad (2.26d)$$

10. Sous-groupe normal, définition 2.3.

Injectif Si $\varphi(h_1, k_1) = \varphi(h_2, k_2)$ nous avons successivement

$$h_1 k_1 = h_2 k_2 \quad (2.27a)$$

$$h_1 k_1 h_2^{-1} = k_2 \quad (2.27b)$$

$$h_1 k_1 h_2^{-1} k_1^{-1} = k_2 k_1^{-1} \quad (2.27c)$$

$$h_1 h_2^{-1} = k_2 k_1^{-1}. \quad (2.27d)$$

Le membre de gauche est un élément de H et le membre de droite un élément de K . Vu que $H \cap K = \{e\}$ nous avons $h_1 h_2^{-1} = e$ et $k_2 k_1^{-1} = e$, c'est à dire $h_1 = h_2$ et $k_1 = k_2$.

Surjectif Une élément général de HK est hk avec $h \in H$ et $k \in K$. Cela est l'image de (h, k) par φ . □

Définition 2.21.

L'**exposant** du groupe G est le plus petit entier non nul n tel que $g^n = e$ pour tout $g \in G$. S'il n'existe pas, nous disons que l'exposant du groupe est infini.

Proposition 2.22.

Si l'ensemble des ordres de tous les éléments d'un groupe est majoré, alors l'exposant du groupe est le plus petit commun multiple des ordres des éléments du groupe

Pour un groupe fini, l'exposant est le ppcm des ordres des éléments du groupe.

Le théorème de Burnside 9.209 nous donnera un bon paquet d'exemples de groupes d'exposant fini dans $GL(n, \mathbb{C})$.

Proposition 2.23.

Soit un groupe G . Nous considérons un sous-groupe normal H de G ainsi qu'un homomorphisme $\psi: G \rightarrow H$. Alors

- (1) $\psi(H)$ est normal dans $\psi(G)$
- (2) Si G/H est abélien alors $\psi(G)/\psi(H)$ est abélien.

Démonstration. Soient $h \in H$ et $g \in G$. Alors $\psi(g)\psi(h)\psi(g)^{-1} = \psi(ghg^{-1}) \in \psi(H)$. Donc $\psi(H)$ est normal dans $\psi(G)$.

Pour la seconde partie nous notons $[\dots]$ les classes par rapport à $\psi(H)$ et $\overline{\dots}$ celles par rapport à H . Nous avons

$$[\psi(g_1)][\psi(g_2)] = [\psi(g_1)\psi(g_2)] \quad (2.28a)$$

$$= [\psi(g_1 g_2)] \quad (2.28b)$$

$$= \{\psi(g_1 g_2)\psi(h) \text{ tel que } h \in H\} \quad (2.28c)$$

$$= \{\psi(g_1 g_2 h) \text{ tel que } h \in H\} \quad (2.28d)$$

$$= \psi(\{g_1 g_2 h \text{ tel que } h \in H\}) \quad (2.28e)$$

$$= \psi(\overline{g_1 g_2}) \quad (2.28f)$$

$$= \psi(\overline{g_2 g_1}) \quad (2.28g)$$

$$= \text{refaire à l'envers} \quad (2.28h)$$

$$= [\psi(g_2)][\psi(g_1)]. \quad (2.28i)$$

Par conséquent $\psi(G)/\psi(H)$ est abélien. □

2.3 Groupe dérivé

Définition 2.24.

Si G est un groupe et si $g, h \in G$, nous notons $[g, h] = ghg^{-1}h^{-1}$ le **commutateur** de g et h .

L'élément neutre est toujours un commutateur : pour $g = h$, $[g, g] = ggg^{-1}g^{-1} = e$.

Définition 2.25.

Le **groupe dérivé** de G est le sous-groupe noté $D(G)$ ou $[G, G]$ engendré¹¹ par les commutateurs.

Autrement dit, $D(G)$ est l'intersection de tous les sous-groupes de G contenant tous les commutateurs. Le groupe $D(G)$ contient toujours au moins le neutre parce que c'est un groupe.

En vertu du lemme 2.12, le groupe dérivé de G est l'ensemble des produits finis de commutateurs. C'est-à-dire que si S_m est l'ensemble des produits de m commutateurs, alors

$$D(G) = \bigcup_{m=1}^{\infty} S_m. \quad (2.29)$$

Lemme 2.26.

Le groupe dérivé est un sous-groupe caractéristique¹², et un sous-groupe normal¹³.

Démonstration. Il est évident que si $\alpha \in \text{Aut}(G)$ alors

$$\alpha([g, h]) = [\alpha(g), \alpha(h)], \quad (2.30)$$

c'est-à-dire que $D(G)$ est un sous-groupe caractéristique. En particulier si c est un commutateur, alors xcx^{-1} en est encore un, ce qui montre que $D(G)$ est normal dans G . Plus spécifiquement,

$$x(ghg^{-1}h^{-1})x^{-1} = (xgx^{-1})(xhx^{-1})(xg^{-1}x^{-1})(xh^{-1}x^{-1}) \quad (2.31a)$$

$$= (xgx^{-1})(xhx^{-1})(xgx^{-1})^{-1}(xhx^{-1})^{-1}. \quad (2.31b)$$

□

Proposition 2.27.

Le groupe quotient $G/D(G)$ est abélien.

Démonstration. En ce qui concerne le fait que $G/D(G)$ soit abélien, nous savons que pour tout $g, h \in G$ nous avons $h^{-1}g^{-1}hg \in D(G)$ et donc

$$[g][h] = [gh] = [ghh^{-1}g^{-1}hg] = [hg] = [h][g]. \quad (2.32)$$

□

Le groupe quotient $G/D(G)$ est appelé l'**abélianisé** de G et est parfois noté G^{ab} .

Si $f: G \rightarrow A$ est un homomorphisme entre le groupe G et un groupe abélien A , alors $f(D(G)) = \{0\}$. Du coup f passe au quotient de G par $D(G)$, et il existe une unique application $\bar{f}: G/D(G) \rightarrow A$ telle que $f = \bar{f} \circ \pi$ où $\pi: G \rightarrow G/D(G)$ est la projection canonique.

2.4 Théorèmes d'isomorphismes

Définition 2.28.

Soient un groupe G , un ensemble X et une application $f: X \rightarrow G$. Le **noyau** de f est la partie

$$\ker(f) = \{x \in X \text{ tel que } f(x) = e\} \quad (2.33)$$

où e est l'unité de G .

Si G est un groupe et si N est un sous-groupe normal, alors l'ensemble G/N a une structure de groupe et la projection canonique $\pi: G \rightarrow G/N$ est un homomorphisme surjectif de noyau N .

11. Définition 2.7.

12. Définition 2.4.

13. Définition 2.3.

Théorème 2.29 (Premier théorème d'isomorphisme).

Soit $\theta: G \rightarrow H$ un homomorphisme de groupe. Alors

- (1) $\text{Ker } \theta$ est normal dans G ,
- (2) $\text{Image } \theta$ est un sous-groupe de H
- (3) nous avons un isomorphisme naturel

$$G/\text{Ker } \theta \simeq \text{Image } \theta \quad (2.34)$$

Démonstration. Point par point.

- (1) Le fait que $\text{Ker } \theta$ soit un sous-groupe de G est clair ; montrons qu'il est normal. Si $g \in G$ et $u \in \text{Ker } \theta$, alors $\theta(g^{-1}ug) = \theta(g^{-1})\theta(u)\theta(g) = (\theta(g))^{-1}\theta(g) = 1_H$, et donc $g^{-1}ug \in \text{Ker } \theta$.
- (2) Il suffit de remarquer que si $h = \theta(g)$ et $h' = \theta(g')$, alors $h^{-1}h' = \theta(g^{-1}g')$.
- (3) Si $[g]$ représente la classe de g dans $G/\text{Ker } \theta$, l'isomorphisme est donné par $\varphi[g] = \theta(g)$.

□

Théorème 2.30 (Deuxième théorème d'isomorphisme).

Soient H et N deux sous-groupes de G et supposons que N soit normal. Alors

- (1) $NH = HN$ est un sous-groupe.
- (2) Le groupe N est normal dans NH .
- (3) Le groupe $N \cap H$ est normal dans H .
- (4) Nous avons l'isomorphisme

$$\frac{HN}{N} \simeq \frac{H}{H \cap N}. \quad (2.35)$$

- (5) L'isomorphisme du point (4) est encore valable si N n'est pas normal mais si seulement H normalise N , c'est-à-dire si $hNh^{-1} \in N$ pour tout $h \in H$.

Démonstration. Point par point.

- (1) Il est clair que $1_G \in NH$. Soient nh et $n'h'$ deux éléments de NH ; alors en tenant compte du fait que N est normal,

$$nhn'h' = n \underbrace{hn'h^{-1}}_{\in N} hh' \in NH. \quad (2.36)$$

Cela prouve que NH est un groupe.

De la même façon, nous prouvons que HN est un groupe par

$$hnh'n' = hh' \underbrace{h'^{-1}nh'}_{\in N} n' \in HN \quad (2.37)$$

Nous devons encore prouver que $HN = NH$. Pour cela, $nh \in HN$, car $nh = hh^{-1}nh$, les trois derniers facteurs formant un élément de N par normalité ; de même $hn \in NH$, montrant que $NH = HN$. Enfin, comme $(nh)^{-1} = h^{-1}n^{-1}$, les inverses de NH sont dans $HN = NH$.

- (2) N est normal dans G , a fortiori dans l'un de ses sous-groupes.
- (3) Il suffit de voir que, si $h \in H$ et $n \in N \cap H$, alors $hnh^{-1} \in N \cap H$. Or, $hnh^{-1} \in H$ puisque H est un sous-groupe ; et $hnh^{-1} \in N$ car N est un sous-groupe normal de G .
- (4) Il faut d'abord remarquer que H et N étant des groupes et le produit NH étant un groupe, nous avons $NH = HN$. Soit le morphisme injectif

$$\begin{aligned} j: H &\rightarrow HN \\ h &\mapsto h \end{aligned} \quad (2.38)$$

et la surjection canonique

$$\sigma: HN \rightarrow HN/N \quad (2.39)$$

Nous considérons ensuite l'application composée

$$\begin{aligned} f: H &\rightarrow HN/N \\ h &\mapsto hN. \end{aligned} \quad (2.40)$$

f est surjective L'application f est surjective parce que l'élément $hnN \in HN/N$ est l'image de h , étant donné que $hnN = hN$.

$\text{Ker}(f) = H \cap N$ Si $a \in H \cap N$, nous avons $f(a) = aN = N$, et donc $H \cap N \subset \text{Ker } f$. D'autre part, si $h \in H$ vérifie $h \in \text{Ker } f$, alors $f(h) = hN = N$, ce qui est uniquement possible si $h \in N$.

Le premier théorème d'isomorphisme implique alors que $H/\text{Ker } f \simeq \text{Image } f$, c'est-à-dire

$$H/N \cap H \simeq HN/N. \quad (2.41)$$

□

Théorème 2.31 (Troisième théorème d'isomorphisme).

Soient N et M deux sous-groupes normaux de G avec $M \subset N$. Alors N/M est normal dans G/M et

$$(G/M)/(N/M) \simeq G/N. \quad (2.42)$$

Démonstration. Afin de montrer que N/M est normal dans G/M , nous considérons $g \in G$, $nM \in N/M$ et nous calculons

$$gnMg^{-1} = gng^{-1} \underbrace{gMg^{-1}}_{=M} = \underbrace{gng^{-1}}_{\in N} M \in N/M. \quad (2.43)$$

Pour prouver l'isomorphisme nous considérons le morphisme

$$\begin{aligned} \varphi: G/M &\rightarrow G/N \\ gM &\mapsto gN. \end{aligned} \quad (2.44)$$

C'est surjectif et le noyau est N/M parce que $\varphi(gM) = N$ uniquement si $g \in N$. Nous pouvons appliquer le premier théorème d'isomorphisme à φ en écrivant

$$(G/M)/\text{Ker } \varphi \simeq \text{Image } \varphi, \quad (2.45)$$

c'est-à-dire

$$(G/M)/(N/M) \simeq G/N. \quad (2.46)$$

□

2.5 Indice d'un sous-groupe et ordre des éléments

Lemme 2.32.

Lorsque H est normal dans G , alors la définition

$$[a] \cdot [b] = [ab] \quad (2.47)$$

définit une loi de groupe sur l'ensemble G/H .

Démonstration. Le neutre est $[e]$ et l'associativité ne pose pas plus de problèmes que l'existence d'un inverse. Le point à vérifier est que la formule (2.47) est une bonne définition : $[ah] \cdot [bh'] = [ab]$ pour tout $h, h' \in H$. Nous avons :

$$[ah] \cdot [ah'] = [ahah'] = [ahb]. \quad (2.48)$$

Pour montrer que cela est $[ab]$, l'astuce est d'introduire bb^{-1} à côté du a :

$$[ahb] = [abb^{-1}hb] = [ab] \quad (2.49)$$

parce que $b^{-1}hb \in H$ du fait que H soit normal dans G . $\square$

Exemple 2.33 ([63]).

Il ne faudrait pas croire que le groupe quotient G/H est forcément un sous-groupe de G . Par exemple le quotient $\mathbb{Z}/2\mathbb{Z}$ est l'ensemble $\{0, 1\}$ muni de l'addition. En particulier $1 + 1 = 0$, ce qui est évidemment faux dans $\mathbb{Z}$. Le groupe $(\mathbb{Z}, +)$ ne possède aucun élément d'ordre 2.

Il n'en est pas moins vrai que l'application

$$\begin{aligned} f: G &\rightarrow G/H \\ g &\mapsto [g] \end{aligned} \quad (2.50)$$

est un morphisme de groupes. $\triangle$

Définition 2.34.

Si H est un sous-groupe d'un groupe fini l'**indice** de H dans G est le nombre $|G|/|H|$, souvent noté $|G : H|$.

Le théorème de Lagrange dira en particulier que l'indice est toujours un nombre entier. C'est à ne pas confondre avec le degré d'une extension de corps (définition 6.56).

Théorème 2.35 (Théorème de Lagrange).

Soit H un sous-groupe du groupe fini G . Alors

- (1) L'ordre de H divise l'ordre de G .
- (2) Les trois nombres suivants sont égaux :
 - le nombre de classes de H à gauche,
 - le nombre de classes de H à droite,
 - l'indice de H dans G .

En particulier si H est distingué dans G nous avons

$$|G/H| = \frac{|G|}{|H|}. \quad (2.51)$$

Démonstration. Nous commençons par montrer que les classes de H ont toutes le même nombre d'éléments que H . En effet pour chaque $g \in G$ nous avons la bijection

$$\begin{aligned} \varphi: H &\rightarrow gH \\ h &\mapsto gh. \end{aligned} \quad (2.52)$$

L'injectivité de φ est le fait que $gh = gh'$ implique $h = h'$. La surjectivité est par définition de la classe.

Les classes à gauche formant une partition de G , le cardinal de G est le produit de la taille des classes par le nombre de classes :

$$|G| = |H| \cdot \text{nombre de classes}. \quad (2.53)$$

En particulier nous voyons que $|H|$ divise $|G|$.

La dernière formule exprime simplement que G/H est par définition le nombre de classes de H à gauche (ou à droite) dans G . $\square$

Corolaire 2.36.

L'ordre d'un élément d'un groupe fini divise l'ordre du groupe. En particulier dans un groupe d'ordre n tous les éléments vérifient $q^n = e$.

Démonstration. Soit G un groupe fini et considérons, à $g \in G$ fixé, le sous-groupe

$$H = \{g^k \text{ tel que } k \in \mathbb{N}\}. \quad (2.54)$$

Par le théorème de Lagrange 2.35, l'ordre de H divise $|G|$, mais l'ordre de H est le plus petit k tel que $g^k = e$, c'est-à-dire l'ordre de g . $\square$

D'autres résultats à propos d'ordres et d'indices de groupes finis dans la proposition 3.30 et le lemme 3.32. En particulier le théorème de Cauchy 3.26 qui dit si p divise l'ordre du groupe G , alors G contient au moins un élément d'ordre p .

2.6 Suite de composition

Définition 2.37.

Une **suite de composition** pour un groupe G est une suite finie de sous-groupes $(G_i)_{i=0,\dots,n}$ telle que

$$\{e\} = G_n \subseteq G_{n-1} \subseteq \dots \subseteq G_1 \subseteq G_0 = G \quad (2.55)$$

et telle que G_{i+1} est normal¹⁴ dans G_i . Les groupes G_i/G_{i+1} sont les **quotients** de la suite de composition.

Une suite de **Jordan-Hölder** est une suite de composition dont tous les quotients sont simples.

L'objet de nos prochaines pérégrinations mathématiques est de montrer que tout groupe fini admet une suite de Jordan-Hölder (théorème 2.42).

Lemme 2.38 (du papillon[64]).

Soit G un groupe et des sous-groupes A et B . Soit A' normal dans A et B' normal dans B . Alors

- (1) $A'(A \cap B')$ est normal dans $A'(A \cap B)$
- (2) $(A' \cap B)B'$ est normal dans $(A \cap B)B'$
- (3) Nous avons les isomorphismes de groupes

$$\frac{A'(A \cap B)}{A'(A \cap B')} \simeq \frac{(A \cap B)B'}{(A' \cap B)B'} \simeq \frac{B'(A \cap B)}{B'(A' \cap B)}. \quad (2.56)$$

Démonstration. Nous n'allons pas démontrer chacun des points ; pour plus de détails, nous dirons simplement que « la preuve est très similaire dans les autres cas ».

Commençons par montrer que $A'(A \cap B')$ est un groupe. Si $a, b \in A'$ et $x, y \in A \cap B'$,

$$axby = xx^{-1}axbx^{-1}xy \quad (2.57)$$

En utilisant la normalité, $x^{-1}ax \in A'$, donc $xx^{-1}axbx^{-1} \in A'$ et donc le tout est dans $A'(A \cap B')$. L'ensemble $A'(A \cap B')$ est également stable pour l'inverse parce que

$$x^{-1}a^{-1} = \underbrace{x^{-1}a^{-1}x}_{\in A'} x^{-1}. \quad (2.58)$$

14. Nous rappelons au cas où que « normal » signifie « distingué ».

Nous montrons maintenant que $A'(A \cap B')$ est normal dans $A'(A \cap B)$. Soient $a, b \in A'$, $x \in A \cap B'$ et $f \in A \cap B$. Alors

$$(bf)^{-1}(ax)(bf) = (bf)^{-1}(a \underbrace{xbx^{-1}}_{=c \in A'} xf) \quad (2.59a)$$

$$= f^{-1}b^{-1}acxf \quad (2.59b)$$

$$= f^{-1}b^{-1}acf \underbrace{f^{-1}xf}_{=y \in A \cap B'} \quad (2.59c)$$

$$= \underbrace{f^{-1}b^{-1}acf}_{\in A'} y \quad (2.59d)$$

$$\in A'(A \cap B'). \quad (2.59e)$$

Pour prouver l'isomorphisme

$$\frac{A'(A \cap B)}{A'(A \cap B')} = \frac{(A \cap B)B'}{(A' \cap B)B'}, \quad (2.60)$$

nous allons utiliser le deuxième théorème d'isomorphisme (2.31(5)). Que nous appliquons à $H = A \cap B$ et $N = A'(A \cap B')$. La vérification que H normalise N est usuelle. Nous commençons par écrire

$$\frac{A'(A \cap B')(A \cap B)}{A'(A \cap B')} \simeq \frac{A \cap B}{A \cap B \cap A'(A \cap B')}. \quad (2.61)$$

Pour simplifier un peu cette expression nous prouvons d'abord que

$$(A \cap B) \cap A'(A \cap B') = (A' \cap B)(A \cap B'). \quad (2.62)$$

L'inclusion $\supset$ est facile. Pour l'autre sens, étant donné que $A'(A \cap B') \subset A$ nous avons

$$A \cap B \cap A'(A \cap B) = B \cap A'(A \cap B). \quad (2.63)$$

Un élément de $B \cap A'(A \cap B)$ est un élément de B qui s'écrit sous la forme $s = ax$ avec $a \in A'$ et $x \in A \cap B'$. Nous avons alors $a = sx^{-1}$ avec $s \in B$ et $x^{-1} \in B'$. Par conséquent $a \in B$ et donc $a \in A' \cap B$. Nous avons donc

$$(A \cap B) \cap A'(A \cap B') = B \cap A'(A \cap B) \subset (A' \cap B)(A \cap B'), \quad (2.64)$$

et donc l'égalité (2.62). Toujours dans l'idée de simplifier (2.61) nous remarquons que $A \cap B'$ est un sous-ensemble de $A \cap B'$, donc $A'(A \cap B')(A \cap B) = A'(A \cap B)$. Il reste donc

$$\frac{A'(A \cap B)}{A'(A \cap B')} = \frac{A \cap B}{(A' \cap B)(A \cap B')}. \quad (2.65)$$

Étant donné que les hypothèses sur A et B sont symétriques, le membre de droite peut aussi s'écrire en inversant A et B . Nous en sommes à

$$\frac{B'(A \cap B)}{B'(A' \cap B)} = \frac{A'(A \cap B)}{A'(A \cap B')}. \quad (2.66)$$

Nous devons encore justifier $B'(A \cap B) = (A \cap B)B'$ et $B'(A' \cap B) = (A' \cap B)B'$. Faisons le premier et laissons le second **au lecteur**. Si $b \in B'$ et $x \in A \cap B$, alors

$$bx = x \underbrace{x^{-1}bx}_{\in B'} \in (A \cap B)B'. \quad (2.67)$$

□

Proposition 2.39.

Si G est un groupe fini et que (G_i) est une suite de composition pour G , alors l'ordre de G est le produit des ordres de ses quotients.

Démonstration. Étant donné que G_{i+1} est toujours normal dans G_i , le théorème de Lagrange (2.35) s'applique et nous avons à chaque pas de la suite de composition nous avons

$$\left| \frac{G_i}{G_{i+1}} \right| = \frac{|G_i|}{|G_{i+1}|} \quad (2.68)$$

et il suffit d'écrire $|G|$ de façon télescopique :

$$|G| = \prod_{0 \leq i \leq n-1} \frac{|G_i|}{|G_{i+1}|} \quad (2.69)$$

□

Nous disons que les deux suites de composition $(G_i)_{0 \leq i \leq r}$ et $(G_j)_{0 \leq j \leq s}$ sont **équivalentes** si $r = s$ et s'il existe une permutation $\sigma \in S_{r-1}$ telle que

$$\frac{G_i}{G_{i+1}} \simeq \frac{H_{\sigma(i)}}{H_{\sigma(i)+1}}. \quad (2.70)$$

Proposition 2.40 (Schreider).

Deux suites de composition d'un même groupe admettent des raffinements équivalents.

Démonstration. Soient les suites de composition

$$\{e\} = G_m \subseteq \dots \subseteq G_1 \subseteq G_0 = G \quad (2.71a)$$

$$\{e\} = H_m \subseteq \dots \subseteq H_1 \subseteq H_0 = G \quad (2.71b)$$

Nous raffinons la suite (G_i) en remplaçant $G_{i+1} \subseteq G_i$ par

$$G_{i+1} = G_{i+1}(G_i \cap H_n) \subset G_{i+1}(G_i \cap H_{n-1}) \subseteq \dots \subseteq G_{i+1}(G_i \cap H_0) = G_i, \quad (2.72)$$

et de même pour (H_j) . Le groupe $G_{i+1}(G_i \cap H_k)$ est normal dans $G_{i+1}(G_i \cap H_{k-1})$ parce que G_{i+1} étant normal dans G_i et H_k dans H_{k-1} , le lemme 2.38 s'applique. Nous avons donc bien défini un raffinement.

Nous devons maintenant prouver que les deux raffinements ainsi construits sont des suites de composition équivalentes. D'abord elles ont la même longueur mn parce que chacun des m éléments de la suite (G_i) a été remplacé par n éléments et inversement, chacun de n éléments de la suite (H_j) a été remplacé par m éléments.

Par ailleurs, les quotients du raffinement de (G_i) sont de la forme

$$\frac{G_{i+1}(G_i \cap H_k)}{G_{i+1}(G_i \cap H_{k+1})} \simeq \frac{H_{k+1}(H_k \cap G_i)}{H_{k+1}(H_k \cap G_{i+1})} \quad (2.73)$$

en vertu du lemme du papillon (2.38). Le membre de droite de (2.73) est un des quotients du raffinement de (H_j) . □

Lemme 2.41 (Schreider strictement décroissant).

Soient Σ_1 et Σ_2 , deux suites de composition strictement décroissantes du groupe G . Alors elles admettent des raffinements équivalents strictement décroissants.

Démonstration. Par hypothèse, Σ_1 et Σ_2 n'ont pas de répétitions. Soient Σ_1'' et Σ_2'' , des raffinements équivalents donnés par le lemme de Schreider. Étant donné que ce sont des suites de composition équivalentes, elles ont le même nombre de quotients réduits à $\{e\}$, c'est-à-dire le même nombre de répétitions.

Les suites Σ_1' et Σ_2' obtenues en retirant les répétitions de Σ_1'' et Σ_2'' sont des raffinements équivalents de Σ_1 et Σ_2 et strictement décroissants. □

Théorème 2.42 (Jordan-Hölder).

Tout groupe fini admet une suite de Jordan-Hölder.

Deux suites de Jordan-Hölder sont équivalentes.

Démonstration. Nous ne prouvons que le second point.

Par définition, une suite de Jordan-Hölder n'a pas de raffinement strictement décroissant (à part elle-même) parce que G_{i+1} est normal maximum dans G_i . Si Σ_1 et Σ_2 sont des suites de Jordan-Hölder nous pouvons considérer les raffinements équivalents strictement décroissants Σ'_1 et Σ'_2 du lemme de Schreider 2.41. Nous avons $\Sigma'_1 \sim \Sigma'_2$, mais par ce que nous venons de dire à propos de la maximalité, $\Sigma'_1 = \Sigma_1$ et $\Sigma'_2 = \Sigma_2$. D'où le résultat. $\square$

2.7 Groupes résolubles

Définition 2.43.

Le groupe G est **résoluble** s'il existe une suite finie de sous-groupes G_i

$$\{e\} = G_n \subset G_{n-1} \subset \dots \subset G_1 \subset G_0 = G \quad (2.74)$$

avec G_i normal dans G_{i+1} et G_i/G_{i+1} abélien.

Il s'agit d'un groupe qui admet une suite de composition ¹⁵ dont les quotients sont abéliens.

Lemme 2.44 ([65]).

Soit G un groupe et H un sous-groupe normal. Le groupe G/H est abélien si et seulement si $D(G) \subset H$.

Démonstration. Les propositions suivantes sont équivalentes :

- Le groupe G/H est abélien
- pour tout $x, y \in G$, $\bar{x}\bar{y} = \bar{y}\bar{x}$
- $\bar{x}\bar{y}\bar{x}^{-1}\bar{y}^{-1} = \bar{e}$
- $\overline{xyx^{-1}y^{-1}} = \bar{e}$
- $[x, y] \in H$
- $D(G) \subset H$.

$\square$

Proposition 2.45 ([65]).

Un groupe est résoluble si et seulement si sa suite dérivée termine sur $\{e\}$.

Démonstration. Grâce au lemme 2.26 et à la proposition 2.27, si la suite dérivée termine sur $\{e\}$ alors la suite dérivée est une suite qui répond aux conditions de la définition 2.43 de groupe résoluble.

Il faut donc encore montrer le sens direct. Nous supposons que G est un groupe résoluble et nous étudions sa suite dérivée. Nous avons une suite

$$\{e\} = G_n \subset G_{n-1} \subset \dots \subset G_1 \subset G_0 = G \quad (2.75)$$

avec G_i/G_{i+1} abélien et G_{i+1} normal dans G_i . Nous allons prouver par récurrence que $D^i(G) \subset G_i$.

Pour $i = 0$ nous avons bien $G \subset G_0$. Notre hypothèse de récurrence est :

$$D^i(G) \subset G_i \quad (2.76)$$

Par le lemme 2.44 nous avons aussi

$$D(G_i) \subset G_{i+1}. \quad (2.77)$$

En dérivant (2.76) et en tenant compte de (2.77), $D^{i+1}(G) \subset D(G_i) \subset G_{i+1}$. Donc par récurrence nous avons bien $D^k(G) \subset G_k$ pour tout k . Mais $G_r = \{e\}$ pour un certain r , donc pour ce r nous avons $D^r(G) = \{e\}$, ce qu'il fallait. $\square$

15. Voir définition 2.37.

Proposition 2.46.

Soient des groupes G et H . Nous supposons que G est résoluble et nous considérons un homomorphisme $\psi: G \rightarrow H$. Alors $\psi(G)$ est résoluble.

Démonstration. Vu que G est résoluble, il existe une suite de sous-groupes G_i tels que

$$\{e\} = G_n \subset G_{n-1} \subset \dots \subset G_1 \subset G_0 = G \quad (2.78)$$

avec G_i normal dans G_{i+1} et G_i/G_{i+1} abélien. Nous posons $\psi(G)_i = \psi(G_i)$ et nous avons $\psi(G)_n = \psi(\{e\}) = \{e\}$ ainsi que $\psi(G)_0 = \psi(G)$; donc

$$\{e\} = \psi(G)_n \subset \psi(G)_{n-1} \subset \dots \subset \psi(G)_1 \subset \psi(G)_0 = \psi(G). \quad (2.79)$$

Les faits que $\psi(G)_i$ soit normal dans $\psi(G)_{i+1}$ et que $\psi(G)_i/\psi(G)_{i+1}$ soit abélien est directement la proposition 2.23.

□

2.8 Action de groupes

Le concept d'action d'un groupe est donné par la définition 1.246

Lemme 2.47.

Pour tout $g \in G$,

- (1) L'application $\phi_g: E \rightarrow E$ est injective,
- (2) Pour l'inverse : $(\phi_g)^{-1} = \phi_{g^{-1}}$.

Démonstration. Si $x, y \in E$ sont tels que $\phi_g(x) = \phi_g(y)$ alors en appliquant $\phi_{g^{-1}}$ aux deux membres nous trouvons

$$(\phi_{g^{-1}}\phi_g)(x) = (\phi_{g^{-1}}\phi_g)(y), \quad (2.80)$$

ce qui donne $x = y$ parce que $\phi_{g^{-1}}\phi_g = \phi_{g^{-1}g} = \phi_e = \text{Id}$.

Les dernières trois égalités écrites disent que $\phi_{g^{-1}}$ est l'inverse¹⁶ de ϕ_g .

□

Pour alléger les notations, on convient d'écrire $g \cdot x$, voire plus simplement gx au lieu de $\phi_g(x)$. Le deuxième axiome d'action de groupe dit que la notation ghx ne souffre d'aucune ambiguïté.

Définition 2.48 (Quelques notions autour de l'action).

Si G agit sur un ensemble E , nous notons $G \cdot x$ l'**orbite** de $x \in E$ sous l'action de G :

$$G \cdot x = \{gx \text{ tel que } g \in G\}.$$

Nous notons G_x ou $\text{Fix}(x)$ le **stabilisateur** de x :

$$\text{Fix}(x) = G_x = \{g \in G \text{ tel que } g \cdot x = x\}. \quad (2.81)$$

Pour $g \in G$, nous notons enfin $\text{Fix}(g)$ le **fixateur** de g :

$$\text{Fix}(g) = \{x \in E \text{ tel que } g \cdot x = x\}. \quad (2.82)$$

Définition 2.49.

L'action de G sur E est **fidèle** si l'identité est le seul élément de G à fixer tous les points de E , c'est-à-dire si $gx = x \forall x \in E \Rightarrow g = e$.

Un exemple d'action fidèle tout à fait non trivial sera donné avec l'action du groupe modulaire sur le plan de Poincaré dans le théorème 23.95.

Le groupe G agit toujours sur lui-même à gauche et à droite. L'action à gauche est $g \cdot h = gh$; celle à droite est $g \cdot h = hg^{-1}$.

16. Si vous décidez de dire ça a un jury dans un concours, soyez prêts à préciser les domaines.

Définition 2.50.

L'action **adjointe** définie par $g \cdot h = ghg^{-1}$ est une manière pour un groupe d'agir sur lui-même par automorphismes. Cela est souvent noté $\mathbf{Ad}(g)h = ghg^{-1}$.

En effet pour tout $g \in G$, l'application $\mathbf{Ad}(g): G \rightarrow G$ est un automorphisme de G .

Si H est un sous-groupe de G , nous notons G/H le quotient de G par la relation $g \sim gh$ pour tout $h \in H$. Lorsque la distinction est importante, nous noterons $(G/H)_g$ pour les classes à gauche et $(G/H)_d$ pour les classes à droite.

Nous avons une relation d'équivalence à gauche et une à droite. D'abord

$$x \sim_g y \Leftrightarrow xh = y \quad (2.83)$$

pour un certain $h \in H$. Ensuite

$$x \sim_d y \Leftrightarrow hx = y \quad (2.84)$$

pour un certain $h \in H$.

Le lemme suivant est une généralisation du théorème de Lagrange 2.35.

Lemme 2.51.

L'ensemble $(G/H)_g$ est fini si et seulement si l'ensemble $(G/H)_d$ est fini. S'il en est ainsi, alors $(G/H)_g$ et $(G/H)_d$ ont même cardinal qui vaut l'indice de H dans G .

Démonstration. L'application

$$\begin{aligned} f: (G/H)_g &\rightarrow (G/H)_d \\ [x]_g &\mapsto [x^{-1}]_d \end{aligned} \quad (2.85)$$

est une bijection bien définie. En effet si $x \sim_g y$, nous avons $h \in H$ tel que $y^{-1}h = x^{-1}$, c'est-à-dire que $x^{-1} \sim_d y^{-1}$ et f est bien définie. Le fait que f soit surjective est évident. Pour l'injectivité, soient $x, y \in G$ tels que

$$f([x]_g) = f([y]_g). \quad (2.86)$$

Alors $x^{-1} \sim_d y^{-1}$, ce qui implique l'existence de $h \in H$ tel que $hx^{-1} = y^{-1}$, ou encore que $xh^{-1} = y$, ce qui signifie que $x \sim_g y$.

Pour l'énoncé à propos de l'indice, nous procédons en plusieurs étapes simples.

- (1) Les classes (les éléments de $(G/H)_g$) forment une partition de G .
- (2) Toutes les classes ont le même nombre d'éléments par la bijection

$$\begin{aligned} f: [x]_g &\rightarrow [y]_g \\ xh &\mapsto yh. \end{aligned} \quad (2.87)$$

- (3) Le nombre d'éléments dans une classe est égal à $|H|$ par la bijection

$$\begin{aligned} g: [x]_g &\rightarrow H \\ xh &\mapsto h. \end{aligned} \quad (2.88)$$

Par conséquent

$$|G| = |H| \cdot \text{nombre de classes} = |H| \cdot \text{cardinal de } (G/H)_g, \quad (2.89)$$

et nous avons bien

$$\text{cardinal de } (G/H)_g = \frac{|G|}{|H|} = |G : H|. \quad (2.90)$$

□

Proposition 2.52 (Orbite-stabilisateur[32]).

Soit G un groupe agissant sur un ensemble E et $x \in E$.

- (1) Les ensembles $G \cdot x$ et G/G_x sont équipotents.

(2) L'orbite de $\text{Fix}(x)$ est finie si et seulement si $\text{Fix}(x)$ est d'indice fini dans G . Dans ce cas nous avons

$$\text{Card}(G \cdot x) = |G : \text{Fix}(x)|. \quad (2.91)$$

Une autre façon d'écrire la même formule :

$$|G| = |\text{Fix}(x)| |\mathcal{O}_x|. \quad (2.92)$$

C'est la formule (2.91) qui est nommée **formule des classes** sur wikipédia.

Démonstration. (1) Soit l'application

$$\begin{aligned} \psi: G \cdot x &\rightarrow G/G_x \\ a \cdot x &\mapsto [a]. \end{aligned} \quad (2.93)$$

Cette application est bien définie parce que si $a \cdot x = b \cdot x$, alors il existe $h \in G_x$ tel que $b = ah$, et par conséquent $[a] = [b]$. Cette application est une bijection et par conséquent $G \cdot x$ est équipotent à G/G_x .

(2) Soit $y \in \mathcal{O}_x$ et $A_y = \{g \in G \text{ tel que } g \cdot x = y\}$. L'ensemble A_y est une classe à gauche de $\text{Fix}(x)$, par conséquent $|A_y| = |\text{Fix}(x)|$ pour tout $y \in \mathcal{O}_x$. Les A_y pour différents y sont disjoints et nous avons de plus

$$\bigcup_{y \in \mathcal{O}_x} A_y = G. \quad (2.94)$$

Les ensembles A_y divisent donc G en $|\mathcal{O}_x|$ paquets de $|\text{Fix}(x)|$ éléments. D'où la formule (2.92). □

Corolaire 2.53.

Soit C_g la classe de conjugaison d'un élément g du groupe fini G . Alors

$$\text{Card}(C_g) = |G : Z_G(g)| \quad (2.95)$$

où $Z_G(g)$ est le centralisateur de g dans G ¹⁷ de G .

Démonstration. Cela est une application de la proposition 2.52 (formule (2.91)) dans le cas de l'action adjointe de G sur lui-même.

En effet, si nous considérons l'action adjointe, l'orbite est la classe de conjugaison : $C_g = G \cdot g$. Et le stabilisateur de g pour l'action adjointe n'est autre que le centralisateur de g :

$$\text{Fix}(g) = \{h \in G \text{ tel que } h \cdot g = g\} \quad (2.96a)$$

$$= \{h \in G \text{ tel que } hgh^{-1} = g\} \quad (2.96b)$$

$$= \{h \in G \text{ tel que } gh = hg\} \quad (2.96c)$$

$$= Z_G(g). \quad (2.96d)$$

Donc la formule $\text{Card}(G \cdot g) = |G : Z_G(g)|$ devient, dans le cas de l'action adjointe de G sur lui-même : $\text{Card}(C_g) = |G : Z_G(g)|$. □

Lemme 2.54.

Soit G un groupe agissant sur l'ensemble E . On définit $x \sim x'$ si et seulement s'il existe $g \in G$ tel que $g \cdot x = x'$. Alors

(1) la relation $\sim$ est une relation d'équivalence.

(2) la classe $[x]$ est l'orbite $\mathcal{O}_x$ de x sous G .

Corolaire 2.55 (Équation des orbites).

Soit G un groupe agissant sur l'ensemble E et $\mathcal{O}_1, \dots, \mathcal{O}_k$ la liste des orbites (distinctes). Alors

17. Définition 2.1.

- (1) $E = \bigcup_i \mathcal{O}_i$, l'union est disjointe,
 (2) $\text{Card}(E) = \sum_i \text{Card}(\mathcal{O}_i)$.

Définition 2.56.

Soit G un groupe agissant sur l'ensemble E . Un **domaine fondamental** ou une **transversale** est une partie de E contenant un et un seul élément de chaque orbite.

Autrement dit, les images des éléments d'un domaine fondamental forment une partition de l'ensemble :

$$E = \bigsqcup_{g \in G} g(F) \quad (2.97)$$

où $g(F) = \phi_g(F) = \{\phi_g(x) \text{ tel que } x \in F\}$. L'union est disjointe, c'est-à-dire que si $g \neq g'$, alors $g(F) \cap g'(F) = \emptyset$.

Proposition 2.57 (Équation des classes[66]).

Soit G , un groupe fini opérant sur un ensemble E . Si E'' est un ensemble contenant exactement un élément de chaque orbite dans $E \setminus \text{Fix}_G(E)$, alors

$$|G| = |\text{Fix}_G(E)| + \sum_{x \in E''} \frac{|G|}{|\text{Fix}_G(x)|}. \quad (2.98)$$

Si de plus G est un p -groupe, alors

$$|E| = |\text{Fix}_G(E)| \pmod{p}. \quad (2.99)$$

Démonstration. Par le corolaire 2.55, nous avons $|G| = \sum_{x \in E'} |\mathcal{O}_x|$ où E' est une transversale. En séparant la somme entre les orbites à un élément et les autres,

$$|G| = \text{Card}(\text{Fix}_G(E)) + \sum_{x \in E''} \frac{|G|}{|\text{Fix}_G(x)|} \quad (2.100)$$

où nous avons utilisé le fait que $|G| = |\text{Fix}_G(x)| |\mathcal{O}_x|$.

Si G est un p -groupe alors si $x \in E''$, $\text{Fix}_G(x)$ est un sous-groupe propre de G et donc $|\text{Fix}_G(x)|$ est un diviseur propre de $|G|$. Du coup la fraction $|G|/|\text{Fix}_G(x)|$ est une puissance non nulle de p et l'équation (2.98) devient immédiatement (2.99). $\square$

Corolaire 2.58 (Équation des classes).

Soit G , un groupe et $C_1, \dots, C_l$ la liste de ses classes de conjugaison contenant plus de un élément. Alors

$$\text{Card}(G) = \text{Card}(Z(G)) + \sum_i |G : Z_{g_i}| = \text{Card}(Z(G)) + \sum_i \frac{\text{Card}(G)}{\text{Card}(\text{Fix}(g_i))} \quad (2.101)$$

si $g_i \in C_i$.

Démonstration. Étant donné que les classes de conjugaison sont disjointes, le cardinal de G est bien la somme des cardinaux de ses classes. Les classes ne contenant que un seul élément sont celles des éléments de $Z(G)$. En ce qui concerne les autres orbites, $\text{Card}(C_{g_i}) = |G : Z_{g_i}|$ par le théorème orbite-stabilisateur (proposition 2.52). $\square$

Théorème 2.59 (Formule de Burnside).

Si G est un groupe fini agissant sur l'ensemble fini E et si Ω est l'ensemble des orbites, alors

$$\text{Card}(\Omega) = \frac{1}{|G|} \sum_{g \in G} \text{Card}(\text{Fix}(g)). \quad (2.102)$$

Démonstration. Nous considérons l'ensemble

$$A = \{(g, x) \in G \times E \text{ tel que } gx = x\}, \quad (2.103)$$

et nous en calculons le cardinal de deux façons. D'abord

$$\text{Card}(A) = \sum_{x \in E} \text{Card}\{g \in G \text{ tel que } gx = x\} \quad (2.104a)$$

$$= \sum_{x \in E} \text{Card}(\text{Fix}(x)) \quad (2.104b)$$

$$= \sum_{\omega \in \Omega} \sum_{x \in \omega} \text{Card}(\text{Fix}(x)) \quad (2.104c)$$

$$= \sum_{\omega \in \Omega} \frac{|G|}{\text{Card}(\omega)} \quad (2.104d)$$

$$= |G|. \quad (2.104e)$$

Pour obtenir (2.104d) nous avons utilisé l'équation des classes (2.92). L'autre façon de calculer $\text{Card}(A)$ est de regrouper ainsi :

$$\text{Card}(A) = \sum_{g \in G} \text{Card}\{x \in E \text{ tel que } gx = x\} = \sum_{g \in G} \text{Card}(\text{Fix}(g)). \quad (2.105)$$

En égalisant les deux expressions de $\text{Card}(A)$ nous trouvons

$$|G| \text{Card}(\Omega) = \sum_{g \in G} \text{Card}(\text{Fix}(g)). \quad (2.106)$$

□

Proposition 2.60.

Soit G un groupe et H , un sous-groupe du centre de G .

- (1) H est normal dans G .
- (2) Si G/H est monogène, alors G est abélien.
- (3) Si G est fini de centre Z , alors $|G : H|$ n'est pas premier.

Théorème 2.61.

Soit G un groupe cyclique¹⁸ d'ordre n .

- (1) Tout sous-groupe de G est cyclique.
- (2) Pour chaque diviseur d de n , il existe un unique sous-groupe H_d de G d'ordre d .

Si a est un générateur de G , alors H_d peut être décrit des façons suivantes :

$$H_d = \{x \in G \text{ tel que } x^d = e\} = \{x \in G \text{ tel que } \exists y \in G \text{ tel que } y^{n/d} = x\} = \langle a^{n/d} \rangle. \quad (2.107)$$

Définition 2.62.

Soit G un groupe agissant sur un ensemble E . Nous disons que l'action est **transitive** si elle possède une seule orbite. L'action est **libre** si $g \cdot x = g' \cdot x$ implique $g = g'$.

2.9 Produit semi-direct de groupes

Définition 2.63.

Une **suite exacte** est une suite d'applications comme suit :

$$\dots \xrightarrow{f_i} A_i \xrightarrow{f_{i+1}} A_{i+1} \xrightarrow{f_{i+2}} \dots \quad (2.108)$$

où pour chaque i , les applications f_i et f_{i+1} vérifient $\ker(f_{i+1}) = \text{Image}(f_i)$. Lorsque les ensembles A_i sont des groupes, alors nous demandons de plus que les f_i soient des homomorphismes.

18. Définition 2.15.

Très souvent nous sommes confrontés à des suites exactes de la forme

$$1 \longrightarrow A \xrightarrow{f} G \xrightarrow{g} B \longrightarrow 1 \quad (2.109)$$

où G , A et B sont des groupes, 1 est l'identité. La première flèche est l'application $\{1\} \rightarrow A$ qui à 1 fait correspondre 1 . La dernière est l'application $B \rightarrow 1$ qui à tous les éléments de B fait correspondre 1 . Le noyau de f étant l'image de la première flèche (c'est-à-dire $\{1\}$), l'application f est injective. L'image de g étant le noyau de la dernière flèche (c'est-à-dire B en entier), l'application g est surjective.

Définition 2.64.

Soient N et H deux groupes et un morphisme de groupes $\phi: H \rightarrow \text{Aut}(N)$. Le **produit semi-direct** de N et H relativement à ϕ , noté $N \times_{\phi} H$ est l'ensemble $N \times H$ muni de la loi (que l'on vérifiera être de groupe)

$$(n, h) \cdot (n', h') = (n\phi_h(n'), hh'). \quad (2.110)$$

Attention à l'ordre quelque peu contre-intuitif. Lorsque nous notons $N \times_{\phi} H$, c'est bien $\phi: H \rightarrow \text{Aut}(N)$, c'est-à-dire H qui agit sur N et non le contraire.

Lorsque N et H sont des sous-groupes d'un même groupe, le plus souvent ϕ est l'action adjointe définie en 2.50.

Le théorème suivant permet de reconnaître un produit semi-direct lorsqu'on en voit un.

Théorème 2.65 ([7]).

Soit une suite exacte de groupes

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{s} H \longrightarrow 1 \quad (2.111)$$

S'il existe un sous-groupe $\tilde{H}$ de G à partir duquel s est un isomorphisme, alors

$$G \simeq i(N) \times_{\sigma} \tilde{H} \quad (2.112)$$

où σ est l'action adjointe¹⁹ de $\tilde{H}$ sur $i(N)$.

Démonstration. Nous posons $\tilde{N} = i(N)$ et nous allons subdiviser la preuve en petits pas.

- (1) $\tilde{N}$ est normal dans G . En effet étant donné que la suite est exacte nous avons $\tilde{N} = \ker(s)$. Le noyau d'un morphisme est toujours un sous-groupe normal.
- (2) $\tilde{N} \cap \tilde{H} = \{e\}$. L'application s étant un isomorphisme depuis $\tilde{H}$, il n'y a pas d'éléments de $\tilde{H}$ dans $\ker(s)$ autre que e .
- (3) $G = \tilde{N}\tilde{H}$. Nous considérons $g \in G$ et $h \in \tilde{H}$ tel que $s(g) = s(h)$. L'existence d'un tel h est assurée par le fait que s est surjective depuis $\tilde{H}$. Du coup nous avons $e = s(gh^{-1})$, c'est-à-dire $gh^{-1} \in \ker(s) = \tilde{N}$. Nous avons donc bien la décomposition $g = (gh^{-1})h$, et donc $G = \tilde{N}\tilde{H}$.
- (4) L'écriture $g = nh$ avec $n \in \tilde{N}$ et $h \in \tilde{H}$ est unique. Si $nh = n'h'$, alors $n = n'h'h^{-1}$, ce qui signifierait que $h'h^{-1} \in \tilde{N}$. Mais étant donné que $\tilde{H} \cap \tilde{N} = \{e\}$, nous obtenons $h = h'$ et par suite $n = n'$.
- (5) L'application

$$\begin{aligned} \phi: G &\rightarrow \tilde{N} \times \tilde{H} \\ nh &\mapsto (n, h) \end{aligned} \quad (2.113)$$

est une bijection. C'est une conséquence des points (3) et (4).

- (6) Si sur $\tilde{N} \times \tilde{H}$ nous mettons le produit

$$(n, h) \cdot (n', h') = (n\sigma_h n', hh') \quad (2.114)$$

19. Le fait que H agisse sur $i(N)$ fait partie du théorème.

où σ est l'action adjointe du groupe sur lui-même, c'est-à-dire $\sigma_x(y) = xyx^{-1}$, alors ϕ est un isomorphisme. Si $g, g' \in G$ s'écrivent (de façon unique par le point (5)) $g = nh$ et $g' = n'h'$ alors

$$\phi(nhn'h') = \phi(n \underbrace{hn'h^{-1}}_{\in \tilde{N}} hh') \quad (2.115a)$$

$$= \phi((nhn'h^{-1})(hh')) \quad (2.115b)$$

$$= (nhn'h^{-1}, hh') \quad (2.115c)$$

$$= (n, h) \cdot (n', h') \quad (2.115d)$$

$$= \phi(nh)\phi(n'h'). \quad (2.115e)$$

□

Corolaire 2.66.

Soit G un groupe, et N, H des sous-groupes de G tels que

- (1) H normalise N (c'est-à-dire que $hnh^{-1} \in N$ pour tout $h \in H$ et $n \in N$ ²⁰),
- (2) $H \cap N = \{e\}$,
- (3) $HN = G$.

Alors l'application

$$\begin{aligned} \psi: N \times_{\sigma} H &\rightarrow G \\ (n, h) &\mapsto nh \end{aligned} \quad (2.116)$$

est un isomorphisme de groupes.

Dans les hypothèses, l'ordre entre N et H est important lorsqu'on dit que c'est N qui agit sur H ; mais l'hypothèse $NH = G$ est équivalente à $HN = G$ (passer à l'inverse pour s'en assurer).

Insistons encore un peu sur la notation : dans $N \times_{\sigma} H$, c'est H qui agit sur N par σ .

2.10 Groupe de torsion

Soit G un groupe. Un élément $g \in G$ est un **élément de torsion** s'il est d'ordre fini. La **torsion** de G est l'ensemble de ses éléments de torsion. Nous disons qu'un groupe est un **groupe de torsion** si tous ses éléments sont de torsion.

Exemple 2.67.

Le groupe additif $\mathbb{Q}/\mathbb{Z}$ est un groupe de torsion parce que si $[x] = [p/q]$, alors $q[x] = [p] = [0]$. $\triangle$

2.11 Famille presque nulle

Soit $(G, +)$ un groupe abélien et $\mathcal{F} = \{g_i\}_{i \in I}$ une famille d'éléments de G indicés par un ensemble I . Le **support** de $\mathcal{F}$ est l'ensemble $\{i \in I \text{ tel que } g_i \neq 0\}$. La famille est dite **presque nulle** si le support est fini.

Nous disons que $\mathcal{F}$ est une **suite** si $I = \mathbb{N}$.

20. Ou encore que H agit sur N par automorphismes internes.

Chapitre 3

Anneaux

Attention aux conventions. Dans le Frido, un corps peut être réduit à $\{0\}$ et un idéal premier ne peut pas être $\{0\}$. Ces conventions ont une série de conséquences un peu partout, par exemple dans la proposition 3.75 où nous parlons d'idéal maximum propre. Comparez par exemple avec [67]. Soyez attentifs.

En cas de doutes, nous suivons les conventions de Wikipédia.

3.1 Inversibles et nilpotents

Le concept d'anneau est la définition 1.30.

Lemme 3.1.

Si a et b commutent, nous avons, pour tout $r \in \mathbb{N}$ et $r > 0$, la formule

$$a^{r+1} - b^{r+1} = (a - b) \left(\sum_{k=0}^r a^{r-k} b^k \right). \quad (3.1)$$

Démonstration. Démontrons cela par récurrence. Le cas $r = 0$ est évident. Pour un r donné, si (3.1) est vraie, alors

$$\begin{aligned} a^{r+2} - b^{r+2} &= a^{r+1}a - a^{r+1}b + a^{r+1}b - b^{r+1}b \\ &= a^{r+1}(a - b) + (a^{r+1} - b^{r+1})b \\ &= a^{r+1}(a - b) + (a - b) \left(\sum_{k=0}^r a^{r-k} b^k \right) b \\ &= (a - b) \left(a^{r+1} + \left(\sum_{k=0}^r a^{r-k} b^k \right) b \right) \\ &= (a - b) \left(a^{r+1} + \sum_{k=0}^r a^{r-k} b^{k+1} \right) \\ &= (a - b) \left(a^{r+1} + \sum_{k'=1}^{r+1} a^{(r+1)-k'} b^{k'} \right) \\ &= (a - b) \left(\sum_{k'=0}^{r+1} a^{(r+1)-k'} b^{k'} \right). \end{aligned}$$

□

Proposition 3.2.

Si a est un élément nilpotent de l'anneau A , alors $1 - a$ est inversible. Si a est nilpotent non nul, alors il est diviseur de zéro.

Démonstration. Soit n le minimum tel que $a^n = 0$. En vertu de la formule (3.1) nous avons

$$1 = 1 - a^n = (1 - a)(1 + a + \cdots + a^{n-1}) = (1 + a + \cdots + a^{n-1})(1 - a). \quad (3.2)$$

La somme $1 + a + \cdots + a^{n-1}$ est donc un inverse de $(1 - a)$. $\square$

3.2 PGCD, PPCM et éléments inversibles

La définition de pgcd et ppcm dans un anneau commutatif est la définition 1.169. Dans la plus grande tradition, elle a été introduite sans motivations, et utilisée par-ci par-là. Nous revenons maintenant dessus.

Commençons par donner une autre vision de la divisibilité dans les anneaux intègres.

Proposition 3.3.

Dans un anneau intègre¹ A , on a l'équivalence suivante concernant deux éléments $a, b \in A$:

$$a \mid b \Leftrightarrow (b) \subset (a). \quad (3.3)$$

Donc la divisibilité devient en réalité une relation d'ordre dont nous pouvons chercher un maximum et un minimum. Si S est une partie de A , nous notons $a \mid S$ pour exprimer que $a \mid x$ pour tout $x \in S$; de la même façon, $S \mid b$ signifie que $x \mid b$ pour tout $x \in S$.

Nous rappelons également la définition 1.31 de morphisme d'anneaux. Remarquons que si f est un morphisme, nous avons $f(0) = 0$ et $f(x)^{-1} = f(x^{-1})$.

Lemme 3.4 ([68]).

Les éléments inversibles d'un anneau sont diviseurs de tous les éléments.

Démonstration. Soit k inversible d'inverse $k' : kk' = 1$; soit aussi $a \in A$. Alors $a = k(k'a)$, ce qui montre que k divise a . $\square$

Lemme 3.5 ([68]).

Dans un anneau, 1 est un pgcd de a et b si et seulement si les seuls diviseurs communs sont les inversibles.

Démonstration. Supposons pour commencer que 1 est un pgcd de a et b . Un diviseur commun de a et b doit donc diviser 1. Or un diviseur de 1 est forcément inversible.

Dans l'autre sens, les diviseurs communs de a et b sont tous inversibles et donc diviseurs de 1. Donc 1 est un pgcd de a et b . $\square$

3.2.1 Calcul effectif du PGCD et de Bézout

Soient a et b , deux entiers que nous allons prendre positifs. Nous allons voir maintenant l'algorithme de **Euclide étendu** qui est capable, pour a et b donnés, de calculer le PGCD de a et b , et un couple de Bézout (u, v) tel que $ua + vb = \text{pgcd}(a, b)$. Ce calcul est indispensable si on veut implémenter RSA (19.2).

Cela se base sur le lemme suivant.

Lemme 3.6.

Soient $a, b \in \mathbb{N}$ et des nombres q et r tels que $a = qb + r$. Alors $\text{pgcd}(a, b) = \text{pgcd}(r, b)$.

Démonstration. Il suffit de voir que les diviseurs communs de a et b sont diviseurs de r et que les diviseurs communs de r et b divisent a .

Si s divise a et b , alors dans l'équation

$$\frac{a}{s} = \frac{qb}{s} + \frac{r}{s}$$

1. Définition 1.174.

les termes a/s et qb/s sont entiers, donc r/s est aussi entier, et s divise r .

Inversement, si s divise r et b , alors il divise $qb + r$ et donc a . $\square$

Remarque 3.7.

Ce lemme est surtout intéressant lorsque $a = qb + r$ est la division euclidienne de a par b : en effet, dans ce cas $r < b$, et le calcul du PGCD de deux nombres (a et b) est ramené à un calcul de PGCD de deux nombres plus petits (b et r).

L'algorithme pour calculer $\text{pgcd}(a, b)$ consiste à écrire des divisions euclidiennes successives de la manière suivante :

$$a = q_2b + r_2 \qquad r_2 < b \qquad (3.4a)$$

$$b = q_3r_2 + r_3 \qquad r_3 < r_2 \qquad (3.4b)$$

$$\vdots \qquad (3.4c)$$

en remarquant que $\text{pgcd}(a, b) = \text{pgcd}(b, r_2) = \text{pgcd}(r_2, r_3)$. Étant donné que les inégalités $r_2 < b$ et $r_3 < r_2$ sont strictes, en continuant ainsi nous finissons sur zéro, c'est-à-dire qu'il existera un n pour lequel $r_{n+1} = 0$; et donc

$$r_{n-1} = q_{n+1}r_n,$$

et à ce moment nous avons $\text{pgcd}(a, b) = \text{pgcd}(r_{n-1}, r_n) = r_n$.

3.2.1.1 Algorithme d'Euclide pour le PGCD

Écrivons l'algorithme[69] en détail (parce que Bézout, ça va être la même chose en cinq fois plus compliqué). On pose

$$r_0 = a \qquad (3.5a)$$

$$r_1 = b \qquad (3.5b)$$

(ce qui explique que nous n'ayons pas utilisé r_0 et r_1 précédemment). Ensuite on écrit la division euclidienne $a = q_2b + r_2$, c'est-à-dire $r_0 = q_2r_1 + r_2$. Cela donne r_2 et q_2 en termes de r_0 et r_1 :

$$r_2 = r_0 - q_2r_1. \qquad (3.6)$$

Ensuite, sachant r_2 nous pouvons continuer :

$$r_1 = q_3r_2 + r_3 \qquad (3.7)$$

donne q_3 et $r_3 = r_1 - q_3r_2$. On continue avec $r_2 = q_4r_3 + r_4$. Tout cela pour poser la suite

$$\begin{aligned} r_0 &= a \\ r_1 &= b \\ r_k &= q_{k+2}r_{k+1} + r_{k+2} \end{aligned} \qquad (3.8)$$

où la troisième définit r_{k+2} et q_{k+2} en fonction de r_k et r_{k+1} , à l'aide du théorème de la division euclidienne. La suite (r_k) ainsi construite est strictement décroissante et à chaque étape le lemme 3.6 et le principe de l'algorithme d'Euclide nous donnent

$$\begin{cases} \text{pgcd}(r_k, r_{k+1}) = \text{pgcd}(r_{k+1}, r_{k+2}) = \text{pgcd}(a, b) \\ 0 \leq r_{k+1} < r_k. \end{cases} \qquad \begin{aligned} (3.9a) \\ (3.9b) \end{aligned}$$

La suite étant strictement décroissante, nous prenons r_n , le dernier non nul : $r_{n+1} = 0$. Dans ce cas la dernière équation sera

$$r_{n-1} = q_nr_n \qquad (3.10)$$

avec $\text{pgcd}(a, b) = \text{pgcd}(r_n, r_{n-1}) = r_n$.

Exemple 3.8.

Calculons le PGCD de 18 et 231. Pour cela nous écrivons les divisions euclidiennes en chaîne :

$$231 = 18 \cdot 12 + 15 \quad (3.11a)$$

$$18 = 1 \cdot 15 + 3 \quad (3.11b)$$

$$15 = 5 \cdot 3 + 0. \quad (3.11c)$$

Donc le PGCD est 3 (le dernier reste non nul). $\triangle$

3.2.1.2 Algorithme étendu : calcul effectif des coefficients de Bézout

La difficulté est de construire la suite qui donne des coefficients de Bézout. Elle va être construite à l'envers. Nous supposons déjà connaître la liste complète des r_k jusqu'à $r_n = \text{pgcd}(a, b)$, ainsi que la liste complète des divisions euclidiennes

$$r_k = q_{k+2}r_{k+1} + r_{k+2}. \quad (3.12)$$

Nous voulons trouver les couples (u_k, v_k) de telle façon à avoir à chaque étape

$$r_n = u_k r_k + v_k r_{k-1}. \quad (3.13)$$

Notons que c'est à chaque fois r_n que nous construisons. La première équation de type Bézout à résoudre est

$$r_n = u_n r_n + v_n r_{n-1}, \quad (3.14)$$

sachant que $r_{n-1} = q_n r_n$. On pose $v_n = 0$ et $u_n = 1$ et c'est bon. Pour la récurrence, supposons les coefficients u_k et v_k connus, et déterminons les coefficients u_{k-1} et v_{k-1} . Pour ce faire, nous égalons les deux expressions pour r_n :

$$r_n = u_k r_k + v_k r_{k-1} = u_{k-1} r_{k-1} + v_{k-1} r_{k-2}; \quad (3.15)$$

dans laquelle nous substituons $r_{k-2} = q_k r_{k-1} - r_k$:

$$u_k r_k + v_k r_{k-1} = u_{k-1} r_{k-1} + v_{k-1} (q_k r_{k-1} - r_k) \quad (3.16)$$

$$= (u_{k-1} + q_k v_{k-1}) r_{k-1} - v_{k-1} r_k \quad (3.17)$$

et nous égalons les coefficients de r_k et r_{k-1} pour obtenir

$$\begin{cases} v_{k-1} = u_k \\ u_{k-1} = v_k - v_{k-1} q_k. \end{cases} \quad (3.18a)$$

$$(3.18b)$$

Dès que u_k et v_k ainsi que q_k sont connus, on peut calculer u_{k-1} et v_{k-1} .

La dernière équation, celle avec $k = 1$, est

$$r_n = u_1 r_1 + v_1 r_0, \quad (3.19)$$

c'est-à-dire

$$\text{pgcd}(a, b) = u_1 b + v_1 a. \quad (3.20)$$

Nous avons ainsi trouvé des coefficients de Bézout pour a et b .

3.2.2 Générateurs**Proposition 3.9** ([70]).

Soit $n \geq 2$.

(1) L'anneau $\mathbb{Z}/n\mathbb{Z}$ contient n éléments

(2) Nous avons $\mathbb{Z}/n\mathbb{Z} = \{[k]_n\}_{k=0, \dots, n-1}$.

Proposition 3.10 ([70]).

Soient $n \geq 2$, a premier avec n , $b \in \mathbb{N}$, et $m_1, \dots, m_n \in \mathbb{N}$. Alors

- (1) Nous avons $\mathbb{Z}/n\mathbb{Z} = \{[am_i + b]_n\}_{i=1, \dots, n}$,
- (2) Nous avons $\mathbb{Z}/n\mathbb{Z} = \{[b + k]_n\}_{k=0, \dots, n-1}$
- (3) Nous avons $\mathbb{Z}/n\mathbb{Z} = \{[ka]_{k=0, \dots, n-1}\}$.

Proposition 3.11 ([70]).

Soit $n \geq 2$ et $m \in \mathbb{Z}$. Nous avons équivalence entre

- (1) $\text{pgcd}(n, m) = 1$,
- (2) $[m]_n$ engendre le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$
- (3) $[m]_n$ est inversible dans $((\mathbb{Z}/n\mathbb{Z})^*, \cdot)$.

3.2.3 Générateurs pour le groupe multiplicatif

Cette section est presque certainement à déplacer.

Proposition 3.12 ([71]).

Le groupe $((\mathbb{Z}/n\mathbb{Z})^*, \cdot)$ est cyclique.

La proposition suivante est un pas important dans l'algorithme de Shor permettant aux ordinateurs quantiques de factoriser rapidement des grands nombres.

Proposition 3.13 ([72]).

Soient $A, B \in \mathbb{N}$ tels que $\text{pgcd}(A, B) = 1$. Alors il existe $p, m \in \mathbb{N}$ tels que $A^p = mB + 1$.

3.2.4 Décomposition en facteurs premiers**Lemme 3.14** (Lemme de Gauss).

Soient $a, b, c \in \mathbb{Z}$ tels que a divise bc . Si a est premier avec c , alors a divise b .

Démonstration. Vu que a est premier avec c , nous avons $\text{pgcd}(a, c) = 1$ et le théorème de Bézout 1.181 nous donne donc $s, t \in \mathbb{Z}$ tels que $sa + tc = 1$. En multipliant par b , nous avons $sab + tbc = b$. Mais les deux termes du membre de gauche sont multiples de a parce que a divise bc . Par conséquent b est somme de deux multiples de a et donc est multiple de a . $\square$

Lemme 3.15 (Lemme d'Euclide[73]).

Si un nombre premier p divise le produit de deux nombres entiers b et c , alors p divise b ou c .

Démonstration. Vu que p est premier, s'il ne divise pas a c'est que $\text{pgcd}(a, p) = 1$. Dans ce cas le lemme de Gauss 3.14 implique que p divise b . $\square$

Le théorème fondamental de l'arithmétique permet de décomposer des nombres en facteurs premiers.

Théorème 3.16 (Décomposition en facteurs premiers[74]).

Tout entier strictement positif peut être écrit comme un produit de nombres premiers d'une unique façon, à l'ordre près des facteurs.

En d'autres termes, pour tout entier $n > 1$, il existe une unique suite finie unique $(p_1, k_1), \dots, (p_r, k_r)$ telle que :

- (1) les p_i sont des nombres premiers tels que, si $i < j$, alors $p_i < p_j$;
- (2) les k_i sont des entiers naturels non nuls ;
- (3) $n = \prod_{i=1}^r p_i^{k_i}$.

Démonstration. Soit n un entier positif. Nous prouvons l'existence d'une décomposition en facteurs premiers par récurrence. Le nombre $n = 1$ est le produit d'une famille finie de nombres premiers : la famille vide.

Supposons que tout entier strictement inférieur à un certain entier $n > 1$ est produit de nombres premiers. Deux possibilités apparaissent pour n : il est premier ou non. Si n est premier, et donc produit d'un unique entier premier, à savoir lui-même, le résultat est vrai. Si n n'est pas premier, il se décompose sous la forme kl avec k et l strictement inférieurs à n . Dans ce cas, l'hypothèse de récurrence implique que les entiers k et l peuvent s'écrire comme produits de nombres premiers. Leur produit aussi, ce qui fournit une décomposition de n en produit de nombres premiers. Par application du principe de récurrence, tous les entiers naturels peuvent s'écrire comme produit de nombres premiers.

Nous prouvons maintenant l'unicité. Prenons deux produits de nombres premiers qui sont égaux. Prenons n'importe quel nombre premier p du premier produit. Il divise le premier produit, et, de là, aussi le second. Par le lemme d'Euclide 3.15, p doit alors diviser au moins un facteur dans le second produit. Mais les facteurs sont tous des nombres premiers eux-mêmes, donc p doit être égal à un des facteurs du second produit. Nous pouvons donc simplifier par p les deux produits. En continuant de cette manière, nous voyons que les facteurs premiers des deux produits coïncident précisément. $\square$

Lemme 3.17 ([1]).

Nous notons $\mathcal{P}$ l'ensemble des nombres premiers dans $\mathbb{N}$. Soient des suites finies $(a_p)_{p \in \mathcal{P}}$ et $(b_p)_{p \in \mathcal{P}}$. Nous posons

$$a = \prod_{p \in \mathcal{P}} p^{a_p} \quad \text{et} \quad b = \prod_{p \in \mathcal{P}} p^{b_p}. \quad (3.21)$$

Alors $a \mid b$ si et seulement si $a_p \leq b_p$ pour tout p .

Démonstration. Dire que $a \mid b$ signifie qu'il existe $s \in \mathbb{N}$ tel que $as = b$; le théorème 3.16 nous permet de décomposer s en $s = \prod_{p \in \mathcal{P}} p^{s_p}$. Vu que le produit dans $\mathbb{N}$ est commutatif et associatif,

$$b = as = \prod_{p \in \mathcal{P}} p^{s_p + a_p}. \quad (3.22)$$

Par unicité de la décomposition de b (toujours le théorème 3.16), nous en déduisons que $b_p = s_p + a_p \geq a_p$.

Dans l'autre sens, l'hypothèse $a_p \leq b_p$ implique l'existence de $s_p \geq 0$ tels que $b_p - a_p = s_p$. En posant $s = \prod_{p \in \mathcal{P}} p^{s_p}$, nous avons

$$as = \prod_{p \in \mathcal{P}} p^{s_p + a_p} = \prod_{p \in \mathcal{P}} p^{b_p} = b. \quad (3.23)$$

Donc $a \mid b$. $\square$

Proposition 3.18.

Soient $x \in \mathbb{Z}$ ainsi que $p, q \in \mathbb{N}$. Si q divise x^p , alors q divise x .

Lemme 3.19.

Soient un nombre premier q ainsi que $a \in \mathbb{Z}$. Soit un naturel $n \geq 1$. Le nombre q divise a si et seulement si il divise a^n .

Démonstration. Nous numérotions les nombres premiers p_i pour que p_1 soit q . La décomposition en nombre premiers du théorème 3.16 nous dit que

$$a = q^{a_1} \prod_{i \neq 1} p_i^{a_i} \quad (3.24)$$

et

$$a^n = q^{na_1} \prod_{i \neq 1} p_i^{na_i} \quad (3.25)$$

Nous avons équivalence entre les énoncés suivants :

- q divise a
- $a_1 \neq 0$
- $na_1 \neq 0$ (parce que $n \neq 0$)
- q divise a^n .

□

Lemme 3.20 ([1]).

Dans $\mathbb{N}$, le pgcd² et le ppcm sont uniques.

Démonstration. Supposons que δ_1 et δ_2 soient des pgcd de la partie S . Vu que $\delta_1 \mid S$, nous avons $\delta_1 \mid \delta_2$ parce que δ_2 est un pgcd. Le même raisonnement, inversant δ_1 et δ_2 montre que $\delta_2 \mid \delta_1$. Si (a_p) sont les éléments de la décomposition de δ_1 et (b_p) ceux de δ_2 , alors le lemme 3.17 nous indique que $a_p \leq b_p$ et $b_p \leq a_p$, ce qui implique que $a_p = b_p$.

Le ppcm se fait de même.

□

Lemme 3.21 ([1]).

Soient $a, b \in \mathbb{Z}$ et $k \in \mathbb{N}$ tels que $ab = q^k$ et $\text{pgcd}(a, b) = 1$. Alors il existe $\alpha, \beta \in \mathbb{Z}$ tels que $a = \alpha^k$ et $b = \beta^k$.

Démonstration. Nous décomposons a, b et q en facteurs premiers suivant le théorème 3.16 :

$$a = \prod_i p_i^{a_i} \quad (3.26a)$$

$$b = \prod_i p_i^{b_i} \quad (3.26b)$$

$$q = \prod_i p_i^{q_i}. \quad (3.26c)$$

En utilisant l'hypothèse :

$$ab = \prod_i p_i^{a_i+b_i} = \left(\prod_i p_i^{q_i} \right)^k = \prod_i p_i^{kq_i}. \quad (3.27)$$

En vertu de l'unicité de la décomposition en facteurs premiers, pour chaque i nous avons

$$a_i + b_i = kq_i. \quad (3.28)$$

Vu que a et b sont premiers entre eux, si $a_i \neq 0$ alors $b_i = 0$ et inversement. Prenons un i tel que $a_i \neq 0$. Alors $b_i = 0$ et nous avons $a_i = kq_i$. Idem pour les b_i .

Donc tous les a_i et les b_i qui sont non nuls sont des multiples de k . Nous posons $a_i = ks_i$ et nous reportons dans (3.26a) :

$$a = \prod_i p_i^{ks_i} = \left(\prod_i p_i^{s_i} \right)^k, \quad (3.29)$$

de telle sorte que a soit une puissance k^e . La même chose tient pour b .

□

Proposition 3.22.

Soient $a, b \in \mathbb{Z} \setminus \{0\}$ décomposés en $a = \prod_{p \in \mathcal{P}} p^{a_p}$ et $b = \prod_{p \in \mathcal{P}} p^{b_p}$. En posant

$$m_p = \min\{a_p, b_p\} \quad (3.30a)$$

$$M_p = \max\{a_p, b_p\}, \quad (3.30b)$$

nous avons

$$\text{pgcd}(a, b) = \prod_{p \in \mathcal{P}} p^{m_p} \quad (3.31a)$$

$$\text{ppcm}(a, b) = \prod_{p \in \mathcal{P}} p^{M_p}. \quad (3.31b)$$

2. Le pgcd et ppcm sont définis dans 1.169.

Démonstration. Nous notons $\delta = \prod_{p \in \mathcal{P}} p^{m_p}$ et $\mu = \prod_{p \in \mathcal{P}} p^{M_p}$.

Nous commençons par montrer que δ est le pgcd de a et b . Vu que $\delta_p = \min\{a_p, b_p\}$, nous avons $\delta_p \leq a_p$ et $\delta_p \leq b_p$. Le lemme 3.17 nous dit alors que $\delta \mid a$ et $\delta \mid b$. De même, si $s \mid a$ et $s \mid b$, nous avons $s_p \leq a_p$ et $s_p \leq b_p$, ce qui montre que $s_p \leq m_p$ et donc que $s \mid \delta$.

Le fait que μ soit le ppcm de a et b se montre de même. $\square$

Corolaire 3.23 ([1]).

Un élément $m \in \mathbb{Z}^*$ vérifie $m \leq p^n$ et $\text{pgcd}(m, p^n) \neq 1$ si et seulement si $m = qp$ pour un certain $q \leq p^{n-1}$.

ii Avertissement/question à la lectrice !! 3.24

Il faut vérifier si le corolaire 3.23 est correct. Et puis rédiger des démonstrations de tout ce petit monde.

Lemme 3.25.

Un entier $n \geq 1$ se décompose de façon unique en produit de la forme $n = qm^2$ où q est un entier sans facteurs carrés et m , un entier.

Démonstration. Pour $n = 1$, c'est évident. Nous supposons $n \geq 2$.

En ce qui concerne l'existence, nous décomposons n en facteurs premiers³ et nous séparons les puissances paires des puissances impaires :

$$n = \prod_{i=1}^r p_i^{2\alpha_i} \prod_{j=1}^s q_j^{2\beta_j+1} \quad (3.32a)$$

$$= \underbrace{\left(\prod_{i=1}^r p_i^{2\alpha_i} \prod_{j=1}^s q_j^{2\beta_j} \right)}_{m^2} \underbrace{\prod_{j=1}^s q_j}_{q}. \quad (3.32b)$$

Nous passons à l'unicité. Supposons que $n = q_1 m_1^2 = q_2 m_2^2$ avec q_1 et q_2 sans facteurs carrés (dans leur décomposition en facteurs premiers). Soit $d = \text{pgcd}(m_1, m_2)$ et k_1, k_2 définis par $m_1 = dk_1$, $m_2 = dk_2$. Par construction, $\text{pgcd}(k_1, k_2) = 1$. Étant donné que

$$n = q_1 d^2 k_1^2 = q_2 d^2 k_2^2, \quad (3.33)$$

nous avons $q_1 k_1^2 = q_2 k_2^2$ et donc k_1^2 divise $q_2 k_2^2$. Mais k_1 et k_2 n'ont pas de facteurs premiers en commun, donc k_1^2 divise q_2 , ce qui n'est possible que si $k_1 = 1$ (parce que k_1^2 n'a que des facteurs premiers alors que q_2 n'en a pas). Dans ce cas, $d = m_1$ et m_1 divise m_2 . Si $m_2 = lm_1$ alors l'équation (3.33) se réduit à $n = q_1 m_1^2 = q_2 l^2 m_1^2$ et donc

$$q_1 = q_2 l^2, \quad (3.34)$$

ce qui signifie $l = 1$ et donc $m_1 = m_2$. $\square$

Les nombres premiers ne sont pas si rares que ça dans $\mathbb{N}$. Nous allons voir dans 15.103 que la somme des inverses des nombres premiers diverge. Pour comparaison, la somme des inverses des carrés converge par la proposition 11.127. Il y a donc, dans un certains sens, plus de nombres premiers que de carrés ; dans un autre sens, il y en a autant : une infinité dénombrable.

3.2.5 Ordre d'un élément dans un groupe fini

Il y a des informations en plus dans la partie sur les groupes monogènes, 5.2.

Théorème 3.26 (Théorème de Cauchy[75]).

Soit un groupe fini d'ordre n . Pour tout diviseur premier p de n , le groupe G possède au moins un élément d'ordre p .

3. Théorème 3.16.

Le lemme suivant indique que sous hypothèse de commutativité, l'ordre d'un élément est une notion multiplicative.

Lemme 3.27 ([76]).

Soit G un groupe et $a, b \in G$ tels que $ab = ba$ d'ordres respectivement r et s , deux nombres premiers entre eux. Alors l'élément ab est d'ordre rs .

Démonstration. Étant donné que $(ab)^{rs} = a^{rs}b^{rs} = 1$, l'ordre de ab divise rs . Et vu que r et s sont premiers entre eux, l'ordre de ab s'écrit sous la forme r_1s_1 avec $r_1 \mid r$ et $s_1 \mid s$. Nous avons

$$a^{r_1s_1}b^{r_1s_1} = (ab)^{r_1s_1} = 1, \quad (3.35)$$

que nous élevons à la puissance r_2 où r_2 est défini en posant $r = r_1r_2$:

$$a^{rs_1}b^{rs_1} = 1. \quad (3.36)$$

Et comme $a^{rs_1} = 1$, nous concluons que $b^{rs_1} = 1$. Donc $s \mid rs_1$. Par le lemme de Gauss 3.14, nous avons en fait $s \mid s_1$. Vu qu'on a aussi $s_1 \mid s$, nous avons $s = s_1$.

Le même type d'argument donne $r = r_1$, et finalement l'ordre de ab est $r_1s_1 = rs$. $\square$

Lemme 3.28 ([32]).

Un sous-groupe d'indice 2 est un sous-groupe normal.

Démonstration. Si H est un tel sous-groupe d'un groupe G , alors G possède exactement deux classes à gauche par rapport à H (théorème de Lagrange 2.35) et se partitionne donc en deux parties : $G = H \cup xH$ avec $x \notin H$. De même pour les classes à droite : $G = H \cup Hx$. Puisque la classe à droite Hx n'est pas H , on a $xH = Hx$, et H est normal dans G par la proposition 2.17. $\square$

Lemme 3.29 ([77]).

Soit H , un sous-groupe normal d'indice m de G . Alors pour tout $a \in G$ nous avons $a^m \in H$.

Démonstration. Par définition de l'indice, le groupe G/H est d'ordre m . Donc si $[a] \in G/H$, nous avons $[a]^m = [e]$, ce qui signifie $[a^m] = [e]$, ou encore $a^m \in H$. $\square$

Proposition 3.30 ([77]).

Soit un groupe fini G et H , un sous-groupe normal d'ordre n et d'indice m avec m et n premiers entre eux. Alors H est l'unique sous-groupe de G à être d'ordre n .

Démonstration. Soit H' un sous-groupe d'ordre n . Si $h \in H'$ alors $h^n = 1$ et $h^m \in H$ par le lemme 3.29. Étant donné que m et n sont premiers entre eux, par le théorème de Bézout 1.181, il existe $a, b \in \mathbb{Z}$ tels que

$$am + bn = 1. \quad (3.37)$$

Du coup $h = h^1 = (h^m)^a(h^n)^b$. En tenant compte du fait que $h^n = 1$ et $h^m \in H$, nous avons $h \in H$. Ce que nous venons de prouver est que $H' \subset H$ et donc que $H = H'$ parce que $|H'| = |H| = |G|/m$. $\square$

3.31.

Notons que cette proposition ne dit pas qu'il existe un sous-groupe d'ordre n et d'indice m . Il dit juste que s'il y en a un et s'il est normal, alors il n'y en a pas d'autres.

Lemme 3.32.

L'ensemble des ordres⁴ d'un groupe commutatif est stable par PPCM⁵.

Autrement dit, si $x \in G$ est d'ordre r et si $y \in G$ est d'ordre s , alors il existe un élément d'ordre $\text{ppcm}(r, s)$.

4. Définition 2.19.

5. Définition 1.169.

Démonstration. Soit $m = \text{ppcm}(r, s)$. Afin d'écrire m sous une forme pratique, nous considérons les décompositions en facteurs premiers de r et s :

$$r = \prod_{i=1}^k p_i^{\alpha_i} \quad (3.38a)$$

$$s = \prod_{i=1}^k p_i^{\beta_i} \quad (3.38b)$$

où $\{p_i\}_{i=1\dots k}$ est l'ensemble des nombres premiers arrivant dans les décompositions de r et de s . Si nous posons

$$r' = \prod_{\substack{i=1 \\ \alpha_i > \beta_i}}^k p_i^{\alpha_i} \quad (3.39a)$$

$$s' = \prod_{\substack{i=1 \\ \alpha_i \leq \beta_i}}^k p_i^{\beta_i}, \quad (3.39b)$$

alors $\text{ppcm}(r, s) = r's'$ et r' et s' sont premiers entre eux. L'élément $x^{r/r'}$ est d'ordre r' et l'élément $y^{s/s'}$ est d'ordre s' . Maintenant nous utilisons le fait que G soit commutatif et le lemme 3.27 pour conclure que l'ordre de $x^{r/r'}y^{s/s'}$ est $r's' = m$. $\square$

3.2.6 Écriture des fractions

Théorème 3.33.

Tout élément de $\mathbb{Q}^+$ s'écrit de façon unique comme quotient de deux entiers premiers entre eux.

Démonstration. En deux parties⁶

Unité Supposons avoir $\frac{a}{b} = \frac{c}{d}$ avec $\text{pgcd}(a, b) = \text{pgcd}(c, d) = 1$. Nous avons

$$ad = bc \quad (3.40)$$

donc

(1) a divise bc mais est premier avec b donc a divise c par le lemme de Gauss 3.14.

(2) c divise ad mais est premier avec d donc c divise a par le lemme de Gauss 3.14.

En conclusion a divise c et c divise a , ergo $a = c$. L'égalité $b = d$ est alors immédiate.

Existence Soit le quotient $\frac{a}{b}$. Nous avons

$$\frac{a}{b} = \frac{a/\text{pgcd}(a, b)}{b/\text{pgcd}(a, b)}, \quad (3.41)$$

qui est encore un quotient d'entiers parce que $\text{pgcd}(a, b)$ divise aussi bien a que b . Il faut montrer que les nombres $a/\text{pgcd}(a, b)$ et $b/\text{pgcd}(a, b)$ sont premiers entre eux. Pour cela nous supposons que k est un diviseur commun. En particulier, les nombres $a/k \text{pgcd}(a, b)$ et $b/k \text{pgcd}(a, b)$ sont des entiers, ce qui fait que $k \text{pgcd}(a, b)$ est un diviseur commun de a et b . Étant donné que $\text{pgcd}(a, b)$ est le plus grand tel diviseur, nous devons avoir $k \text{pgcd}(a, b) = \text{pgcd}(a, b)$ c'est-à-dire que $k = 1$. Donc les nombres $a/\text{pgcd}(a, b)$ et $b/\text{pgcd}(a, b)$ sont premiers entre eux. $\square$

Proposition 3.34.

Les entiers p et q sont premiers entre eux si et seulement si p^2 et q^2 sont premiers entre eux.

6. Définitions des pgcd et ppcm en 1.169.

Démonstration. Si p^2 et q^2 sont premiers entre eux, par le théorème de Bézout 1.181 il existe $a, b \in \mathbb{Z}$ tels que

$$ap^2 + bq^2 = 1 \quad (3.42)$$

Dans ce cas, $(ap)p + (bq)q = 1$, ce qui montre (par encore Bézout, mais l'autre sens) que p et q sont premiers entre eux.

Réciproquement, supposons que p et q ne sont pas premiers entre eux. Alors $\text{pgcd}(p, q) = k \neq 1$. L'entier k divise p et donc p^2 ; et l'entier k divise q et donc q^2 . Au final, k divise p^2 et q^2 , ce qui montre que p^2 et q^2 ne sont pas premiers entre eux. $\square$

Une des conséquences de ces résultats sera le fait que $\sqrt{n}$ est irrationnelle dès que n n'est pas un carré parfait, théorème 3.35.

Nous avons déjà vu dans la proposition 1.278 que $\sqrt{2}$ était irrationnel. En fait le théorème suivant va nous montrer que le nombre $\sqrt{n}$ est soit entier, soit irrationnel.

Théorème 3.35.

Soit $n \in \mathbb{N}$. Le nombre $\sqrt{n}$ est rationnel si et seulement si n est un carré parfait.

Démonstration. Supposons que $\sqrt{n}$ soit rationnel. Le théorème 3.33 nous donne $p, q \in \mathbb{N}$ premiers entre eux tels que $\sqrt{n} = p/q$. La proposition 3.34 nous enseigne de plus que p^2 et q^2 sont premiers entre eux. Nous avons

$$p^2 = nq^2. \quad (3.43)$$

Le nombre q est alors un diviseur commun de q^2 et de p . Donc $q = 1$ et $n = p^2$ est un carré parfait. $\square$

3.2.7 Équation diophantienne linéaire à deux inconnues

Soient a, b et c des entiers naturels donnés. Nous considérons l'équation

$$ax + by = c \quad (3.44)$$

à résoudre[78] pour $(x, y) \in \mathbb{N}^2$.

Si a ou b est nul, c'est facile; nous supposons donc que a et b sont tout deux non nuls. Nous commençons par simplifier l'équation en cherchant les diviseurs communs. Soit $d = \text{pgcd}(a, b)$ et notons $a = da'$, $b = db'$. Nous avons déjà l'équation

$$d(a'x + b'y) = c, \quad (3.45)$$

et donc si c n'est pas un multiple de d , il n'y a pas de solutions⁷. Si par contre c est un multiple de d alors nous écrivons $c = c'd$ et l'équation devient

$$a'x + b'y = c' \quad (3.46)$$

C'est maintenant que nous utilisons le théorème de Bézout 1.181 : vu que a' et b' sont premiers entre eux, nous avons la relation $a'u + b'v = 1$ pour certains⁸ nombres entiers u et v . Nous récrivons notre équation sous la forme $a'x + b'y = c'(a'u + b'v)$ et rassemblons les termes :

$$a'(x - c'u) = b'(c'v - y). \quad (3.47)$$

C'est-à-dire que si (x, y) est une solution, alors a' divise $b'(c'v - y)$. Mais comme a' et b' sont premiers entre eux, le nombre a' doit forcément⁹ diviser $c'v - y$. Disons $c'v - y = ka'$. Alors $a'(x - c'u) = b'ka'$ et donc

$$x = b'k + c'u. \quad (3.48)$$

7. Exemple : $8x + 2y = 9$. Le membre de gauche est certainement un nombre pair et il n'y a donc pas de solutions.

8. Nous avons décrit un algorithme pour les trouver en démontrant l'équation 3.20.

9. C'est Gauss 3.14 qui le dit, et vous savez que lorsque Gauss dit, c'est *forcément* vrai.

Nous trouvons alors une expression pour y en injectant cela dans $a'x + b'y = c'$ et en utilisant Bézout : $a'c'u = (1 - b'v)c'$. Au final nous avons prouvé que toutes les solutions sont de la forme

$$\begin{cases} x = b'k + c'u \\ y = vc' - a'k \end{cases} \quad (3.49a)$$

$$(3.49b)$$

avec $k \in \mathbb{Z}$. Si nous voulons réellement seulement des solutions dans $\mathbb{N}$ et non dans $\mathbb{Z}$, il faut seulement un peu restreindre les valeurs de k . Il en reste un nombre fini parce que l'équation pour x borne k vers le bas tandis que celle pour y borne k vers le haut.

Par ailleurs, il est très vite vérifié que tous les couples (x, y) de la forme (3.49) sont solutions.

Exemple 3.36.

Résoudre l'équation $2x + 6y = 52$.

Nous pouvons factoriser 2 dans le membre de gauche et simplifier alors toute l'équation par 2 :

$$x + 3y = 26. \quad (3.50)$$

Nous cherchons une relation de Bézout pour $u + 3v = 1$. Ce n'est heureusement pas très compliqué : $u = -5$, $v = 2$. Nous pouvons alors écrire

$$x + 3y = 26 \times (-5 + 3 \times 2), \quad (3.51)$$

et donc $x + 5 \times 26 = 3(y - 26 \times 6)$, et en posant $k = y - 26 \times 6$ nous avons

$$x = 3k - 130. \quad (3.52)$$

En injectant nous trouvons l'équation $3k - 130 + 3y = 26$ et donc

$$y = 52 - k. \quad (3.53)$$

△

3.2.8 Quotients

Nous écrivons $a \equiv b \pmod{p}$ essentiellement s'il existe $k \in \mathbb{Z}$ tel que $b + kp = a$. Plus généralement nous notons $[a]_p = \{a + kp \mid k \in \mathbb{Z}\}$ et l'écriture « $a \equiv b \pmod{p}$ » peut tout autant signifier $a \equiv [b]_p$ que $a \in [b]_p$. La différence entre les deux est subtile mais peut de temps en temps valoir son pesant d'or.

Proposition 3.37.

Soit $n \in \mathbb{N}$. Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est monogène. Si $n \neq 0$, il est cyclique d'ordre n .

Démonstration. Nous considérons la surjection canonique $\mu: \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$. Si $a \in \mathbb{Z}$, alors $\mu(a) = a\mu(1)$. Par conséquent $\mathbb{Z}/n\mathbb{Z} = \text{gr}(\mu(1))$ parce que tout groupe contenant $\mu(1)$ contient tous les multiples de $\mu(1)$, et par conséquent contient $\mu(\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$.

Soit $x \in \mathbb{Z}/n\mathbb{Z}$ et considérons x_0 , le plus petit naturel représentant x . Nous notons $x = [x_0]$. Le théorème de la division euclidienne 1.177 donne l'existence de q et r avec $0 \leq r < n$ et $q \geq 0$ tels que

$$x_0 = nq + r. \quad (3.54)$$

Nous avons $[x_0] = [r] = \mu(r)$ parce que $x_0 - r$ est un multiple de n . Nous avons donc $[x_0] \in \mu(\mathbb{N}_{n-1})$. Par conséquent

$$\mathbb{Z}/n\mathbb{Z} = \mu(\mathbb{Z}) = \mu(\mathbb{N}_{n-1}). \quad (3.55)$$

La restriction $\mu: \mathbb{N}_{n-1} \rightarrow \mathbb{Z}/n\mathbb{Z}$ est donc surjective. Montrons qu'elle est également injective. Si $\mu(x_0) = \mu(x_1)$, alors $x_1 = x_0 + kn$. Si nous supposons que $x_1 > x_0$, alors $k > 0$ et si $x_0 \in \mathbb{N}_{n-1}$, alors $x_1 > n - 1$.

L'ordre de $\mathbb{Z}/n\mathbb{Z}$ est donc le même que le cardinal de $\mathbb{N}_{n-1}$, c'est-à-dire n . Le groupe $\mathbb{Z}/n\mathbb{Z}$ est donc fini, d'ordre n et monogène parce que $\mathbb{Z}/n\mathbb{Z} = \text{gr}(\mu(1))$. Il est donc cyclique. □

Lemme 3.38 ([79]).

Soit $q \in \mathbb{N}$ avec $q \geq 2$. Soient $n, d \in \mathbb{N}$ tels que $q^d - 1 \mid q^n - 1$. Alors $d \mid n$.

Démonstration. Par le théorème de division euclidienne 1.177, il existe $a, b \in \mathbb{Z}$ tels que $n = ad + b$ avec $0 \leq b < d$. En remarquant que $q^d \in [1]_{q^d-1}$ nous avons

$$q^n = (q^d)^a q^b \in [1]_{q^d-1} q^b = [q^b]_{q^d-1}. \quad (3.56)$$

Pour cela nous avons utilisé d'abord le fait que si $a \in [z]_k$, alors $a^n \in [z^n]_k$ et ensuite le fait que $[1]_k x = [x]_k$. D'autre part l'hypothèse $q^d - 1 \mid q^n - 1$ implique

$$q^n \in [1]_{q^d-1}. \quad (3.57)$$

Par conséquent le nombre q^n est à la fois dans $[q^b]_{q^d-1}$ et dans $[1]_{q^d-1}$. Cela implique que

$$[1]_{q^d-1} = [q^b]_{q^d-1}, \quad (3.58)$$

ou encore que $q^b \in [1]_{q^d-1}$ ou encore que $q^d - 1 \mid q^b - 1$.

Étant donné que $b < d$ et que $q \geq 2$, nous avons que $q^b - 1 < q^d - 1$; donc pour que $q^d - 1$ divise $q^b - 1$, il faut que $q^b - 1$ soit zéro, c'est-à-dire $b = 0$.

Mais dire $b = 0$ revient à dire que $d \mid n$, ce qu'il fallait démontrer. $\square$

3.3 Binôme de Newton et morphisme de Frobenius

Proposition 3.39 ([80]).

Pour tout $x, y \in \mathbb{R}$ et $n \in \mathbb{N}$, nous avons

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k \quad (3.59)$$

où

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \quad (3.60)$$

sont les **coefficients binomiaux**.

Démonstration. La preuve se fait par récurrence. La vérification pour $n = 0$ et $n = 1$ se fait aisément pour peu que l'on se rappelle que $x^0 = 1$ et que $0! = 1$, ce qui donne entre autres $\binom{0}{0} = 1$.

Supposons que la formule (3.59) soit vraie pour $n \geq 1$, et prouvons la pour $n + 1$. Nous avons

$$\begin{aligned} (x + y)^{n+1} &= (x + y) \cdot \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k \\ &= \sum_{k=0}^n \binom{n}{k} x^{n-k+1} y^k + \sum_{k=0}^n \binom{n}{k} x^{n-k} y^{k+1} \\ &= x^{n+1} + \sum_{k=1}^n \binom{n}{k} x^{n-k+1} y^k + \sum_{k=0}^{n-1} \binom{n}{k} x^{n-k} y^{k+1} + y^{n+1}. \end{aligned} \quad (3.61)$$

La seconde grande somme peut être transformée en posant $i = k + 1$:

$$\sum_{k=0}^{n-1} \binom{n}{k} x^{n-k} y^{k+1} = \sum_{i=1}^n \binom{n}{i-1} x^{n-(i-1)} y^{i-1+1}, \quad (3.62)$$

dans lequel nous pouvons immédiatement renommer i par k . En remplaçant dans la dernière expression de (3.61), nous trouvons

$$(x + y)^{n+1} = x^{n+1} + y^{n+1} + \sum_{k=1}^n \left[\binom{n}{k} + \binom{n}{k-1} \right] x^{n-k+1} y^k. \quad (3.63)$$

La thèse découle maintenant de la formule

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k} \quad (3.64)$$

qui est vraie parce que

$$\frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)(n-k+1)!} = \frac{n!(n-k+1) + n!k}{k!(n-k+1)!} = \frac{n!(n+1)}{k!(n-k+1)!}, \quad (3.65)$$

par simple mise au même dénominateur. $\square$

Tant que nous sommes à démontrer des égalités, en voici une.

Lemme 3.40 ([81]).

Pour $a, b \in \mathbb{R}$ et $n \in \mathbb{N}$ nous avons

$$a^n + (-1)^{n-1}b^n = (a+b) \sum_{k=0}^{n-1} (-1)^k a^{n-1-k} b^k. \quad (3.66)$$

Démonstration. C'est un simple calcul :

$$(a+b) \sum_{k=0}^{n-1} (-1)^k a^{n-1-k} b^k = \sum_{k=0}^{n-1} (-1)^k a^{n-k} b^k + \sum_{k=0}^{n-1} (-1)^k a^{n-k-1} b^{k+1} \quad (3.67a)$$

$$= a^n + \sum_{k=1}^{n-1} (-1)^k a^{n-k} b^k + \sum_{k=0}^{n-2} (-1)^k a^{n-k-1} b^{k+1} + (-1)^{n-1} b^n \quad (3.67b)$$

$$= a^n + (-1)^{n-1} b^n \quad (3.67c)$$

Justifications.

- Pour (3.67b). Dans la première somme, nous avons séparé le terme $k=0$ et dans la seconde nous avons séparé le terme $k=n-1$
- Pour (3.67c). Dans la seconde somme, décaler les termes pour sommer de 1 à $n-1$ et remarquer que ce qu'on obtient annule la première somme. $\square$

Proposition 3.41.

Soit A un anneau commutatif de caractéristique première p . Alors $\sigma(x) = x^p$ est un automorphisme de l'anneau A . Nous avons la formule

$$(a+b)^p = a^p + b^p \quad (3.68)$$

pour tout $a, b \in A$.

Démonstration. Nous utilisons la formule du binôme de la proposition 3.39 et le fait que les coefficients binomiaux non extrêmes sont divisibles par p et donc nuls. $\square$

3.4 Idéal dans un anneau

La définition d'un idéal dans un anneau est la définition 1.167.

Définition 3.42 (Idéal engendré par un élément).

Si p est un élément d'un anneau A alors nous notons (p) l'idéal dans A **engendré** par p , c'est-à-dire pA .

Définition 3.43.

Un sous-ensemble $B \subset A$ d'un anneau est un **sous anneau** si

- (1) $1 \in B$
- (2) B est un sous-groupe pour l'addition
- (3) B est stable pour la multiplication.

Remarque 3.44.

Un idéal n'est pas toujours un anneau parce que l'identité pourrait manquer. Un idéal qui contient l'identité est l'anneau complet.

Exemple 3.45.

L'ensemble $2\mathbb{Z}$ est un idéal de $\mathbb{Z}$. On peut aussi le noter (2). $\triangle$

Proposition 3.46 (Premier théorème d'isomorphisme pour les anneaux).

Soient A et B des anneaux et un homomorphisme $f: A \rightarrow B$. Nous considérons l'injection canonique $j: f(A) \rightarrow B$ et la surjection canonique $\phi: A \rightarrow A/\ker f$. Alors il existe un unique isomorphisme

$$\tilde{f}: A/\ker f \rightarrow f(A) \quad (3.69)$$

tel que $f = j \circ \tilde{f} \circ \phi$.

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \phi \downarrow & & \downarrow j \\ A/\ker f & \xrightarrow{\tilde{f}} & f(A) \subset B \end{array} \quad (3.70)$$

Proposition 3.47.

Soient I un idéal de A et la projection canonique

$$\phi: A \rightarrow A/I. \quad (3.71)$$

Elle est une bijection entre les idéaux de A contenant I et les idéaux de A/I .

Dit de façon imagée :

$$\{\text{idéaux de } A \text{ contenant } I\} \simeq \{\text{idéaux de } A/I\}. \quad (3.72)$$

Démonstration. Si $I \subset J$ et si J est un idéal de A , alors $\phi(J)$ est un idéal dans A/I . En effet un élément de $\phi(J)$ est de la forme $\phi(j)$ et un élément de A/I est de la forme $\phi(i)$. Leur produit vaut

$$\phi(i)\phi(j) = \phi(ij) \in \phi(J). \quad (3.73)$$

Soit maintenant K un idéal dans A/I et soit $J = \phi^{-1}(K)$. Étant donné qu'un idéal doit contenir 0 (parce qu'un idéal est un groupe pour l'addition), $[0] \in K$ et par conséquent $I \subset \phi^{-1}(K)$. $\square$

Proposition 3.48 ([1]).

Si A est un anneau, nous avons les équivalences

- (1) A est un corps¹⁰.
- (2) A est non nul et ses seuls¹¹ idéaux à gauche sont $\{0\}$ et A .
- (3) A est non nul et ses seuls idéaux à droite sont $\{0\}$ et A .

Démonstration. Nous allons montrer que le point (1) est équivalent aux deux autres.

(3) implique (2) Si I est un idéal à gauche différent de $\{0\}$, alors il contient un certain $a \neq 0$.

Vu que A est un corps, il contient un inverse a^{-1} , et comme I est un idéal, $a^{-1}I \subset I$. En particulier $a^{-1}a \in I$. Donc $1 \in I$ et $I = A$.

10. Définition 1.190.

11. Je vous laisse vous poser de grandes questions sur le fait que le vide est un idéal ou non.

(2) implique (1) Supposons que les seuls idéaux de A soient $\{0\}$ et A . Soit $a \in A$. Si a est non nul, alors $aA = A$, en particulier, $1 \in aA$, c'est-à-dire qu'il existe $b \in A$ tel que $ab = 1$. L'élément a est donc inversible. □

Définition 3.49.

Un idéal I dans un anneau A est dit **idéal maximal** ou **idéal maximum** si tout idéal J vérifiant $I \subset J \subset A$ est soit I , soit A .

Proposition 3.50 (Thème 49).

Un idéal I dans un anneau A est maximum si et seulement si A/I est un corps.

Démonstration. Soit un idéal maximum $I \subset A$. Alors les idéaux contenant I sont A et I . L'application ϕ de la proposition 3.47 est une bijection, donc l'ensemble des idéaux de A/I ne contient que deux éléments. Les seuls idéaux de A/I sont donc $\{0\}$ et A/I ; donc A/I est un corps par la proposition 3.48.

Dans l'autre sens, c'est la même chose : si A/I est un corps, il possède exactement deux idéaux, donc A ne contient que deux idéaux contenant I . Donc I est un idéal maximum. □

3.5 Polynômes de plusieurs variables

Définition 3.51.

L'ensemble des **polynôme de n variables** sur l'anneau A est $A^{(\mathbb{N}^n)}$, c'est-à-dire l'ensemble des suites indexées par $\mathbb{N}^n$ et dont seulement une quantité finie de coefficients sont non nuls.

Le produit sur $A[X_1, \dots, X_n]$ est défini par

$$(PQ)(k_1, \dots, k_n) = \sum_{\substack{(l_1, \dots, l_n), (m_1, \dots, m_n) \in \mathbb{N}^n \times \mathbb{N}^n \\ l_i + m_i = k_i}} P_{l_1, \dots, l_n} Q_{m_1, \dots, m_n}. \quad (3.74)$$

3.52.

Dans $A[X_1, \dots, X_n]$, la multiplication n'est pas la multiplication de fonctions $\mathbb{N}^n \rightarrow \mathbb{K}$, parce que le but est d'obtenir la multiplication usuelle au niveau des évaluations.

Définition 3.53.

Si P est un polynôme de n variables sur A , et si $(x_1, \dots, x_n) \in A^n$, **l'évaluation** de P sur $(x_1, \dots, x_n)$ est

$$P(x_1, \dots, x_n) = \sum_{(k_1, \dots, k_n) \in \mathbb{N}^n} P_{k_1, \dots, k_n} x_1^{k_1} \dots x_n^{k_n}. \quad (3.75)$$

Notez que la somme, bien que sur $\mathbb{N}^n$, est une somme finie.

3.54.

Comme dans le cas des polynômes d'une seule variable, les X_i dans la notation $A[X_1, \dots, X_n]$ sont à prendre à la légère. L'anneau des polynômes de n variables sur A aurait mieux fait d'être noté par exemple par $\mathcal{P}_n(A)$.

Le fait est que nous avons les polynômes élémentaires définis par

$$X_1(k_1, \dots, k_n) = \begin{cases} 1 & \text{si } (k_1, \dots, k_n) = (1, 0, \dots, 0) \\ 0 & \text{sinon.} \end{cases} \quad (3.76)$$

et que l'anneau des polynômes peut être vu comme A (les polynômes constants) étendus par les X_i .

Quoi qu'il en soit, les X_i dans la notation $A[X_1, \dots, X_n]$ sont des indices muets. L'anneau $A[X_1, \dots, X_n]$ est exactement le même que $A[T_1, \dots, T_n]$.

3.5.1 Divisibilité et classes d'association

Lemme 3.55.

Si A est un anneau intègre et si $a, b \in A$ sont tels que $a \mid b$ et $b \mid a$, alors il existe un inversible $u \in A$ tel que $a = ub$.

Démonstration. Les hypothèses à propos de la divisibilité nous indiquent que $a = xb$ et $b = ya$ pour certains $x, y \in A$. Du coup,

$$b(1 - yx) = 0. \quad (3.77)$$

Étant donné que A est intègre, cela montre que $b = 0$ ou $1 - yx = 0$. Si $b = 0$ nous avons immédiatement $a = 0$ et le lemme est prouvé. Si au contraire $yx = 1$, c'est que y et x sont inversibles et inverses l'un de l'autre. $\square$

Définition 3.56.

On dit de deux éléments $a, b \in A$ qu'ils sont **associés** si ils vérifient les hypothèses du lemme 3.55; en d'autres termes, a et b sont associés s'il existe un inversible $u \in A$ tel que $a = ub$.

La **classe d'association** d'un élément $a \in A$ est l'ensemble des éléments qui lui sont associés; en d'autres termes, c'est $aU(A)$.

Exemple 3.57.

Dans $\mathbb{Z}[i]$, les inversibles sont ± 1 et $\pm i$. Donc les éléments associés à z sont $z, -z, iz$ et $-iz$.

Notons au passage que la notion de divisibilité dans $\mathbb{Z}[i]$ n'est pas immédiatement intuitive. En effet bien que 7 ne soit pas divisible par 2 (ni dans $\mathbb{Z}$ ni dans $\mathbb{Z}[i]$), le nombre $7 + 6i$ est divisible par $2 + i$ dans $\mathbb{Z}[i]$. En effet :

$$(2 + i)(4 + i) = 7 + 6i. \quad (3.78)$$

$\triangle$

Exemple 3.58.

Si $\mathbb{K}$ est un corps, l'élément XY de $\mathbb{K}[X, Y]$ n'est pas premier parce que $XY \mid X^2Y^2$ alors que XY ne divise ni X^2 ni Y^2 . $\triangle$

!! Avertissement/question à la lectrice !! 3.59

Est-ce que quelqu'un connaît un anneau contenant $\mathbb{Z}$ dans lequel 7 est divisible en 2 ?

Peut-être $\mathbb{Z}$ étendu par tous les $1/2^n$?

3.5.2 PGCD et PPCM

Pour le théorème de Bézout et autres opérations avec des modulo, voir le thème 53. Le pgcd et le ppcm sont définis en 1.169.

Lemme 3.60.

Soient A un anneau intègre et $S \subset A$. Si δ est un PGCD de S , alors l'ensemble des PGCD de S est la classe d'association de δ .

De la même façon si μ est un PPCM de S , alors l'ensemble des PPCM de S est la classe d'association de μ .

Démonstration. Soient δ un PGCD de S et u un inversible dans A . Si $x \in S$ nous avons $\delta \mid x$ et donc $x = a\delta$. Par conséquent $x = au^{-1}u\delta$ et donc $u\delta$ divise x . De la même manière, si d divise x pour tout $x \in S$, alors d divise δ et donc $\delta = ad$ et $u\delta = aud$, ce qui signifie que d divise $u\delta$.

Dans l'autre sens nous devons prouver que si δ' est un autre PGCD de S , alors il existe un inversible $u \in A$ tel que $\delta' = u\delta$. Vu que δ' divise x pour tout $x \in S$, nous avons $\delta' \mid \delta$, et symétriquement nous trouvons $\delta \mid \delta'$. Par conséquent (lemme 3.55), il existe un inversible u tel que $\delta = u\delta'$.

Le même type de raisonnement tient pour le PPCM. $\square$

Si δ est un PGCD de S , nous dirons *par abus de langage* que δ est le PGCD de S , gardant en tête qu'en réalité toute sa classe d'association est PGCD. Nous noterons aussi, toujours par abus que $\delta = \text{pgcd}(S)$.

Remarque 3.61.

La classe d'association d'un élément n'est pas toujours très grande. Les inversibles dans $\mathbb{Z}$ étant seulement ± 1 , nous pouvons obtenir l'unicité du PGCD et du PPCM en imposant qu'ils soient positifs.

Pour les polynômes, nous obtenons l'unicité en demandant que le PGCD soit unitaire.

Dans les cas pratiques, il y a donc en réalité peu d'ambiguïté à parler du PGCD ou du PPCM d'un ensemble.

3.5.3 Anneaux intègres et corps

Le fait d'être intègre pour un anneau n'assure pas le fait d'être un corps. Nous avons cependant ce résultat pour les anneaux finis.

Proposition 3.62.

Un anneau fini intègre est un corps.

Démonstration. Soit A un tel anneau. Soit $a \neq 0$. Les applications

$$l_a: x \rightarrow ax \quad (3.79a)$$

$$r_a: x \rightarrow xa \quad (3.79b)$$

sont injectives. En tant que applications injectives entre ensembles finis, elles sont surjectives. Il existe donc b et c tels que $1 = ba = ac$. Il se fait que b et c sont égaux parce que ¹²

$$b = b(ac) = (ba)c = c. \quad (3.80)$$

Par conséquent b est un inverse de a . □

Proposition 3.63.

Soit $n \in \mathbb{N}^*$. Les conditions suivantes sont équivalentes :

- (1) n est premier.
- (2) $\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre.
- (3) $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Démonstration. L'équivalence entre les deux premiers points est le contenu du corolaire 1.200. Le fait que $\mathbb{Z}/n\mathbb{Z}$ soit un corps lorsque $\mathbb{Z}/n\mathbb{Z}$ est intègre est la proposition 3.62. Le fait que $\mathbb{Z}/n\mathbb{Z}$ soit intègre lorsque $\mathbb{Z}/n\mathbb{Z}$ est un corps est une propriété générale des corps : ce sont en particulier des anneaux intègres (lemme 1.194). □

3.5.4 Élément irréductible

Définition 3.64 (Élément irréductible[82]).

*Un élément d'un anneau commutatif est **irréductible** si il n'est ni inversible, ni le produit de deux éléments non inversibles.*

3.65.

Nous allons voir dans la section 3.8 que le concept d'élément irréductible n'est vraiment utile que dans le cas des anneaux intègres.

12. Il faut être un peu souple avec les notations communément employées dans les ouvrages mathématiques, et que nous reprenons telles quelles. Dans l'équation qui suit, $b(ac)$ est le produit de b par l'élément ac , et non quelque chose comme le produit de b avec l'idéal (ac) par exemple.

Exemple 3.66.

Un corps n'a pas d'éléments irréductibles parce qu'à part zéro tous les éléments sont inversibles. Mais 0 n'est pas irréductible parce qu'il peut être écrit comme produit d'éléments non inversibles : $0 = 0 \cdot 0$. $\triangle$

Exemple 3.67.

Les éléments irréductibles de l'anneau $\mathbb{Z}$ sont les nombres premiers. En effet les seuls inversibles de $\mathbb{Z}$ sont ± 1 . Si p est premier et $p = ab$ avec $a, b \in \mathbb{Z}$, alors nous avons soit $a = \pm 1$ soit $b = \pm 1$. $\triangle$

3.6 Anneau factoriel

Définition 3.68 (Anneau factoriel).

Un anneau commutatif A est **factoriel** s'il vérifie les propriétés suivantes.

- (1) L'anneau A est intègre (pas de diviseurs de zéro).
- (2) Si $a \in A$ est non nul et non inversible, alors il admet une décomposition en facteurs irréductibles : $a = p_1 \dots p_k$ où les p_i sont irréductibles.
- (3) Si $a = q_1 \dots q_m$ est une autre décomposition de a en irréductibles, alors $m = k$ et il existe une permutation¹³ $\sigma \in S_k$ telle que p_i et $q_{\sigma(i)}$ soient associés¹⁴.

Un anneau factoriel permet de caractériser le pgcd et le ppcm de nombres.

Proposition 3.69.

Soit une famille $\{a_n\}$ d'éléments de A qui se décomposent en irréductibles comme

$$a_i = \prod_k p_k^{\alpha_{k,i}}. \quad (3.81)$$

Alors

$$\text{pgcd}\{a_n\} = \prod_k p_k^{\min_i \{\alpha_{k,i}\}}. \quad (3.82)$$

De plus le PGCD est :

- (1) Un multiple de tous les diviseurs communs des a_i .
- (2) Unique pour cette propriété à multiple près par un inversible¹⁵.

De la même manière,

$$\text{ppcm}\{a_n\} = \prod_k p_k^{\max_i \{\alpha_{k,i}\}}. \quad (3.83)$$

Un anneau factoriel a une relation de préordre partiel donnée par $a < b$ si a divise b . En termes d'idéaux, cela donne l'ordre inverse de celui de l'inclusion¹⁶ : $a < b$ si et seulement si $(b) \subset (a)$.

Exemple 3.70.

L'anneau $\mathbb{Z}[i\sqrt{3}]$ n'est pas factoriel parce que 4 a au moins deux décompositions distinctes en irréductibles :

$$4 = 2 \cdot 2, \quad (3.84)$$

et

$$4 = (1 + i\sqrt{3})(1 - i\sqrt{3}). \quad (3.85)$$

$\triangle$

Nous allons voir dans l'exemple 3.105 que $\mathbb{Z}[i\sqrt{2}]$ est factoriel parce qu'il sera euclidien.

13. Définition 1.146.

14. Définition 3.56.

15. Soyez prudent avec cette affirmation : je n'en n'ai pas de démonstrations sous la main et ne suis pas certain que ce soit vrai.

16. Voir proposition 3.3.

3.7 Anneau principal et idéal premier

Définition 3.71.

Un idéal I dans A est **principal à gauche** s'il existe $a \in I$ tel que $I = Aa$. Il est **principal à droite** s'il existe $a \in I$ tel que $I = aA$. Nous disons qu'il est **principal** s'il est principal à gauche et à droite.

Définition 3.72.

Un anneau est **principal** si

- (1) il est commutatif et intègre
- (2) tous ses idéaux sont principaux.

Souvent pour prouver qu'un anneau est principal, nous prouvons qu'il est euclidien (définition 3.100) et nous utilisons la proposition 3.102 qui dit qu'un anneau euclidien est principal.

Une manière de prouver qu'un anneau n'est pas principal est de prouver qu'il n'est pas factoriel, théorème 3.93.

Définition 3.73.

Nous disons qu'un idéal I dans A est **premier** si I est strictement inclus dans A et si pour tout $a, b \in A$ tels que $ab \in I$ nous avons $a \in I$ ou $b \in I$.

Lemme 3.74.

L'idéal nul (réduit à $\{0\}$) est premier si et seulement si A est intègre.

Démonstration. En deux sens.

Si $\{0\}$ est premier Alors $A \neq \{0\}$ parce que $I = \{0\}$ est propre (définition d'idéal premier).

De plus, si $ab = 0$, alors $ab \in I$ qui est un idéal premier. Donc soit a soit b est dans I , c'est-à-dire que soit a soit b est nul. Donc A est intègre.

Si A est intègre Alors $A \neq \{0\}$ et l'idéal $I = \{0\}$ est strictement inclus dans A . Si $ab \in I$, alors $ab = 0$ et comme A est intègre, soit a soit b est nul, c'est-à-dire appartient à I . □

Proposition 3.75 ([67]).

Soit un anneau commutatif¹⁷ et un idéal I dans A .

- (1) I est un idéal premier si et seulement si A/I est un anneau intègre.
- (2) I est un idéal maximal si et seulement si A/I est un corps.
- (3) Tout idéal maximal propre est premier.

Démonstration. En plein d'étapes.

I premier implique A/I intègre Évacuons le cas trivial pour être sûr. Si $I = \{0\}$ alors A est intègre par le lemme 3.74. Donc $A/I = A/\{0\} = A$ est intègre également.

Soient $a, b \in A$ tels que $[a][b] = [0]$. Donc $[ab] = [0]$, c'est-à-dire $ab \in I$. Vu que I est un idéal premier nous avons $a \in I$ ou $b \in I$, c'est-à-dire $[a] = 0$ ou $[b] = 0$; nous en déduisons que A/I est un anneau intègre.

A/I intègre implique I premier Soit $ab \in I$. Alors $[ab] = 0$, ce qui signifie que $[a][b] = 0$ donc que $[a] = 0$ ou que $[b] = 0$ parce que A/I est intègre. Mais la condition $[a] = 0$ signifie $a \in I$, et $[b] = 0$ signifie $b \in I$. Nous avons donc prouvé que soit a soit b est dans I , c'est-à-dire que I est premier.

Si I est un idéal maximum Nous devons montrer que tout élément non nul de A/I est inversible. Un élément non nul de A/I est $[x]$ avec $x \in A \setminus I$.

Nous considérons $J = Ax + I$, qui est un idéal parce que pour tout $a \in A$, $aAx + aI \in Ax + I$. Mais comme I est maximal, $J = I$ ou $J = A$.

17. Tous les anneaux du Frido sont commutatifs

Si $J = I$, nous aurions que pour tout $a \in A$ et pour tout $i \in I$, $ax + i \in I$. En particulier pour $a = 1$ et $i = 0$ nous aurions $x \in I$, ce qui est contraire à l'hypothèse faite sur x .

Donc $J = A$. En particulier, $1 \in J$, c'est-à-dire qu'il existe $a \in A$ et $i \in I$ tels que $ax + i = 1$. En passant aux classes, $[ax] = 1$, c'est-à-dire $[a][x] = 1$ qui signifie que $[a]$ est un inverse de $[x]$ dans A/I .

Si A/I est un corps Si $x \in A \setminus I$, il faut prouver que tout idéal contenant I et x est A .

Un idéal contenant I et x doit contenir l'idéal $J = Ax + I$. Vu que $x \notin I$, nous avons $[x] \neq 0$ dans A/I . Donc $[x]$ est inversible et il existe $a \in A$ tel que $[ax] = [1]$. C'est-à-dire que $ax - 1 \in I$. Nous avons alors

$$1 = ax + \underbrace{(1 - ax)}_{\in I}. \quad (3.86)$$

C'est-à-dire que $1 \in Ax + I$ et donc $Ax + I = A$.

Enfin nous prouvons que tout idéal maximal propre est premier.

Si I est maximal, A/I est un corps par le point (2), et vu que I est propre, le corps A/I n'est pas réduit à $\{0\}$. Donc le lemme 1.194 dit que A/I est un anneau intègre. Le point (1) dit alors que I est un idéal premier. $\square$

Remarque 3.76.

Vu qu'un corps peut être réduit à $\{0\}$, dans (2), l'idéal peut être A . Mais pas dans (3), parce qu'un idéal premier est propre, ça fait partie de la définition 3.73.

Proposition 3.77 ([83]).

Si A est un anneau commutatif intègre, alors un idéal I dans A est premier si et seulement si A/I est intègre.

Démonstration. Supposons que I soit un idéal premier. Si $\bar{a}, \bar{b} \in A/I$ sont tels que $\bar{a}\bar{b} = 0$, alors $\overline{ab} = 0$, ce qui signifie que $ab \in I$. Mais alors, vu que I est premier, soit a soit b est dans I . Cela signifie que soit $\bar{a}$ soit $\bar{b}$ est nul dans A/I . Cela prouve que A/I est un anneau intègre.

Dans l'autre sens, nous supposons que A/I est intègre. Cela implique immédiatement que $I \neq A$ parce que A/A n'est pas un anneau intègre (tout le monde est évidemment diviseur de zéro).

Soient donc $a, b \in A$ tels que $ab \in I$. Alors $\overline{ab} = \bar{a}\bar{b} = 0$ dans A/I , mais comme A/I est intègre, cela implique que soit $\bar{a}$ soit $\bar{b}$ est nul. Autrement dit, soit a soit b est dans I . $\square$

Proposition 3.78 (Thème 49, [1]).

Soit A un anneau principal¹⁸ qui n'est pas un corps. Pour un idéal propre I de A , les conditions suivantes sont équivalentes :

- (1) I est un idéal maximal¹⁹ ;
- (2) I est un idéal premier non nul²⁰ ;
- (3) il existe p irréductible²¹ dans A tel que $I = (p)$.

Démonstration. En plusieurs implications.

(1) implique (2) Par hypothèse, I est un idéal propre, de plus il n'est pas égal à $\{0\}$, parce que lorsque A et $\{0\}$ sont les seuls idéaux, nous avons un corps (proposition 3.48). Étant donné que I est un idéal maximal, le quotient A/I est un corps par la proposition 3.50.

Soient maintenant, pour entrer dans le vif du sujet, des éléments $a, b \in A$ tels que $ab \in I$. Dans le corps A/I nous avons $\bar{a}\bar{b} = 0$, et par définition du produit dans le quotient, $\overline{ab} = 0$. Par intégrité de l'anneau A/I (un corps est un anneau intègre, lemme 1.197) nous avons soit $\bar{a} = 0$, soit $\bar{b} = 0$, soit les deux en même temps. Dans tous les cas, soit a soit b est dans I .

18. Définition 3.72.

19. Définition 3.49.

20. Définition 3.73.

21. Définition 3.64.

(2) implique (3) Maintenant I est un idéal premier non réduit à $\{0\}$. Vu que A est un anneau principal, il existe $x \in A$ tel que $I = (x)$. Nous devons prouver que x peut être choisi irréductible ; et nous allons faire plus : nous allons prouver que x ne peut être que irréductible ²².

Supposons que x ne soit pas irréductible. Alors il existe $a, b \in A$ non inversibles tels que $x = ab$. Si $a \in (x)$ alors il existe $k \in A$ tel que $a = xk$, et en particulier, $a = abk$, c'est-à-dire $1 = bk$ (parce que A est principal et donc intègre). Cela signifie que b est inversible alors que nous avions dit qu'il ne l'était pas. Nous en déduisons que a n'est pas dans (x) . On montre de manière similaire que b n'est pas dans (x) non plus.

Nous nous retrouvons donc avec $a, b \in A$ tel que $ab \in I$ sans que ni a ni b soient dans I . Cela contredit le fait que I soit un idéal premier. En conclusion, x est irréductible.

(3) implique (1) Nous avons $I = (p)$ avec p irréductible dans A . Supposons que J est un idéal différent de A contenant I . Vu que A est principal, il existe $y \in A$ tels que $J = (y)$. En particulier $p \in J$, donc $p = ay$ pour un certain $a \in A$. Mais p est irréductible, donc soit a est inversible, soit y est inversible. Si y est inversible, alors $J = A$, ce qui est exclu. Si a est inversible, alors $(y) = (p)$, et $I = J$.

□

3.79.

Dans la proposition 3.78, l'hypothèse d'idéal propre est importante. En effet dans le cas $I = A$, nous avons évidemment que I est un idéal maximum. Mais A n'est d'abord pas un idéal premier parce qu'un idéal premier doit être strictement inclus dans l'anneau. Et ensuite, A est en général loin d'être garanti d'être égal à (p) pour un de ses éléments p .

Proposition 3.80.

Soit A un anneau principal, et soit $p \in A$ un élément irréductible. Alors

- (1) (p) est un idéal maximum.
- (2) $A/(p)$ est un corps.

Démonstration. Nous notons $I = (p)$. Soit un idéal J contenant I . Vu que A est principal, J aussi est monogène : $J = (q)$. Mais comme p est dans I qui est dans J , il existe $a \in A$ tel que $p = qa$.

Vu que p est irréductible, soit q soit a est inversible. Si q est inversible, alors $J = A$. Si a est inversible, alors nous avons $p = qa$, donc $q = pa^{-1}$, ce qui signifie que $q \in (p)$ et donc que $J = I$.

Cela prouve que (p) est un idéal maximum.

Le fait que $A/(p)$ soit un corps est maintenant la proposition 3.50.

□

Exemple 3.81.

L'anneau $\mathbb{Z}$ est principal parce qu'il est intègre et que ses seuls idéaux sont les $n\mathbb{Z}$ qui sont principaux : $n\mathbb{Z}$ est engendré par n . △

Exemple 3.82 (Les idéaux de $\mathbb{Z}/n\mathbb{Z}$).

Les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont principaux, mais l'anneau $\mathbb{Z}/n\mathbb{Z}$ n'est pas principal lorsque n n'est pas premier. Nous allons voir ça.

Les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont principaux

Soit un idéal S dans $\mathbb{Z}/n\mathbb{Z}$. Nous considérons la projection canonique $\phi: \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$. La proposition 3.47 dit que $S = \phi(J)$ où J est un idéal de $\mathbb{Z}$ contenant $n\mathbb{Z}$. Mais le corolaire 1.188 nous dit qu'alors $J = m\mathbb{Z}$ pour un certain m . Pour que $m\mathbb{Z}$ contienne $n\mathbb{Z}$, il faut que m divise n .

Bref, $S = \phi(m\mathbb{Z})$ avec $m \mid n$. Nous montrons maintenant que S est engendré par $[m]_n$. D'abord, l'élément $[m]_n$ est bien dans $\phi(m\mathbb{Z})$. Ensuite un élément de $\phi(m\mathbb{Z})$ est de la forme

$$[km]_n = k[m]_n \in ([m]_n). \quad (3.87)$$

Donc $S \subset ([m]_n)$. Et l'inclusion dans l'autre sens est tout aussi immédiate : un élément de $([m]_n)$ est de la forme

$$k[m]_n = [km]_n = \phi(km) \in \phi(m\mathbb{Z}). \quad (3.88)$$

22. ça me semble un peu trop facile. Lisez attentivement, et écrivez-moi pour dire si vous êtes d'accord ou pas.

Si n n'est pas premier, $\mathbb{Z}/n\mathbb{Z}$ n'est pas principal Le fait est que lorsque n n'est pas premier, $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre (corolaire 1.200).

Moralité Un anneau comme $\mathbb{Z}/6\mathbb{Z}$ est un anneau dont tous les idéaux sont principaux, mais qui n'est pas principal.

△

Exemple 3.83.

Nous verrons dans la proposition 26.22 que l'anneau des fonctions holomorphes sur un compact de $\mathbb{C}$ est principal. △

Définition 3.84.

Nous disons que deux éléments d'un anneau principal sont **premiers entre eux** si leur PGCD est 1.

Théorème 3.85.

Si A est un anneau principal et si p et q sont premiers entre eux dans A , alors on a l'isomorphisme d'anneaux

$$A/pqA \simeq A/pA \times A/qA. \quad (3.89)$$

3.7.1 Bézout

Théorème 3.86 ([84]).

Toute partie S d'un anneau principal admet un PGCD et un PPCM. De plus

$$\delta = \text{pgcd}(S) \Leftrightarrow (\delta) = \sum_{s \in S} (s)\mu = \text{ppcm}(S) \Leftrightarrow (\mu) = \bigcap_{s \in S} (s) \quad (3.90)$$

Démonstration. Vu que l'anneau A est principal, tous ses idéaux sont principaux et donc engendrés par un seul élément. En particulier il existe $\delta, \mu \in A$ tels que

$$(\delta) = \sum_{s \in S} (s) \quad (3.91a)$$

$$(\mu) = \bigcap_{s \in S} (s) \quad (3.91b)$$

PGCD Montrons ce que δ est un PGCD de S . Pour tout $x \in S$, nous avons $(x) \subset (\delta)$, et donc $\delta \mid x$. Par ailleurs si $d \mid x$ pour tout $x \in S$, nous avons $(x) \subset (d)$ et donc

$$\sum_{x \in S} (x) \subset (d), \quad (3.92)$$

puis $(\delta) \subset (d)$ et finalement $d \mid \delta$.

PPCM Si $x \in S$ nous avons $(\mu) \subset (x)$ et donc $x \mid \mu$. D'autre part si $x \mid m$ pour tout $x \in S$, alors $(m) \subset (x)$ et donc $(m) \subset (\mu)$, finalement $\mu \mid m$.

□

Corolaire 3.87 (Théorème de Bézout[84]).

Soit un anneau principal A . Deux éléments $a, b \in A$ sont premiers entre eux si et seulement s'il existe un couple $(u, v) \in A^2$ tel que

$$ua + vb = 1. \quad (3.93)$$

À la place de 1 on aurait pu écrire n'importe quel inversible.

Démonstration. Pour cette preuve, nous allons écrire $\text{pgcd}(a, b)$ l'ensemble de PGCD de a et b , c'est-à-dire la classe d'association d'un PGCD.

Si a et b sont premiers entre eux, alors

$$1 \in \text{pgcd}(a, b) = \sum_{x=a, b} (x) = (a) + (b). \quad (3.94)$$

À l'inverse, si nous avons $ua + vb = 1$, alors $1 \in (a) + (b)$, mais vu que $(a) + (b)$ est un idéal principal, $(1) = (a) + (b)$ et donc $1 \in \text{pgcd}(a, b)$. $\square$

Le lemme de Gauss est une application immédiate de Bézout. Il y aura aussi un lemme de Gauss à propos de polynômes (lemme 6.47), et une généralisation directe au théorème de Gauss, théorème 6.46.

Lemme 3.88 (Lemme de Gauss[85]).

Soit A un anneau principal et $a, b, c \in A$ tels que a divise bc . Si a est premier avec c , alors a divise b .

Démonstration. Vu que a est premier avec c , nous avons $\text{pgcd}(a, c) = 1$ et Bézout (1.181) nous donne donc $s, t \in A$ tels que $sa + tc = 1$. En multipliant par b ,

$$sab + tbc = b. \quad (3.95)$$

Mais les deux termes du membre de gauche sont multiples de a parce que a divise bc . Par conséquent b est somme de deux multiples de a et donc est multiple de a . $\square$

Un cas usuel d'utilisation est le cas de $A = \mathbb{N}^*$.

3.7.2 Idéal premier

Proposition 3.89 ([86, 1], thème 55).

Soit un anneau principal A et un élément $p \neq 0$ dans A . Nous avons équivalence de :

- (1) (p) est un idéal premier,
- (2) p est un élément premier,
- (3) p est un élément irréductible,
- (4) (p) est un idéal maximum propre²³.

Démonstration. En plusieurs implications.

(1) implique (2) En plusieurs points.

- La condition $p \neq 0$ est dans les hypothèses de la proposition.
- Si p était inversible, nous aurions $(p) = A$ et donc pas que (p) est un idéal premier.
- Soient $a, b \in A$ tels que $p \mid ab$. En particulier, $(ab) \in (p)$. Mais comme (p) est un idéal premier, cela implique soit $a \in (p)$ soit $b \in (p)$. Donc soit p divise a soit p divise b .

(2) implique (3) Un anneau principal est intègre ; c'est dans la définition 3.72. Dans un anneau intègre, tout élément premier est irréductible, c'est la proposition 1.203.

(3) implique (4) Soit un idéal I contenant (p) . Vu que A est principal, I est engendré par un seul élément ; soit $I = (a)$. Vu que $p \in I$, l'élément a divise p . Mais comme p est un élément premier, $a \mid p$ implique $a = p$ ou $a = 1$. Dans le premier cas, $I = (a) = (p)$, et dans le second cas, $I = (a) = (1) = A$. Donc (p) est bien un idéal maximum.

De plus l'idéal (p) est propre. En effet avoir $(p) = A$ dirait en particulier que $1 \in (p)$, c'est-à-dire qu'il existe $x \in A$ tel que $xp = 1$. Or p étant irréductible, il est non inversible.

(4) implique (1) C'est la proposition 3.75(3).

23. Ce « propre » n'est pas dans l'énoncé sur Wikipédia. Je ne comprends pas pourquoi, et j'ai posé la question sur la page de discussion.

https://fr.wikipedia.org/wiki/Discussion:Idéal_premier

□

Un exemple d'élément premier non irréductible est $[4]_6$ dans l'anneau non principal $\mathbb{Z}/6\mathbb{Z}$. Voir 3.98 et le lemme 3.99.

3.7.3 Anneau noethérien

Définition 3.90.

Un anneau est dit **noethérien** si toute suite croissante d'idéaux est stationnaire (à partir d'un certain rang).

Montrer que tout anneau principal est noethérien est le premier pas pour montrer que tout anneau principal est factoriel.

Lemme 3.91.

Tout anneau principal²⁴ est noethérien.

Démonstration. Soit (J_n) une suite croissante d'idéaux et J la réunion. L'ensemble J est encore un idéal parce que les J_i sont emboîtés. Étant donné que l'idéal est principal nous pouvons prendre $a \in J$ tel que $J = (a)$. Il existe N tel que $a \in J_N$. Alors pour tout $n \geq N$ nous avons

$$J \subset J_N \subset J_n \subset J. \quad (3.96)$$

La première inclusion est le fait que $J = (a)$ et $a \in J_N$. La seconde est la croissance des idéaux et la troisième est le fait que J est une union. Par conséquent pour tout $n \geq N$ nous avons $J_N = J_n = J$. La suite est par conséquent stationnaire. □

Exemple 3.92.

Il y a moyen d'avoir un anneau noetherien non principal. C'est le cas de $\mathbb{Z}/6\mathbb{Z}$ dont nous parlerons dans 3.99. △

Théorème 3.93 ([87]).

Tout anneau principal est factoriel.

Exemple 3.94 ($\mathbb{Z}[i\sqrt{5}]$ n'est ni factoriel ni principal).

Vu que $(i\sqrt{5})^2 = -5$, les éléments de $\mathbb{Z}[i\sqrt{5}]$ sont les éléments de $\mathbb{C}$ de la forme $a + bi\sqrt{5}$ avec $a, b \in \mathbb{Z}$. Nous définissons la **norme** sur $\mathbb{Z}[i\sqrt{5}]$ par²⁵

$$N: \mathbb{Z}[i\sqrt{5}] \rightarrow \mathbb{N} \\ z \mapsto z\bar{z}. \quad (3.97)$$

Le fait que ce soit à valeurs dans $\mathbb{N}$ est un simple calcul :

$$N(x + iy\sqrt{5}) = (x + iy\sqrt{5})(x - iy\sqrt{5}) = x^2 + 5y^2. \quad (3.98)$$

De plus N est multiplicative : $N(z_1 z_2) = N(z_1)N(z_2)$.

Nous pouvons maintenant déterminer les inversibles de $\mathbb{Z}[i\sqrt{5}]$. Si α est inversible, alors il existe β tel que $\alpha\beta = 1$. Au niveau de la norme,

$$N(\alpha)N(\beta) = 1, \quad (3.99)$$

ce qui implique que $N(\alpha) = 1$. Or l'équation $x^2 + 5y^2 = 1$ dans $\mathbb{N}$ donne $y = 0$, $x = \pm 1$.

Au final, les inversibles de $\mathbb{Z}[i\sqrt{5}]$ sont ± 1 .

L'anneau $\mathbb{Z}[i\sqrt{5}]$ n'est alors pas factoriel (définition 3.68) parce que

$$2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}). \quad (3.100)$$

Cela donne deux décompositions du nombre 6 en produit d'éléments non associés²⁶ (2 n'est associé qu'à 2 et -2) parce que les inversibles sont 1 et -1 .

Le fait que $\mathbb{Z}[i\sqrt{5}]$ ne soit pas factoriel implique qu'il ne soit pas principal, théorème 3.93. △

24. Définition 3.72.

25. C'est le carré de la norme usuelle, mais c'est l'usage dans le milieu.

26. Définition 3.56.

3.8 Anneau $\mathbb{Z}/6\mathbb{Z}$

Nous allons donner quelques propriétés de cet anneau, et en particulier voir que dans cet anneau non intègre, la notion d'élément irréductible n'est pas très intéressante.

Voici pour commencer un calcul la table de multiplication de $A = \mathbb{Z}/6\mathbb{Z}$. Pour les multiples de (par exemple) $[4]_6$ nous écrivons

$$1 \times [4]_6 = [4]_6 \quad (3.101)$$

et ensuite

$$2 \times [4]_6 = [8]_6 = [2]_6, \quad (3.102)$$

puis

$$3 \times [4]_6 = [2 + 4]_6 = [6]_6 = [0]_6, \quad (3.103)$$

et caetera. Le résultat est :

$\times$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	0	0	0	0	0	0
$[1]_6$	0	1	2	3	4	5
$[2]_6$	0	2	4	0	2	4
$[3]_6$	0	3	0	3	0	3
$[4]_6$	0	4	2	0	4	2
$[5]_6$	0	5	4	3	2	1

(3.104)

Pour ne pas alourdir, nous n'avons pas écrit $[x]_6$ partout au lieu de x .

3.95 (Inversibles).

Les éléments inversibles de $\mathbb{Z}/6\mathbb{Z}$ sont ceux qui ont un $[1]_6$ dans leur table de multiplication. Ce sont donc

$$U(\mathbb{Z}/6\mathbb{Z}) = \{[1]_6, [5]_6\}. \quad (3.105)$$

3.96 (Diviseurs de zéro).

Les diviseurs de zéro sont ceux qui ont un $[0]_6$ dans leur table de multiplication, c'est-à-dire

$$\{[2]_6, [3]_6, [4]_6\}. \quad (3.106)$$

3.97 (Irréductibles).

Les irréductibles sont ceux qui ne sont ni inversibles ni produit de deux éléments non inversibles. Les non inversibles sont :

$$\{[0]_6, [2]_6, [3]_6, [4]_6\}. \quad (3.107)$$

Ils sont candidats à être irréductibles. Les produits de ces éléments (on oublie les crochets) sont :

$$2 \times 2 = 4 \quad (3.108a)$$

$$2 \times 3 = 0 \quad (3.108b)$$

$$2 \times 4 = 2 \quad (3.108c)$$

$$3 \times 3 = 3 \quad (3.108d)$$

$$3 \times 4 = 0 \quad (3.108e)$$

$$4 \times 4 = 4. \quad (3.108f)$$

Donc $[0]_6$, $[2]_6$, $[3]_6$ et $[4]_6$ ne sont plus candidats à être irréductible. Bref, il ne reste aucun candidats.

L'anneau $\mathbb{Z}/6\mathbb{Z}$ n'a aucun élément irréductible.

3.98 (Éléments premiers).

Les éléments non nuls et non inversibles sont 2, 3 et 4.

Pour 2 L'élément $[2]_6$ divise 2, 4 et 0.

- Les (a, b) tels que $ab = 2$ sont : $(1, 2)$, $(2, 4)$ et $(5, 4)$. L'élément 2 divise donc toujours a ou b .
- Les (a, b) tels que $ab = 4$ sont : $(1, 4)$, $(2, 5)$ et $(4, 4)$. L'élément 2 divise donc toujours a ou b .
- Les (a, b) tels que $ab = 0$ sont : $(0, x)$, $(3, 2)$ et $(4, 3)$. L'élément 2 divise donc toujours a ou b . En particulier, $[2]_6$ divise $[0]_6$; c'est important.

Donc $[2]_6$ est un élément premier.

Pour 3 L'élément $[3]_6$ divise 3 et 0.

- Les (a, b) tels que $ab = 3$ sont : $(1, 3)$ et $(3, 5)$. L'élément 3 divise donc toujours a ou b .
- Les (a, b) tels que $ab = 0$ sont : $(0, x)$, $(3, 2)$ et $(4, 3)$. L'élément 3 divise donc toujours a ou b .

Donc $[3]_6$ est un élément premier. L'élément $[4]_6$ divise 4, 2 et 0.

- Les (a, b) tels que $ab = 4$ sont : $(1, 4)$, $(2, 5)$ et $(4, 4)$. L'élément 4 divise donc toujours a ou b .
- Les (a, b) tels que $ab = 2$ sont : $(1, 2)$, $(2, 4)$ et $(5, 4)$. L'élément 4 divise donc toujours a ou b .
- Les (a, b) tels que $ab = 0$ sont : $(0, x)$, $(3, 2)$ et $(4, 3)$. L'élément 4 divise donc toujours a ou b .

Donc $[4]_6$ est un élément premier.

Au final, les éléments premiers dans $\mathbb{Z}/6\mathbb{Z}$ sont

$$\{[2]_6, [3]_6, [4]_6\}. \quad (3.109)$$

Vous noterez que $\mathbb{Z}/6\mathbb{Z}$ a des éléments premiers non irréductibles. Cela est un contre-exemple à la proposition 3.89 dans le cas d'un anneau non-intègre.

Lemme 3.99 ([1]).

L'anneau $\mathbb{Z}/6\mathbb{Z}$ est noetherien, mais ni intègre ni principal²⁷.

Démonstration. Vu que c'est un anneau fini, toute suite croissante de quoi que ce soit devient stationnaire ; donc $\mathbb{Z}/6\mathbb{Z}$ est noetherien.

Vu que $\mathbb{Z}/6\mathbb{Z}$ a des diviseurs de zéro, il n'est pas intègre. Et vu qu'il n'est pas intègre, il n'est pas factoriel non plus. $\square$

3.9 Anneau euclidien

Définition 3.100 (Wikipédia).

Soit A un anneau intègre. Un **stathme euclidien** sur A est une application $\alpha: A \setminus \{0\} \rightarrow \mathbb{N}$ tel que

(1) $\forall a, b \in A \setminus \{0\}$, il existe $q, r \in A$ tel que

$$a = qb + r \quad (3.110)$$

et $\alpha(r) < \alpha(b)$.

(2) Pour tout $a, b \in A \setminus \{0\}$, $\alpha(b) \leq \alpha(ab)$.

Un anneau est **euclidien** s'il accepte un stathme euclidien.

Le stathme est la fonction qui donne le « degré » à utiliser dans la division euclidienne. La contrainte est que le degré du reste soit plus petit que le degré du dividende.

27. Toutes les définitions dans le thème 55.

Exemple 3.101.

Le stathme de $\mathbb{N}$ pour la division euclidienne usuelle est $\alpha(n) = n$. Si $a, b \in \mathbb{N}$ nous écrivons

$$a = qb + r \quad (3.111)$$

où q est l'entier le plus proche *inférieur* à a/b (on veut que le reste soit positif) et $r = a - qb$. Nous avons donc

$$r - b = a - b(q + 1) < a - b\frac{a}{b} = 0, \quad (3.112)$$

ce qui montre que $r < b$. △

Cet exemple ne fonctionne pas avec $\mathbb{Z}$ au lieu de $\mathbb{N}$ parce que le stathme doit avoir des valeurs dans $\mathbb{N}$. Cela ne veut cependant pas dire qu'il n'existe pas de stathme sur $\mathbb{Z}$; cela veut seulement dire que $\alpha(x) = x$ ne fonctionne pas.

Proposition 3.102 ([88]).

Un anneau euclidien est principal.

Démonstration. Soit A un anneau principal et α un stathme sur A . Nous considérons un idéal I non nul de A . Nous devons montrer que I est généré par un élément. En l'occurrence nous allons montrer qu'un élément $a \in I \setminus \{0\}$ qui minimise $\alpha(a)$ va générer²⁸. Soit $x \in I$. Par construction, il existe $q, r \in A$ tels que $x = aq + r$ avec $r = 0$ ou $\alpha(r) < \alpha(a)$. Étant donné que $x, a \in I$, $r \in I$. Si $r \neq 0$, alors r contredirait la minimalité de $\alpha(a)$. Donc $r = 0$ et $x = aq$, ce qui signifie que I est principal. □

Proposition 3.103.

L'anneau $\mathbb{Z}$ est principal et euclidien.

Démonstration. Nous allons seulement montrer que $\alpha(x) = |x|$ est un stathme euclidien. Ainsi $\mathbb{Z}$ sera euclidien et donc principal par la proposition 3.102.

D'abord $\mathbb{Z}$ est intègre, c'est l'exemple 1.198.

La condition $\alpha(b) \leq \alpha(ab)$ est immédiate : $|a| \leq |ab|$ pour tout $a, b \in \mathbb{Z}$.

Soient maintenant $a, b \in \mathbb{Z}$. Nous définissons $q_0, r_0 \in \mathbb{N}$ tels que

$$|a| = q_0|b| + r_0 \quad (3.113)$$

avec $r_0 < |b|$. Cela existe parce que $\alpha(x) = x$ est un stathme sur $\mathbb{N}$ par l'exemple 3.101.

Si $a > 0$ et $b > 0$ Alors $a = q_0b + r_0$ et le couple (q_0, r_0) vérifie les conditions de la définition 3.100(1).

Si $a > 0$ et $b < 0$ Alors $a = -q_0b + r_0$, et le couple $(-q_0, r_0)$ vérifie les conditions de la définition 3.100(1).

Si $a < 0$ et $b > 0$ Alors $a = -q_0b - r_0$, et le couple $(-q_0, -r_0)$ vérifie les conditions de la définition 3.100(1) parce que

$$\alpha(-r_0) = r_0 < |b| = \alpha(b). \quad (3.114)$$

Si $a < 0$ et $b < 0$ Alors $a = q_0b - r_0$, et le couple $(q_0, -r_0)$ vérifie les conditions de la définition 3.100(1). □

Nous venons de voir que $\mathbb{Z}$ est principal; le lemme suivant nous dit que $\mathbb{Z}[X]$ n'est pas principal, lui.

Lemme 3.104 ([89]).

Si A est un anneau intègre²⁹ qui n'est pas un corps, alors $A[X]$ n'est pas principal.

28. Un tel élément existe...

29. Définition 1.174.

Démonstration. Soit un élément non nul $a \in A$.

Un idéal principal contenant a et X est $A[X]$ Soit (P) un idéal principal contenant a et X .

Vu que $a \in (P)$, il existe Q tel que $a = QP$. Donc P divise a dans $\mathbb{Z}[X]$. Les degrés font que P est un polynôme constant, c'est-à-dire en réalité un élément de A . Soit $P = k \in A$.

Vu que P divise X , nous avons aussi $X = kQ$ pour un certain $Q \in \mathbb{Z}[X]$. Les degrés disent qu'il existe $k' \in A$ tel que $Q = k'X$ et donc $X = k'kQ$, ce qui implique que $kk' = 1$.

L'idéal engendré par k contient donc en particulier $kk' = 1$ et donc contient $A[X]$ en entier :

$$1 = k'k \in k'(P) = (P). \quad (3.115)$$

Si $(a, X) = A[X]$ alors a est inversible Si $(a, X) = A[X]$, en particulier, $1 \in (a, X)$, ce qui signifie qu'il existe des polynômes $U, V \in A[X]$ tels que

$$1 = UX + Va. \quad (3.116)$$

Nous évaluons cette égalité en 0 : vu que $(UX)(0) = 0$ nous avons $1 = V(0)a$, ce qui signifie que $V(0)$ est un inverse de a . Donc a est inversible.

Si a n'est pas inversible alors (a, X) n'est pas principal Si (a, X) était principal, alors nous aurions, par ce qui est dit plus haut, $(a, X) = A[X]$. Mais cette dernière égalité impliquerait que a est inversible.

En conclusion, si A n'est pas un corps, il possède un élément ni nul ni inversible. Dans ce cas, l'idéal (a, X) n'est pas principal dans $A[X]$ et nous en déduisons que $A[X]$ n'est pas un anneau principal. $\square$

Nous verrons dans le lemme 3.127 que si $\mathbb{K}$ est un corps, alors $\mathbb{K}[X]$ est principal.

Exemple 3.105.

Prouvons que $\mathbb{Z}[i\sqrt{2}]$ est un anneau euclidien. Pour cela nous démontrons que

$$\begin{aligned} N: \mathbb{Z}[i\sqrt{2}] &\rightarrow \mathbb{N} \\ a + bi\sqrt{2} &\mapsto a^2 + 2b^2 \end{aligned} \quad (3.117)$$

est un stathme euclidien.

Soient $z = a + bi\sqrt{2}$, $t = a' + b'i\sqrt{2}$. Nous cherchons q et r tels que la division euclidienne s'écrive $z = qt + r$. Soient $\alpha, \beta \in \mathbb{Q}$ tels que

$$\frac{z}{t} = \alpha + \beta i\sqrt{2}. \quad (3.118)$$

Nous désignons par $\alpha + \epsilon_1$ et $\beta + \epsilon_2$ les entiers les plus proches de α et β . Nous avons $|\epsilon_1|, |\epsilon_2| \leq \frac{1}{2}$. Nous posons alors naturellement

$$q = (\alpha + \epsilon_1) + (\beta + \epsilon_2)i\sqrt{2} \quad (3.119)$$

et nous calculons $r = z - qt$:

$$2b'\epsilon_2 - a'\epsilon_1 + i\sqrt{2}(\epsilon_1b' - a'\epsilon_2). \quad (3.120)$$

Nous trouvons

$$N(r) = a'^2\epsilon_1^2 + 4b'^2\epsilon_2^2 + 2a'\epsilon_1\epsilon_2 + 2b'\epsilon_1\epsilon_2 \leq \frac{3}{4}a'^2 + \frac{3}{2}b'^2. \quad (3.121)$$

D'autre part $N(t) = a'^2 + 2b'^2$, et nous avons donc bien $N(r) < N(t)$.

En ce qui concerne la seconde propriété du stathme, un petit calcul montre que

$$N(z) = (a^2 + 2b^2)(a'^2 + 2b'^2), \quad (3.122)$$

et tant que $t \neq 0$ nous avons bien $N(z) > N(r)$. $\triangle$

Notons en particulier que $\mathbb{Z}[i\sqrt{2}]$ est factoriel et principal.

Exemple 3.106 (Décomposition en facteurs irréductibles dans $\mathbb{Z}[i\sqrt{2}]$).

Les éléments inversibles de $\mathbb{Z}[i\sqrt{2}]$ sont ± 1 , donc deux éléments a et b sont associés (définition 3.56) si et seulement si $a = \pm b$.

De plus si p est irréductible³⁰, alors $-p$ est irréductible. Les éléments irréductibles de $\mathbb{Z}[i\sqrt{2}]$ arrivent donc par paires d'éléments associés. Soit $\{p_i\}$ une sélection de un élément irréductible parmi chaque paire. Tout élément x de $\mathbb{Z}[i\sqrt{2}]$ peut alors être écrit $x = \pm p_1^{\alpha_1} \dots p_n^{\alpha_n}$. Ce fait va être pratique pour comparer des décompositions en facteurs irréductibles d'éléments. $\triangle$

Le lemme suivant fait en pratique partie de l'exemple 3.109, mais nous l'isolons pour plus de clarté³¹.

Lemme 3.107.

Si a et b sont deux éléments premiers entre eux de $\mathbb{Z}[i\sqrt{2}]$, et s'il existe $y \in \mathbb{Z}[i\sqrt{2}]$ tel que $ab = y^3$, alors a et b sont des cubes (dans $\mathbb{Z}[i\sqrt{2}]$).

Démonstration. D'après l'exemple 3.106 nous pouvons écrire

$$y = \pm p_1^{\sigma_1} \dots p_n^{\sigma_n} \quad (3.123a)$$

$$a = \pm p_1^{\alpha_1} \dots p_n^{\alpha_n} \quad (3.123b)$$

$$b = \pm p_1^{\beta_1} \dots p_n^{\beta_n} \quad (3.123c)$$

où les p_i sont les irréductibles de $\mathbb{Z}[i\sqrt{2}]$ « modulo ± 1 » au sens où la liste des irréductibles est $\{p_i\} \cup \{-p_i\}$ (union disjointe). Étant donné que a et b sont premiers entre eux, α_i et β_i ne peuvent pas être non nuls en même temps alors que leur somme doit faire $3\sigma_i$. Nous avons donc pour chaque i soit $\alpha_i = 3\sigma_i$ soit $\beta_i = 3\sigma_i$ (et bien entendu si $\sigma_i = 0$ alors $\alpha_i = \beta_i = 0$).

Étant donné que ± 1 sont également deux cubes, a et b sont bien des cubes.

Notons que nous avons utilisé de façon capitale le fait que $\mathbb{Z}[i\sqrt{2}]$ était factoriel. $\square$

3.9.1 Équations diophantiennes

Exemple 3.108.

L'équation diophantienne

$$x^2 = 3y^2 + 8 \quad (3.124)$$

n'a pas de solutions. En effet si nous prenons l'équation modulo 3 nous obtenons

$$[x^2]_3 = [3y^2 + 8]_3 = [8]_3 = [2]_3. \quad (3.125)$$

Or dans $\mathbb{Z}/3\mathbb{Z}$, aucun carré n'est égal à deux : $0^2 = 0 \neq 2$, $1^2 = 1 \neq 2$ et $2^2 = 4 = 1 \neq 2$. $\triangle$

Exemple 3.109.

Résolvons l'équation diophantienne

$$x^2 + 2 = y^3. \quad (3.126)$$

Une première remarque est que x doit être impair. En effet si $x = 2k$, nous devons avoir y^3 pair. Mais si un cube pair est divisible par 8, donc $y^3 = 8l$. L'équation devient $4k^2 + 2 = 8l^3$, c'est-à-dire $2k^2 + 1 = 4l^3$. Le membre de gauche est impair tandis que celui de droite est pair. Impossible.

Nous pouvons écrire l'équation sous la forme $x^2 + 2 = (x + i\sqrt{2})(x - i\sqrt{2})$. Et nous considérons $\mathbb{Z}[i\sqrt{2}]$ muni de son stathme N donné par (3.117).

L'élément $i\sqrt{2}$ est irréductible parce que $N(i\sqrt{2}) = 2$, et si nous avons $i\sqrt{2} = pq$, alors nous aurions $N(p)N(q) = 2$, ce qui n'est possible que si $N(p)$ ou $N(q)$ vaut 1.

30. Définition 3.64

31. Merci à [Marvoir](#) pour m'avoir souligné le manque.

Nous prouvons maintenant que les éléments $x + i\sqrt{2}$ et $x - i\sqrt{2}$ sont premiers entre eux. Supposons que d soit un diviseur commun ; alors il divise aussi la somme et la différence. Donc d divise à la fois $2x$ et $2i\sqrt{2}$.

Étant donné que $i\sqrt{2}$ est irréductible et que $2i\sqrt{2} = (-i\sqrt{2})^3$, les diviseurs de $2i\sqrt{2}$ sont les puissances de $(-i\sqrt{2})$. Du coup nous devrions avoir $d = (i\sqrt{2})^\beta$ et donc

$$x = (i\sqrt{2})^\beta q \quad (3.127)$$

pour un certain $q \in \mathbb{Z}[i\sqrt{2}]$. Dans ce cas nous avons $N(x) = 2^\beta N(q)$, mais nous avons déjà précisé que x ne pouvait pas être pair, donc $\beta = 0$ et nous avons $d = 1$.

Vu que les nombres $x \pm i\sqrt{2}$ sont premiers entre eux et que leur produit doit être un cube, ils doivent être séparément des cubes (lemme 3.107). Nous devons donc résoudre séparément $x \pm i\sqrt{2} = y^3$.

Cherchons les x et y entiers tels que $x + i\sqrt{2} = y^3$. Si nous posons $z = a + bi\sqrt{2}$, il suffit de calculer z^3 :

```
-----
| Sage Version 4.8, Release Date: 2012-01-20                               |
| Type notebook() for the GUI, and license() for information.             |
|-----|
sage: var('a,b')
(a, b)
sage: z=a+I*sqrt(2)*b
sage: (z**3).expand()
3*I*sqrt(2)*a^2*b - 2*I*sqrt(2)*b^3 + a^3 - 6*a*b^2
```

En identifiant cela à $x + i\sqrt{2}$ nous trouvons le système

$$\begin{cases} x = a^3 - 6ab^2 \\ 1 = 3a^2b - 2b^3 \end{cases} \quad (3.128a)$$

$$(3.128b)$$

où, nous le rappelons, x , a et b sont des entiers. La seconde équation montre que b doit être inversible : $b(3a^2 - 2b^2) = 1$. Il y a donc les possibilités $b = \pm 1$. Pour $b = 1$ l'équation devient $3a^2 - 2 = 1$, c'est-à-dire $a = \pm 1$. Pour $b = -1$ l'équation devient $3a^2 - 2 = -1$, impossible. En conclusion les possibilités sont

$$(x, z) = (-5, 1 + i\sqrt{2}) \quad (3.129a)$$

$$(x, z) = (5, -1 + i\sqrt{2}) \quad (3.129b)$$

$$(3.129c)$$

Le travail avec $x - i\sqrt{2}$ donne les mêmes résultats.

Les deux solutions de l'équation $x^2 + 2 = y^3$ sont alors $(5, 3)$ et $(-5, 3)$. $\triangle$

3.9.2 Triplets pythagoriciens et équation de Fermat pour $n = 4$

Définition 3.110.

Les solutions entières (positives) de l'équation $x^2 + y^2 = z^2$ sont appelés **triplets pythagoriciens**.

Ils donnent toutes les possibilités de triangles rectangles dont les côtés ont des longueurs entières.

Définition 3.111.

On dit qu'un triplet pythagoricien est **primitif** si les trois nombres sont premiers dans leur ensemble³².

32. Définition 1.180.

Remarquons que cela est équivalent à montrer que les trois nombres sont premiers deux à deux : en effet, si deux parmi x , y et z sont divisibles par un nombre, alors tous les trois sont divisibles par ce nombre³³, donc les nombres x , y et z sont premiers deux à deux.

Lemme 3.112.

Dans un triplet pythagoricien primitif (x, y, z) , on a toujours z impair et :

- soit x impair et y pair ;
- soit x pair et y impair.

Démonstration. Remarquons que le fait d'imposer que le triplet soit primitif, interdit aux nombres x et y d'être pairs en même temps. En effet, si c'était le cas, alors x^2 et y^2 seraient aussi pairs, donc leur somme z^2 aussi, d'où z serait pair et les trois nombres ne seraient pas premiers entre eux.

Nous montrons à présent que les nombres x et y ne sont pas tous les deux impairs. Par l'absurde, si $x = 2a + 1$, nous avons $x^2 = 4a^2 + 4a + 1 \in [1]_4$; de la même manière, $y^2 \in [1]_4$. On en déduit alors que $z^2 = x^2 + y^2 \in [2]_4$. Le nombre z^2 est donc pair, donc z est pair : disons $z = 2c$. Alors, $z^2 = 4c^2 \in [0]_4$. Comme les classes modulo 4 sont disjointes, nous aboutissons à une contradiction. $\square$

Proposition 3.113 (Triplets pythagoriciens[90, 91]).

Un triplet $(x, y, z) \in (\mathbb{N}^*)^3$ est solution de $x^2 + y^2 = z^2$ si et seulement s'il existe $d \in \mathbb{N}$ et $u, v \in \mathbb{N}^*$ premiers entre eux tels que

$$\begin{cases} x = d(u^2 - v^2) & (3.130a) \\ y = 2d uv & (3.130b) \\ z = d(u^2 + v^2) & (3.130c) \end{cases}$$

ou

$$\begin{cases} x = 2d uv & (3.131a) \\ y = d(u^2 - v^2) & (3.131b) \\ z = d(u^2 + v^2) & (3.131c) \end{cases}$$

La différence entre les deux est seulement d'inverser les rôles de x et y .

Démonstration. Montrons d'abord que les formules proposées sont bien des solutions ; nous vérifions (3.130) :

$$x^2 + y^2 = d^2(u^2 - v^2)^2 + 4d^2 u^2 v^2 = d^2(u^2 + v^2)^2, \quad (3.132)$$

qui correspond bien au z^2 proposé.

Nous allons maintenant prouver la réciproque : toute solution est d'une des deux formes proposées. Déterminer les triplets primitifs suffira parce que si (x, y, z) n'est pas une solution primitive, alors en posant $k = \text{pgcd}(x, y, z)$, le triplet $(\frac{x}{k}, \frac{y}{k}, \frac{z}{k})$ est primitif. Connaissant les triplets primitifs, nous obtenons tous les autres par simple multiplication.

Soit donc (x, y, z) un triplet pythagoricien primitif. Sans perte de généralité³⁴, grâce au lemme 3.112, nous pouvons supposer x est pair tandis que y et z sont impairs. Comme $x^2 = (z + y)(z - y)$, nous avons

$$\left(\frac{x}{2}\right)^2 = \left(\frac{z + y}{2}\right)^2 \left(\frac{z - y}{2}\right)^2. \quad (3.133)$$

Vu que z et y sont premiers entre eux, les nombres $z - y$ et $z + y$ sont également premiers entre eux³⁵. Donc les facteurs premiers (qui arrivent au moins au carré) de $(x/2)^2$ sont chacun soit dans

33. Parce que k et k^2 ont les mêmes facteurs premiers.

34. En échangeant les rôles de x et y ici, nous obtenons à la fin la seconde forme des solutions.

35. Si $z - y = kn$ et $z + y = km$, faisant la somme et la différence on voit que y et z sont divisibles par k .

$(z + y)/2$ soit dans $(z - y)/2$. Nous en déduisons que ces derniers sont des carrés d'entiers. Nous posons

$$\frac{z - y}{2} = u^2 \quad \frac{z + y}{2} = v^2. \quad (3.134)$$

Bien entendu u et v sont non nuls parce que nous avons exclu la possibilité de triplets dont un élément serait nul. Avec tout cela nous avons $(x/2)^2 = u^2 v^2$ et donc $x = 2uv$ puis par somme et différence :

$$\begin{cases} x = 2uv & (3.135a) \\ y = v^2 - u^2 & (3.135b) \\ z = u^2 + v^2, & (3.135c) \end{cases}$$

ce qu'il fallait. $\square$

Remarque 3.114.

Les solutions dans lesquelles x , y ou z sont nuls sont faciles à classer. La solution $(1, 0, 1)$ n'est pas dans les formes proposées. En effet elle ne peut pas être de la première forme : avoir $y = 0$ demanderait qu'un nombre parmi d , u et v soit nul, ce qui est interdit. La solution $(1, 0, 1)$ ne peut pas non plus être de la seconde forme parce que x y est pair.

Proposition 3.115 ([90]).

Les équations $x^4 + y^4 = z^2$ et $x^2 + y^4 = z^4$ n'ont pas de solutions dans $(\mathbb{N}^*)^3$.

Démonstration. Si la première équation n'a pas de solutions, alors la seconde n'en n'a pas non plus parce que z^4 est un carré. Nous nous concentrons donc sur l'équation $x^4 + y^4 = z^2$ et nous supposons qu'il existe au moins une solution dans $(\mathbb{N}^*)^3$. Nous en choisissons une (x, y, z) avec z minimum (les z dans différentes solutions étant dans $\mathbb{N}$, il en existe forcément un minimum³⁶). Du coup, les trois nombres x , y et z sont premiers dans leur ensembles parce que une division par leur pgcd donnerait une nouvelle solution qui contredirait la minimalité de z .

Nous posons $x^4 = \bar{x}^2$ et $y^4 = \bar{y}^2$. Ils vérifient l'équation $\bar{x}^2 + \bar{y}^2 = z^2$ et par la proposition 3.113, il existe $u, v \in \mathbb{N}^*$ premiers entre eux tels que, sans perte de généralité³⁷, on ait

$$\begin{cases} \bar{x} = 2uv & (3.136a) \\ \bar{y} = u^2 - v^2 & (3.136b) \\ z = u^2 + v^2. & (3.136c) \end{cases}$$

Si u est pair, alors v est impair (et inversement) parce que $\text{pgcd}(u, v) = 1$. Si u est pair, alors $u = 2a$ et $v = 2b + 1$, ce qui donne $\bar{y} = 4a^2 - 4b^2 - 4b - 1 \in [-1]_4$. Or nous avons déjà vu qu'un carré est dans $[0]_4$ ou dans $[1]_4$. Il faut donc que u soit impair. Le lemme 3.112 implique alors que v soit pair.

De l'équation 3.136b, nous en déduisons que $v^2 + \bar{y} = u^2$; de plus u^2 , v^2 et $\bar{y}$ sont premiers dans leur ensemble : en effet, u et v sont premiers entre eux, et si l'un parmi u^2 et v^2 a un facteur commun avec $\bar{y}$, alors l'autre doit l'avoir aussi (dans une égalité $a + b = c$, si deux des nombres ont un diviseur commun, le troisième l'a aussi). Comme $\bar{y} = y^2$, le triplet (v, y, u) est un triplet pythagoricien primitif. Nous réappliquons la proposition 3.113, en se souvenant que v est pair : il existe donc deux nombres r et s premiers entre eux tels que

$$\begin{cases} v = 2rs & (3.137a) \\ y = r^2 - s^2 & (3.137b) \\ u = r^2 + s^2. & (3.137c) \end{cases}$$

36. Voir quelque chose comme le lemme 1.118.

37. En inversant les rôles de x et y au besoin.

Avec cela, $\bar{x} = 2uv = 4rs(r^2 + s^2)$. Remarquons que les trois nombres r , s et $r^2 + s^2$ sont premiers entre eux dans leur ensemble ; or, comme $\bar{x}$ est un carré ces nombres doivent séparément être des carrés :

$$\begin{cases} r = \alpha^2 & (3.138a) \\ s = \beta^2 & (3.138b) \\ r^2 + s^2 = \gamma^2. & (3.138c) \end{cases}$$

En mettant les deux premiers dans la troisième, nous avons $\alpha^4 + \beta^4 = \gamma^2$. Donc $(\alpha^2, \beta^2, \gamma)$ est une solution. Nous allons prouver que $\gamma < z$, ce qui terminera la preuve, puisque z était supposé minimal. Nous avons :

$$\begin{aligned} z &= u^2 + v^2 && \text{par 3.136c} \\ &= r^2 + s^2 + 4r^2s^2 && \text{par 3.137} \\ &= \gamma^2 + 4r^2s^2 \\ &> \gamma^2, \end{aligned}$$

et a fortiori $\gamma < z$. □

3.10 Polynômes à coefficients dans un anneau commutatif

Lemme 3.116.

Nous considérons un polynôme $P \in A[X]$, et le quotient $A[X]/(P)$. Pour tout polynôme $Q \in A[X]$ nous avons les égalités

$$Q(\bar{X}) = \overline{Q(X)} = \bar{Q}. \quad (3.139)$$

Démonstration. Si $Q = \sum_k a_k X^k$, alors par la linéarité de la prise de classes,

$$\bar{Q} = \sum_k a_k \bar{X}^k. \quad (3.140)$$

Nous insistons sur le fait que cette égalité n'est rien d'autre que l'itération de la définition de la somme dans l'espace quotient : $\bar{x} + \bar{y} = \overline{x+y}$ ainsi que du produit $k\bar{x} = \overline{kx}$ (définition 1.168). Toujours par définition du produit appliqué à l'élément $\bar{X}$ nous avons $(\bar{X})^2 = \overline{X^2}$; par récurrence $\bar{X}^k = \overline{X^k}$, et

$$\bar{Q} = \sum_k a_k \bar{X}^k = Q(\bar{X}). \quad (3.141)$$

Le fait que $\bar{Q} = \overline{Q(X)}$ n'est rien d'autre que le fait que dans $A[X]$ nous avons $Q = Q(X)$, comme expliqué dans le lemme 1.245. □

3.10.1 Monômes

3.117.

Les éléments de la forme λX^k avec $\lambda \in A$ et $k \in \mathbb{N}$ sont des **monômes**.

Nous allons aussi considérer

$$A_n[X] = \{P \in A[X] \text{ tel que } \deg(P) \leq n\}. \quad (3.142)$$

Cela est un sous-module libre.

3.10.2 Évaluation

Soit $P \in A[X]$. À priori, P n'est qu'une suite dans A indexée par $\mathbb{N}$.

Nous avons déjà défini son évaluation sur un élément $\alpha \in A$ dans la définition 1.242 :

$$P(\alpha) = \sum_k a_k \alpha^k. \quad (3.143)$$

Cette somme est toujours finie.

3.118.

L'ensemble $A[X]$ est une algèbre et donc un espace vectoriel. Il possède un unique élément nul qui est celui dont tous les coefficients sont nuls ; cela est immédiat par la construction en tant que suites presque nulles.

Il n'y a à priori pas équivalence entre le fait d'être un polynôme nul et le fait de s'évaluer à zéro sur tous les éléments de A . Cela sera discuté dans le théorème 6.103 et l'exemple 19.40.

Définition 3.119.

Soient un anneau A et un anneau B qui contient A (comme sous-anneau). Pour $\alpha \in B$ nous définissons $A[\alpha]_B$ comme étant l'intersection de tous les sous-anneaux de B contenant A .

Comme dit plus haut, nous nous permettons d'écrire $A[\alpha]$ sans préciser B lorsque ce dernier sera clair dans le contexte.

Proposition 3.120.

Soient un anneau A et un anneau B qui contient A (comme sous-anneau). Pour tout $\alpha \in B$ nous avons

$$A[\alpha] = \{P(\alpha) \text{ tel que } P \in A[X]\} \quad (3.144)$$

où encore une fois, $P(\alpha)$ est calculé dans B ; le contexte est clair là-dessus.

Démonstration. Si A' est un sous-anneau de B contenant A et α , alors A' contient tous les $P(\alpha)$ avec $P \in A[X]$. Nous avons donc

$$\{P(\alpha) \text{ tel que } P \in A[X]\} \subset A[\alpha]. \quad (3.145)$$

Par ailleurs, $\{P(\alpha) \text{ tel que } P \in A[X]\}$ est un sous-anneau de B contenant A et α . Donc $A[\alpha]$ y est inclus. $\square$

3.10.3 Polynômes sur un anneau intègre**Théorème 3.121.**

L'anneau A est intègre si et seulement si $A[X]$ est intègre.

Démonstration. Soient P et Q des éléments non nuls de $A[X]$. Vu que l'anneau A est intègre, nous avons

$$\deg(PQ) = \deg(P) + \deg(Q) \quad (3.146)$$

et le produit ne peut pas être nul. L'anneau $A[X]$ est donc intègre.

Si $A[X]$ est intègre, A est intègre parce qu'il peut être vu comme sous anneau. $\square$

3.122.

Si A n'est pas intègre, soient $\alpha, \beta \in A$ non nuls tels que $\alpha\beta = 0$. Le produit des polynômes $X \mapsto \alpha X$ et $X \mapsto \beta$ est $(\alpha X)(\beta) = 0$; le degré du produit n'est pas la somme des degrés.

Les personnes qui ont tout compris jusqu'ici remarqueront que la notation « $X \mapsto P(X)$ » n'est pas correcte parce que du point de vue que nous adoptons ici, un polynôme n'est pas une application.

Corolaire 3.123.

Si A est intègre, les inversibles de $A[X]$ sont les éléments de $U(A)$.

Démonstration. Pour que Q soit inversible, il faut un P tel que $PQ = 1$. Mais l'anneau A étant intègre, les degrés s'additionnent. Par conséquent ils doivent être de degrés zéro et il faut que $P, Q \in A$. Enfin pour qu'ils soient inversibles, ils doivent être dans $U(A)$. $\square$

La **valuation** du polynôme $P = \sum_n a_n X^n$, notée $\text{val}(P)$, est

$$\text{val}(P) = \min\{n \text{ tel que } a_n \neq 0\}. \quad (3.147)$$

Nous avons $\text{val}(P) \leq \deg(P)$ et $\text{val}(P) = \deg(P)$ si et seulement si P est un monôme. Si $P = 0$, nous convenons que $\text{val}(0) = \infty$ et $\deg(0) = -\infty$.

3.10.4 Division euclidienne

Le théorème suivant établit la **division euclidienne** dans $A[X]$ du polynôme P par un polynôme D .

Théorème 3.124.

Soit $D \neq 0$ dans $A[X]$ de coefficient dominant inversible dans A . Pour tout $P \in A[X]$, il existe $Q, R \in A[X]$ tels que

$$P = QD + R \quad (3.148)$$

avec $\deg(R) < \deg(D)$.

Les polynômes Q et R sont déterminés de façon univoque par cette condition.

Définition 3.125.

Le polynôme Q est le **quotient** et R est le **reste** de la division euclidienne de P par D . Si le reste de la division de P par D est nul on dit que D **divise** P et on note $D \mid P$. Autrement dit D divise P s'il existe Q tel que $P = QD$.³⁸

3.126.

Le théorème 3.124 nous incite à utiliser le degré comme stathme euclidien sur $A[X]$ dès que A est un anneau intègre. Or cela ne fonctionne en général pas parce que très peu de polynômes ont à priori un coefficient dominant inversible.

Lemme 3.127 (Thème 49).

Si $\mathbb{K}$ est un corps³⁹, alors l'anneau $\mathbb{K}[X]$ est euclidien et principal.

Démonstration. Vu que $\mathbb{K}$ est un corps, tous les éléments sont inversibles et le degré donne un stathme par le théorème 3.124. L'anneau $\mathbb{K}[X]$ est donc euclidien et par conséquent principal (proposition 3.102). $\square$

Dans le théorème 6.39 nous donnerons une preuve directe du fait que $\mathbb{K}[X]$ est principal en montrant que tous ses idéaux sont principaux. Nous y démontrerons donc un peu moins pour un peu plus cher, mais avec le plaisir de ne pas devoir passer par un stathme.

Définition 3.128 ([92]).

Soit un anneau A . Deux polynômes P et Q dans $A[X]$ sont dits **étrangers** entre eux si 1 est un pgcd⁴⁰ de P et Q . Un ensemble de polynômes $(P_i)_{i \in I}$ est étranger **dans leur ensemble** si 1 est un pgcd des P_i .

Les polynômes P et Q sont **premiers entre eux** si les seuls diviseurs communs de P et Q sont les inversibles.

Les notions de polynômes étrangers entre eux ou de polynômes premiers entre eux ne sont pas identiques, comme le montre l'exemple suivant.

Exemple 3.129 ([1]).

Soient dans $\mathbb{Z}[X]$ les polynômes $P(X) = 2X + 2$ et $Q(X) = 2X^2 + 2$. Le nombre 2 est diviseur commun et n'est pas un diviseur de 1. Donc 1 n'est pas un pgcd de P et Q . Ils ne sont pas étrangers.

Mais ils sont premiers entre eux parce qu'ils n'ont pas d'autres diviseurs communs que les inversibles (1 et -1). $\triangle$

38. Ceci se rapproche tout naturellement des notions de divisibilité dans un anneau intègre général, vues en sous-section 3.5.1.

39. Définition 1.190.

40. Définition 1.169.

3.10.5 Polynôme primitif

Définition 3.130.

Le **contenu** du polynôme $P = \sum_i a_i X^i \in \mathbb{K}[X]$ est le pgcd de ses coefficients : $c(P) = \text{pgcd}(a_i)$.

Définition 3.131 (Ordre d'un polynôme).

Soit P un polynôme irréductible de degré n sur $\mathbb{F}_p[X]$. L'**ordre** de P est

$$\min\{k \text{ tel que } P \mid X^k - 1\}. \quad (3.149)$$

Définition 3.132 (Polynôme primitif).

Soit p , un nombre premier et P un polynôme de degré n dans $\mathbb{F}_p[X]$. Nous disons que P est **primitif** si

- (1) P est unitaire et irréductible,
- (2) les racines de P sont d'ordre $p^n - 1$ dans $\mathbb{F}_p[X]/P$.

Définition 3.133 (Polynôme primitif au sens du pgcd).

Soit un anneau A . Un polynôme $P \in A[X]$ est **primitif au sens du pgcd** si ses coefficients sont premiers entre eux.

3.134.

Pour rappel, il y a plusieurs façons de périphraser le fait que les coefficients soient premiers entre eux. Nous pouvons dire ...

- (1) Le pgcd de ses coefficients est 1 parce que c'est la définition 3.84 d'avoir des nombres premiers entre eux.
- (2) Le contenu de ses coefficients est 1. Parce que le contenu est précisément le pgcd, définition 3.130.

La notion de polynôme primitif au sens du pgcd est particulière aux polynômes à coefficients dans un anneau comme le montre le lemme suivant.

Lemme 3.135.

Si $\mathbb{K}$ est un corps, tout polynôme unitaire dans $\mathbb{K}[X]$ non nul est primitif au sens du pgcd.

Démonstration. Un polynôme unitaire a un 1 parmi ses coefficients, donc le pgcd est forcément 1. □

Lorsque nous utiliserons la notion de polynôme primitif au sens du pgcd, nous le mentionnerons explicitement. C'est pas exemple le cas pour le corolaire 3.147.

3.10.6 Racines des polynômes

Définition 3.136.

Soient A un anneau et $P \in A[X]$. On appelle **racine** un élément $\alpha \in A$ tel que $P(\alpha) = 0$; c'est-à-dire que, en remplaçant toutes les occurrences de X par α dans l'expression de P , on obtient 0.

Proposition 3.137.

Soient A un anneau et P un polynôme non nul dans $A[X]$. Si $\alpha \in A$ est une racine de P alors $X - \alpha$ divise P , et réciproquement.

Démonstration. Nous notons le polynôme $\mu = X - \alpha$ par analogie avec le polynôme minimal dont il sera question dans la très semblable proposition 6.88. Le sens réciproque est clair : si μ divise P , alors α est racine de P .

Pour le sens direct, remarquons que si α est racine de P , alors P est de degré au moins égal à 1, et nous pouvons donc effectuer la division euclidienne⁴¹ de P par μ : il existe des polynômes Q

41. Théorème 3.124.

et R tels que

$$P = Q\mu + R \quad (3.150)$$

avec $\deg(R) < \deg(\mu)$. Donc R est une constante, élément de A : appelons-le a . En évaluant (3.150) en α , il vient

$$0 = P(\alpha) = Q(\alpha)\mu(\alpha) + a, \quad (3.151)$$

et nous en déduisons que $a = 0$, ce qui montre que $P = Q\mu$ et que μ divise P . $\square$

Définition 3.138 (Racine simple et multiple d'un polynôme).

Soit A un anneau ainsi qu'un polynôme $P \in A[X]$ et $\alpha \in A$ racine de P . La **multiplicité** de α par rapport à P est l'entier h tel que P est divisible par $(X - \alpha)^h$ mais pas divisible par $(X - \alpha)^{h+1}$. Nous noterons $\theta_\alpha(P)$ la multiplicité de α par rapport à P .

3.139.

Pour une définition générale d'une racine simple de l'équation $f(x) = 0$, voir la définition 34.50. La proposition 3.137 nous indique que toute racine est de multiplicité au moins 1.

Proposition 3.140.

Soient un anneau A , un polynôme $P \in A[X]$ de degré n , ainsi qu'une racine $\alpha \in A$ de P . Alors il existe un polynôme $Q \in A[X]$ de degré $n - 1$ tel que $P = (X - \alpha)Q$.

Proposition 3.141.

L'élément $\alpha \in A$ est une racine de multiplicité h du polynôme P si et seulement s'il existe $Q \in A[X]$ tel que $P = (X - \alpha)^h Q$ avec $Q(\alpha) \neq 0$.

Lemme 3.142.

Soient P et Q des polynômes non nuls de $A[X]$ et $\alpha \in A$. Alors

- (1) $\theta_\alpha(P + Q) \leq \min\{\theta_\alpha(P), \theta_\alpha(Q)\}$, et l'égalité a lieu si $\theta_\alpha(P) \neq \theta_\alpha(Q)$;
- (2) $\theta_\alpha(PQ) \geq \theta_\alpha(P) + \theta_\alpha(Q)$, et l'égalité a lieu si A est intègre.

Dans le théorème suivant, la partie importante en pratique est la seconde partie parce qu'elle dit que, lorsque nous cherchons les racines d'un polynôme, nous pouvons nous arrêter lorsque nous en avons trouvé autant que le degré, multiplicité comprise.

Théorème 3.143.

Soit A un anneau intègre et $P \in A[X] \setminus \{0\}$, un polynôme de degré n .

- (1) Si $\alpha_1, \dots, \alpha_p \in A$ sont des racines deux à deux distinctes de multiplicités $k_1, \dots, k_p$, alors il existe $Q \in A[X]$, de degré $n - p$, tel que $P = Q \prod_{i=1}^p (X - \alpha_i)^{k_i}$ et $Q(\alpha_i) \neq 0$ pour tout i .
- (2) La somme des multiplicités des racines de P est au plus $\deg(P)$.

Démonstration. Si $p = 1$, soit α une racine de multiplicité k de P . La définition de la multiplicité d'une racine nous dit que P est divisible par $(X - \alpha)^k$ mais pas par $(X - \alpha)^{k+1}$. Donc il existe $Q \in A[X]$ tel que $P = Q(X - \alpha)^k$. Il reste à voir que $Q(\alpha) \neq 0$. Cela est une conséquence de la proposition 3.137 : si $Q(\alpha)$ était nul, on pourrait lui factoriser $(X - \alpha)$ et donc avoir $(X - \alpha)^{k+1}$ qui se factorise dans P , ce qui n'est pas possible.

Nous supposons que $p \geq 2$ et nous effectuons une récurrence sur p . Nous considérons donc les $p - 1$ premières racines $\alpha_1, \dots, \alpha_{p-1}$ et un polynôme $R \in A[X]$ tel que $R(\alpha_i) \neq 0$ pour $i = 1, \dots, p - 1$ et

$$P = \underbrace{(X - \alpha_1)^{k_1} \dots (X - \alpha_{p-1})^{k_{p-1}}}_S R. \quad (3.152)$$

Par hypothèse $P(\alpha_p) = S(\alpha_p)R(\alpha_p) = 0$. L'anneau A étant intègre, $S(\alpha_p) \neq 0$ parce que $\alpha_i \neq \alpha_p$ pour $i \neq p$. Par conséquent, $R(\alpha_p) = 0$.

Nous devons encore vérifier que la multiplicité α_p est k_p par rapport à R . Pour cela nous utilisons le point (2) du lemme 3.142 afin de dire que le degré de α_p pour $P = SR$ est k_p . Par conséquent

$$R = (X - \alpha_p)^{k_p} T \quad (3.153)$$

avec $T(\alpha_p) \neq 0$ et enfin

$$P = \prod_{i=1}^p (X - \alpha_i) T. \quad (3.154)$$

De plus $T(\alpha_i) \neq 0$, sinon $R(\alpha_i)$ serait nul. $\square$

Corolaire 3.144.

Un polynôme de degré n sur un anneau intègre possède au maximum n racines distinctes.

Démonstration. Le théorème 3.143(2) dit que la somme des multiplicités des racines de P est au maximum n . Mais la proposition 3.137 dit que toutes les racines ont une multiplicité au moins un. Donc il ne peut pas y en avoir plus de n . $\square$

Proposition 3.145 ([93, 94]).

Soit un anneau intègre et $n > 0$. Les racines n^e de l'unité forment un groupe cyclique dont l'ordre divise n .

Lemme 3.146.

Soit le polynôme $P = X^2 - 1$ sur l'anneau intègre⁴² A . Si $1 \neq -1$ ⁴³, alors les racines de P sont ± 1 .

Démonstration. Le fait que ± 1 sont racines est le lemme 1.165(1)(4). Vu que par hypothèse $1 \neq -1$, le corollaire 3.144 termine la preuve. $\square$

Corolaire 3.147 (Conséquence du lemme de Gauss[95]).

Soient A un anneau factoriel et $\text{Frac}(A)$ son corps des fractions. Un polynôme non constant $P \in A[X]$ est irréductible (sur A) si et seulement s'il est irréductible et primitif au sens du pgcd⁴⁴ sur $\text{Frac}(A)[X]$.

Exemple 3.148.

Il ne faudrait pas croire qu'être irréductible dans un anneau A implique d'être irréductible dans le corps des fractions. En effet soit $A = \mathbb{Z}[\sqrt{5}]$ et $P = X^2 - X - 1$. Nous savons que sa factorisation est

$$P = \left(X - \frac{1 + \sqrt{5}}{2}\right) \left(X - \frac{1 - \sqrt{5}}{2}\right). \quad (3.155)$$

Si vous ne le saviez pas, faites juste le calcul pour vous en assurer.

Ce polynôme est irréductible sur $\mathbb{Z}[\sqrt{5}]$ mais pas irréductible sur $\text{Frac}(\mathbb{Z}[\sqrt{5}])$. $\triangle$

3.10.7 Quelques identités

Lemme 3.149.

Quelques identités de polynômes.

- (1) Si n est impair, alors $1 + X$ divise $1 + X^n$.
- (2) Pour tout n nous avons $X^n - 1 = (X - 1)(1 + X + \dots + X^{n-1})$.
- (3) $X^n - a^n = (X - a) \sum_{i=0}^{n-1} a^i X^{n-1-i}$.

42. Définition 1.174.

43. À mon avis cette hypothèse n'est pas nécessaire. Et d'ailleurs j'ai un peu du mal à voir des exemples exotiques d'anneaux intègres dans lesquels $1 = -1$. Il y aurait $[0, 1]$ modulo 2, certaines de ses parties, comme $\mathbb{Z}/2\mathbb{Z}$. Et quoi d'autre ?

44. Définition 3.133.

Démonstration. Nous démontrons uniquement le point (2), puisque les autres ont été vus en début de chapitre⁴⁵. Le cas $n = 1$ est évident. Procédons alors par récurrence en considérant un nombre entier impair n :

$$1 + X^{n+2} = 1 + X^n + X^{n+2} - X^n \quad (3.156a)$$

$$= (1 + X)P + X^n(X^2 - 1) \quad (3.156b)$$

$$= (1 + X)P + X^n(X + 1)(X - 1) \quad (3.156c)$$

$$= (1 + X)(P + X^n(X - 1)). \quad (3.156d)$$

□

45. Voir l'égalité (3.1).

Chapitre 4

Espaces vectoriels (début)

4.1 Parties libres, génératrices, bases et dimension

Nous avons déjà défini (dans 1.214) un espace vectoriel comme étant un module sur un corps commutatif. En explicitant un peu, cela donne ceci[96].

Un espace vectoriel sur le corps $\mathbb{K}$ est un ensemble V muni de deux opérations :

- une loi de composition interne $+: V \times V \rightarrow V$,
- une loi de composition externe $\cdot: \mathbb{K} \times V \rightarrow V$

telles que

- (1) $(V, +)$ soit un groupe abélien,
- (2) pour tout $u, v \in V$ et pour tout $k, k' \in \mathbb{K}$,

$$k(u + v) = (ku) + (kv) \quad (4.1a)$$

$$(kk')u = k(k'u) \quad (4.1b)$$

$$(k + k')u = (ku) + (k'u) \quad (4.1c)$$

$$1u = u \quad (4.1d)$$

où 1 est le neutre de $\mathbb{K}$ et où nous avons directement adopté la notation ku pour $k \cdot u$.

Si $u \in V$, nous notons $-u$ l'inverse de u dans le groupe $(V, +)$.

Définition 4.1 (Partie libre).

Si E est un espace vectoriel, une partie A de E est **libre** si pour tout choix d'un nombre fini d'éléments $\{u_i\}_{i=1,\dots,n}$ de A , l'égalité

$$a_1u_1 + \dots + a_nu_n = 0 \quad (4.2)$$

implique $a_i = 0$ pour tout i (ici les a_i sont dans le corps de base).

Une partie infinie est libre si toutes ses parties finies le sont.

Remarque 4.2.

Notons que le vecteur nul n'est dans aucune partie libre, ne fût-ce que parce que $a0 = 0$ n'implique pas $a = 0$.

Si A est une partie de l'espace vectoriel E nous notons $\text{Span}(A)$ l'ensemble des combinaisons linéaires finies d'éléments de A . Les coefficients de ces combinaisons linéaires sont dans le corps de base $\mathbb{K}$.

Définition 4.3 (Partie génératrice).

Une partie B d'un espace vectoriel E est **génératrice** si $\text{Span}(B) = E$.

Remarque 4.4.

Ces définitions demandent des commentaires en dimension infinie¹.

1. Nous n'avons pas encore défini le concept de dimension, mais nous nous adressons au lecteur trop pressé.

- (1) Tout élément peut être écrit comme combinaison linéaire finie d'une partie génératrice. Cela ne signifie pas que nous pouvons extraire une partie finie qui convient pour tous les éléments à la fois. Lorsque l'espace est de dimension infinie, ceci est particulièrement important.
- (2) La définition séparée de liberté dans le cas des parties infinies a son importance lorsqu'on parle d'espaces vectoriels de dimension infinies (en dimension finie, aucune partie infinie n'est libre) parce que cela fera une différence entre une base algébrique et une base hilbertienne par exemple.

Définition 4.5 (Base).

Une **base** de l'espace vectoriel E est une partie à la fois génératrice et libre.

Nous prouvons à présent que tout élément non nul d'un espace vectoriel possédant une base² se décompose de façon unique en combinaison linéaire finie d'éléments d'une base.

Proposition 4.6 ([1]).

Soient un espace vectoriel E sur $\mathbb{K}$ muni d'une base $\{e_i\}_{i \in I}$. Si $v \in E$, alors il existe un unique couple (J, c) où

- (1) J est une partie finie de I ;
- (2) $c: J \rightarrow \mathbb{K}$ est une application
- (3) $v = \sum_{j \in J} c(j)e_j$.

Les éléments $c(i)$ seront notés v_i et sont les composantes de v dans la base. Sous-entendu, on prolonge c de J vers I par zéro sur $I \setminus J$.

Démonstration. Soit un espace vectoriel E et une base $\{e_i\}_{i \in I}$ où I est un ensemble à priori quelconque. Soit $v \in E$. Vu que $E = \text{Span}\{e_i\}_{i \in I}$, il existe une partie finie J de I et des coefficients $\{v_j\}_{j \in J}$ dans $\mathbb{K}$ tels que

$$v = \sum_{j \in J} v_j e_j. \quad (4.3)$$

Cela donne l'existence.

En ce qui concerne l'unicité, soient J et K des parties finies de I et des coefficients $\{v_j\}_{j \in J}$ et $\{w_k\}_{k \in K}$ tels que

$$v = \sum_{j \in J} v_j e_j = \sum_{k \in K} w_k e_k. \quad (4.4)$$

Nous posons $L = J \cup K$. Remarquez que les unions suivantes sont des unions disjointes :

$$L = (J \setminus K) \cup (J \cap K) \cup (K \setminus J) \quad (4.5a)$$

$$J = (J \setminus K) \cup (J \cap K) \quad (4.5b)$$

$$K = (K \cap J) \cup (K \setminus J). \quad (4.5c)$$

Écrivons $0 = v - v$ en utilisant les expressions de v de (4.4) et en décomposant les sommes :

$$0 = \sum_{j \in J} v_j e_j - \sum_{k \in K} w_k e_k \quad (4.6a)$$

$$= \sum_{j \in J \setminus K} v_j e_j + \sum_{j \in J \cap K} v_j e_j - \sum_{k \in K \cap J} w_k e_k - \sum_{k \in K \setminus J} w_k e_k \quad (4.6b)$$

$$= \sum_{j \in J \setminus K} v_j e_j + \sum_{j \in J \cap K} (v_j - w_j) e_j - \sum_{k \in K \setminus J} w_k e_k. \quad (4.6c)$$

Là-dessus, nous posons

$$\alpha_l = \begin{cases} v_l & \text{si } l \in J \setminus K \\ v_l - w_l & \text{si } l \in J \cap K \\ -w_l & \text{si } l \in K \setminus J. \end{cases} \quad (4.7)$$

2. Nous n'avons pas démontré que tout espace vectoriel possède une base. Donc à notre niveau, il est possible que ce théorème soit sans objet pour beaucoup d'espaces.

Nous avons alors

$$\sum_{l \in L} \alpha_l e_l = 0. \quad (4.8)$$

Vu que $\{e_i\}_{i \in I}$ est libre, la partie $\{e_l\}_{l \in L}$ est également libre. Donc l'équation (4.8) implique que $\alpha_l = 0$ pour tout $l \in L$.

Nous devons prouver que

$$\{j \in J \text{ tel que } v_j \neq 0\} = \{k \in K \text{ tel que } w_k \neq 0\} \quad (4.9)$$

et que pour l dans cet ensemble, $v_l = w_l$.

Soit $j \in J$; il y a deux possibilités : soit $j \in J \setminus K$, soit $j \in J \cap K$. Dans le premier cas nous avons déjà vu que $\alpha_j = v_j = 0$. Dans le second cas, $\alpha_j = v_j - w_j = 0$, c'est-à-dire $v_j = w_j$.

Donc $j \in J$ vérifiant $v_j \neq 0$ implique $j \in J \cap K$ et l'égalité des coefficients. Idem avec $k \in K$ tel que $w_k \neq 0$ implique $k \in J \cap K$. $\square$

Lemme 4.7 ([1]).

Soit un espace vectoriel admettant des bases. Un endomorphisme est une bijection si et seulement si il change toute base en une base.

Démonstration. En deux parties. Soit un espace vectoriel E possédant des bases et un endomorphisme $f: E \rightarrow E$.

Si f est bijective Soit une base $\{v_i\}_{i \in I}$; nous devons voir que $\{f(v_i)\}_{i \in I}$ est une base.

Libre Si J est une partie finie de I et si les λ_j sont des scalaires tels que $\sum_{j \in J} \lambda_j f(v_j) = 0$, alors

$$0 = \sum_{j \in J} \lambda_j f(v_j) = f\left(\sum_{j \in J} \lambda_j v_j\right). \quad (4.10)$$

Mais comme f est bijective, cela implique que $\sum_{j \in J} \lambda_j v_j = 0$. En retour, parce que $\{v_i\}$ est une base, cela implique que $\lambda_j = 0$ pour tout j .

Générateur Soit $x \in E$. Vu que f est bijective, il existe un unique $y \in E$ tel que $x = f(y)$.

Comme $\{v_i\}_{i \in I}$ est une base, il existe une partie finie $J \subset I$ et des scalaires $\{\lambda_j\}_{j \in J}$ tels que

$$y = \sum_{j \in J} \lambda_j v_j. \quad (4.11)$$

Nous avons alors

$$x = f(y) = \sum_{j \in J} \lambda_j f(v_j), \quad (4.12)$$

qui montre que $\{f(v_i)\}_{i \in I}$ est bien génératrice de E .

Si f change les bases en bases Soit un endomorphisme changeant toute base en une base.

Nous devons prouver qu'il est bijectif.

Injective Nous considérons une base $\{v_i\}_{i \in I}$. La partie $\{f(v_i)\}_{i \in I}$ est par hypothèse également une base.

Soient $x, y \in E$ tels que $f(x) = f(y)$. Il existe J et K finis dans I qui permettent de décomposer x et y respectivement dans la base $\{f(v_i)\}_{i \in I}$. Quitte à poser $J' = J \cup K$, nous supposons que J suffit³. Il existe donc des scalaires $\{\lambda_j\}_{j \in J}$ et $\{\mu_j\}_{j \in J}$ tels que $x = \sum_{j \in J} \lambda_j f(v_j)$ et $y = \sum_{j \in J} \mu_j f(v_j)$.

La relation $f(x) = f(y)$ donne immédiatement, par la linéarité de f ,

$$\sum_{j \in J} (\lambda_j - \mu_j) f(v_j) = 0. \quad (4.13)$$

Du fait que $\{f(v_i)\}_{i \in I}$ soit une base, nous déduisons que $\lambda_j - \mu_j = 0$ pour tout j . Donc $x = y$, et f est injective.

3. Nous utilisons le fait que l'union de deux parties finies d'un ensemble est finie (lemme 1.104(2)).

Surjective Soit $x \in E$. Vu que $\{f(v_i)\}_{i \in I}$ est une base, il existe des scalaires λ_j tels que

$$x = \sum_{j \in J} \lambda_j f(v_j) = f\left(\sum_{j \in J} \lambda_j v_j\right). \quad (4.14)$$

Donc f est surjective. □

Définition 4.8.

Un espace vectoriel est **de type fini** s'il contient une partie génératrice finie.

Nous verrons dans les résultats qui suivent que cette définition est en réalité inutile parce qu'un espace vectoriel sera de type fini si et seulement s'il est de dimension finie.

Lemme 4.9.

Si E a une famille génératrice de cardinal n , alors toute famille de $n + 1$ éléments est liée.

Démonstration. Nous procédons par récurrence sur n . Pour $n = 1$, nous avons $E = \text{Span}(e)$ et donc si $v_1, v_2 \in E$ nous avons $v_1 = \lambda_1 e, v_2 = \lambda_2 e$ pour certains éléments non nuls λ_1, λ_2 du corps de base. Nous avons donc $\lambda_2 v_1 - \lambda_1 v_2 = 0$. Cela prouve que $\{v_1, v_2\}$ est liée.

Supposons maintenant que le résultat soit vrai pour $k < n$, c'est-à-dire que pour tout espace vectoriel contenant une partie génératrice de cardinal $k < n$, les parties de $k + 1$ éléments sont liées. Soit maintenant un espace vectoriel muni d'une partie génératrice $G = \{e_1, \dots, e_n\}$ de n éléments, et montrons que toute partie $V = \{v_1, \dots, v_{n+1}\}$ contenant $n + 1$ éléments est liée. Dans nos notations nous supposons que les e_i sont des vecteurs distincts et les v_i également. Nous les supposons également tous non nuls. Étant donné que $\{e_i\}$ est génératrice nous pouvons définir les nombres λ_{ij} par

$$v_i = \sum_{k=1}^n \lambda_{ik} e_k \quad (4.15)$$

Vu que

$$v_{n+1} = \sum_{k=1}^n \lambda_{n+1,k} e_k \neq 0, \quad (4.16)$$

quitte à changer la numérotation des e_i nous pouvons supposer que $\lambda_{n+1,n} \neq 0$. Nous considérons les vecteurs

$$w_i = \lambda_{n+1,n} v_i - \lambda_{i,n} v_{n+1}. \quad (4.17)$$

En calculant un peu,

$$w_i = \lambda_{n+1,n} \sum_k \lambda_{i,k} e_k - \lambda_{i,n} \sum_k \lambda_{n+1,k} e_k \quad (4.18a)$$

$$= \sum_{k=1}^{n-1} (\lambda_{n+1,n} \lambda_{i,k} - \lambda_{i,n} \lambda_{n+1,k}) e_k \quad (4.18b)$$

parce que les termes en e_n se sont simplifiés. Donc la famille $\{w_1, \dots, w_n\}$ est une famille de n vecteurs dans l'espace vectoriel $\text{Span}\{e_1, \dots, e_{n-1}\}$; elle est donc liée par l'hypothèse de récurrence. Il existe donc des nombres $\alpha_1, \dots, \alpha_n \in \mathbb{K}$ non tous nuls tels que

$$0 = \sum_{i=1}^n \alpha_i w_i = \sum_{i=1}^n \alpha_i \lambda_{n+1,n} v_i - \left(\sum_{i=1}^n \alpha_i \lambda_{i,n} \right) v_{n+1}. \quad (4.19)$$

Vu que $\lambda_{n+1,n} \neq 0$ et que parmi les α_i au moins un est non nul, nous avons au moins un des produits $\alpha_i \lambda_{n+1,n}$ qui est non nul. Par conséquent (4.19) est une combinaison linéaire nulle non triviale des vecteurs de $\{v_1, \dots, v_{n+1}\}$. Cette partie est donc liée. □

Lemme 4.10.

Soit L une partie libre et G une partie génératrice. Si l'ensemble des parties libres L' telles que $L \subset L' \subset G$ possède un élément maximum⁴, alors cet élément est une base.

Qu'entend-on par « maximale » ? La partie B doit être libre, contenir L , être contenue dans G et de plus avoir la propriété que $\forall x \in G \setminus B$, la partie $B \cup \{x\}$ est liée.

Démonstration. D'abord si G est une base, alors toutes les parties de G sont libres et le maximum est $B = G$. Dans ce cas le résultat est évident. Nous supposons donc que G est liée.

La partie $B = \{b_1, \dots, b_l\}$ est libre parce qu'on l'a prise parmi les libres. Montrons que B est génératrice. Soit $x \in G \setminus B$; par hypothèse de maximalité, $B \cup \{x\}$ est liée, c'est-à-dire qu'il existe des nombres λ_i, λ_x non tous nuls tels que

$$\sum_{i=1}^l \lambda_i b_i + \lambda_x x = 0. \quad (4.20)$$

Si $\lambda_x = 0$ alors un de λ_i doit être non nul et l'équation (4.20) devient une combinaison linéaire nulle non triviale des b_i , ce qui est impossible parce que B est libre. Donc $\lambda_x \neq 0$ et

$$x = \frac{1}{\lambda_x} \sum_{i=1}^l \lambda_i b_i. \quad (4.21)$$

Donc tous les éléments de $G \setminus B$ sont des combinaisons linéaires des éléments de B , et par conséquent, G étant génératrice, tous les éléments de E sont combinaisons linéaires d'éléments de B . $\square$

Théorème 4.11 (Théorème de la base incomplète).

Soit E un espace vectoriel de type fini sur le corps $\mathbb{K}$.

- (1) Si L est une partie libre et si G est une partie génératrice contenant L , alors il existe une base B telle que $L \subset B \subset G$.
- (2) Toute partie libre peut être étendue en une base.
- (3) Toutes les bases sont finies et ont même cardinal.
- (4) Si V est un sous-espace vectoriel de E , et si L est une base de V , alors il existe une base E qui contient L .

Démonstration. Point par point.

- (1) Vu que E est de type fini, il admet une partie génératrice G de cardinal fini n . Donc une partie libre est de cardinal au plus n par le lemme 4.9. Soit L , une partie libre contenue dans G (ça existe : par exemple $L = \emptyset$). La partie B maximale libre contenue dans G et contenant L est une base par le lemme 4.10.
- (2) Notons que puisque E lui-même est générateur, le point (1) implique que toute partie libre peut être étendue en une base.
- (3) Soient B et B' , deux bases. En particulier B est génératrice et B' est libre, donc le lemme 4.9 indique que $\text{Card}(B') \leq \text{Card}(B)$. Par symétrie on a l'inégalité inverse. Donc $\text{Card}(B) = \text{Card}(B')$.
- (4) La partie L étant une base de V , elle est en particulier libre dans E . Par le point (2), L peut être étendue en une base.

$\square$

Remarque 4.12.

Le théorème de la base incomplète 4.11(2) est ce qui permet de construire une base d'un espace vectoriel en « commençant par » une base d'un sous-espace. En effet si H est un sous-espace de E alors une base de H est une partie libre de E et donc peut être étendue en une base de E .

4. Encore une fois, à part quelques cas triviaux, il n'est pas clair à ce point que ce maximum existe.

Définition 4.13.

La **dimension** d'un espace vectoriel de type fini est le cardinal⁵ d'une⁶ de ses bases.

Il existe une infinité de bases de $\mathbb{R}^m$. On peut démontrer que le cardinal de toute base de $\mathbb{R}^m$ est m , c'est-à-dire que toute base de $\mathbb{R}^m$ possède exactement m éléments.

Exemple 4.14.

La base de **canonique** de $\mathbb{R}^m$ est la partie $\{e_1, \dots, e_m\}$, où le vecteur e_j est

$$e_j = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \leftarrow j\text{-ème} \quad .$$

La composante numéro j de e_i est 1 si $i = j$ et 0 si $i \neq j$. Cela s'écrit $(e_i)_j = \delta_{ij}$ où δ est le **symbole de Kronecker** défini par

$$\delta_{ij} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases} \quad (4.22)$$

Les éléments de la base canonique de $\mathbb{R}^m$ peuvent donc être écrits $e_i = \sum_{k=1}^m \delta_{ik} e_k$. $\triangle$

Le théorème suivant est essentiellement une reformulation du théorème 4.11.

Théorème 4.15.

Soit E un espace vectoriel de dimension finie et $\{e_i\}_{i \in I}$ une partie génératrice de E .

- (1) Il existe $J \subset I$ tel que $\{e_i\}_{i \in J}$ est une base. Autrement dit : de toute partie génératrice nous pouvons extraire une base.
- (2) Soit $\{f_1, \dots, f_l\}$ une partie libre. Alors nous pouvons la compléter en utilisant des éléments e_i . C'est-à-dire qu'il existe $J \subset I$ tel que $\{f_k\} \cup \{e_i\}_{i \in J}$ soit une base.

Proposition 4.16.

Si E est un espace vectoriel de dimension finie n , alors

- (1) toute partie contenant $n + 1$ éléments est liée.
- (2) toute partie libre contenant n éléments est une base,
- (3) toute partie génératrice contenant n éléments est une base.

Démonstration. Soit une partie M contenant $n + 1$ éléments. L'espace E possède une partie génératrice contenant n éléments (n'importe quelle base). Donc M est liée par le lemme 4.9.

Une partie libre contenant n éléments peut être étendue en une base ; si ladite extension est non triviale (c'est-à-dire qu'on ajoute vraiment au moins un élément) une telle base contiendra une partie de $n + 1$ éléments qui serait liée par le lemme 4.9.

Pour la dernière assertion, soit une partie génératrice $\{v_i\}_{i \in I}$ où I contient n éléments. Par le théorème 4.15(1) nous pouvons en extraire une base : il existe $J \subset I$ tel que $\{v_j\}_{j \in J}$ soit une base. Si l'inclusion $J \subset I$ était stricte, alors la base $\{v_j\}_{j \in J}$ contiendrait moins de n éléments, ce qui serait en contradiction avec le théorème 4.11(3). $\square$

Définition 4.17.

Soit F un sous-espace vectoriel de l'espace vectoriel E . La **codimension** de F dans E est

$$\text{codim}_E(F) = \dim(E/F). \quad (4.23)$$

5. Définition 1.103.

6. Le théorème de la base incomplète 4.11(3) montre que cette définition ne souffre d'aucune ambiguïté.

⚠ Avertissement/question à la lectrice !! 4.18

Voir que E/F a une structure vectorielle, expliciter sa dimension en fonction de celles de E et F .

4.1.1 Et en dimension infinie

Dans ZFC, en dimension infinie, il existe aussi une base pour tout espace vectoriel ainsi qu'un théorème de la base incomplète. Nous ne parlerons pas de ce qu'il se passe lorsque nous ne considérons que ZF⁷.

Lemme 4.19 ([97]).

Soient un $\mathbb{K}$ -espace vectoriel E et un sous-espace vectoriel V de E . Soient encore deux sous-espaces vectoriels W_1 et W_2 tels que

$$(1) \quad V \cap W_1 = \{0\};$$

$$(2) \quad V + W_2 = E.$$

Alors il existe un supplémentaire W de V tel que $W_1 \subset W \subset W_2$.

Juste une remarque : dans le Frido le symbole « $\subset$ » ne signifie pas une inclusion stricte.

Démonstration. Nous divisons en petits morceaux.

Un gros ensemble Soit $\mathcal{A}$ l'ensemble des sous-espaces vectoriels S de E tels que $W_1 \subset S \subset W_2$ et $S \cap V = \{0\}$. Vu que $W_1 \subset \mathcal{A}$, cet ensemble n'est pas vide. De plus $\mathcal{A}$ est partiellement ordonné pour l'inclusion.

$\mathcal{A}$ est inductif Nous prouvons maintenant que $\mathcal{A}$ est inductif⁸. Pour cela, soit une partie $\mathcal{A}'$ totalement ordonnée et $U = \bigcup_{A \in \mathcal{A}'} A$.

Alors, la partie U est un sous-espace vectoriel de E . En effet si $x, y \in U$, alors il existe $A_1, A_2 \in \mathcal{A}'$ tels que $x \in A_1$ et $y \in A_2$. Vu que $\mathcal{A}'$ est totalement ordonné, l'un des ensembles parmi A_1 et A_2 est inclus dans l'autre. Sans perdre de généralité, disons $A_1 \subset A_2$. Alors les opérations s'effectuent dans A_2 : nous avons $x, y \in A_2$, et donc $\lambda x \in A_2 \subset U$ ainsi que $x + y \in A_2 \subset U$.

De plus, U contient W_1 , et est contenu dans W_2 . Ainsi, $U \in \mathcal{A}$ et majore $\mathcal{A}'$ pour l'inclusion. En bref, $\mathcal{A}$ est bien inductif.

Utilisation de Zorn Le lemme de Zorn 1.17 nous donne alors un maximum W de $\mathcal{A}$. Ce maximum vérifie

$$(1) \quad W \cap V = \{0\},$$

$$(2) \quad W_1 \subset W \subset W_2,$$

$$(3) \quad \text{pour tout } W' \in \mathcal{A}, \text{ nous avons } W' \subset W \text{ parce que } W \text{ est maximum.}$$

Supplémentaire Montrons que ce W est un supplémentaire de V . Soit $x \in E$. Le but est de trouver une décomposition de x en somme d'un élément de W et un de V . Vu que $V + W_2 = E$ nous avons $v \in V$ et $w_2 \in W_2$ tels que

$$x = v + w_2. \quad (4.24)$$

Si $w_2 \in W$ alors c'est fait. Sinon ...

Soit $X = \text{Span}\{W, w_2\}$. Vu que X contient strictement W et que W est maximum dans $\mathcal{A}$, la partie X n'est pas un élément de $\mathcal{A}$. Vu que X est un sous-espace vectoriel de E tel que $W_1 \subset X \subset W_2$, la seule possibilité pour que X ne soit pas dans $\mathcal{A}$ est que $X \cap V \neq \{0\}$. Soit donc $y \neq 0$ dans $X \cap V$. Par définition de X ,

$$y = w' + \lambda w_2 \quad (4.25)$$

7. Si vous ne savez pas ce que signifient les sigles « ZF » et « ZFC » vous ne devriez pas être en train de lire ceci, et encore moins penser à le resservir à un jury d'agrégation.

8. Définition 1.16.

pour $w' \in W$, $w_2 \in W_2$ et $\lambda \in \mathbb{K}$. Nous avons $\lambda \neq 0$, sinon nous aurions $y \in W \cap V$ et donc $y = 0$ puisque W est dans $\mathcal{A}$. La décomposition (4.25) permet alors d'écrire $w_2 = (y - w')/\lambda$ et finalement

$$x = v + \frac{1}{\lambda}(y - w') = \underbrace{v + \frac{1}{\lambda}y}_{\in V} - \underbrace{\frac{1}{\lambda}w'}_{\in W}. \quad (4.26)$$

La somme d'espaces vectoriels $E = V + W$ est donc établie. □

Corolaire 4.20.

Tout sous-espace vectoriel d'un espace vectoriel possède un supplémentaire.

Démonstration. Soit un espace vectoriel E ainsi qu'un sous-espace vectoriel V . Si $V = E$ nous sommes ok. Sinon nous considérons $v \in E \setminus V$ et nous posons $W_1 = \mathbb{K}v$ et $W_2 = E$.

Vu que V et W_1 sont des espaces vectoriels, nous avons $V \cap W_1 = \{0\}$, et vu que $W_2 = E$ nous avons $V + W_2 = E$. Le lemme 4.19 nous donne alors un supplémentaire de V . □

Proposition 4.21 (Base incomplète).

Tout espace vectoriel (non réduit à $\{0\}$) possède une base.

Démonstration. Soit $\mathcal{A}$ l'ensemble des familles libres de E . Il n'est pas vide parce que $\{v\}$ en est une dès que v est non nul dans E . Rapidement :

- l'ensemble $\mathcal{A}$ est ordonné pour l'inclusion,
- si $\mathcal{A}'$ est une partie totalement ordonnée, l'union est un majorant,
- donc $\mathcal{A}$ est inductif,
- soit un maximum F de $\mathcal{A}$.

La partie F est libre parce qu'elle est dans $\mathcal{A}$. Elle est génératrice parce que si v n'est pas dans $\text{Span}(F)$ alors la partie $F \cup \{v\}$ est encore libre, et majore strictement F pour l'inclusion, ce qui n'est pas possible.

Donc F est une base de E . □

Théorème 4.22 (Base incomplète, dimension quelconque).

Soit une partie $\{e_i\}_{i \in I}$ génératrice de l'espace vectoriel E (ici, I est un ensemble quelconque⁹). Soit $I_0 \in I$ tel que $\{e_i\}_{i \in I_0}$ soit libre.

Alors il existe I_1 tel que $I_0 \subset I_1 \subset I$ tel que $\{e_i\}_{i \in I_1}$ soit une base de E .

Note : une telle partie I_0 existe en prenant un singleton. Mais l'existence n'est pas le sujet ici.

Démonstration. Soit $\mathcal{A}$ l'ensemble des parties J de I telles que $I_0 \subset J \subset I$ et telles que $\{e_i\}_{i \in J}$ soit libre.

Encore une fois, $\mathcal{A}$ est inductif pour l'ordre partiel donné par l'inclusion. Soit J un maximum par le lemme de Zorn 1.17. Vu que $J \in \mathcal{A}$, la partie $\{e_i\}_{i \in J}$ est libre. Mais elle est également génératrice parce que si e_k n'est pas dedans, J ne serait pas maximum, étant majorée par $J \cup \{k\}$.

Donc $\{e_i\}_{i \in J}$ engendre tous les e_i avec $i \in I$ et donc tous les éléments de E . □

4.1.2 Espace librement engendré

Définition 4.23 ([98]).

*Soient un ensemble S et un corps $\mathbb{K}$. L'espace vectoriel **librement engendré** sur S , noté $F_{\mathbb{K}}(S)$ est l'ensemble des applications $S \rightarrow \mathbb{K}$ qui sont non-nulles en un nombre fini de points de S .*

Autrement dit, $\sigma : S \rightarrow \mathbb{K}$ est dans $F_{\mathbb{K}}(S)$ si $\{x \in S \text{ tel que } \sigma(x) \neq 0\}$ est fini¹⁰.

9. Un cas d'utilisation intéressant est de poser $I = E$ et $e_i = i$. Pensez-y.

10. Parce que nous l'aimons bien, nous ne résistons pas à faire un renvoi vers la définition 1.95.

Le lemme suivant donne tout son sens à l'expression « librement » engendré. Il dit que $F(S)$ possède une base indexée par S lui-même.

Lemme 4.24.

L'ensemble des applications δ_s données par

$$\begin{aligned} \delta_s : S &\rightarrow \mathbb{K} \\ t &\mapsto \begin{cases} 1 & \text{si } t = s \\ 0 & \text{sinon} \end{cases} \end{aligned} \quad (4.27)$$

avec $s \in S$ forment une base¹¹ de $F(S)$.

Démonstration. Pour prouver que les δ_s sont générateurs, nous considérons $g : S \rightarrow \mathbb{K}$ non nul sur la partie finie $\{s_i\}_{i \in I}$ de S . Alors nous avons

$$g = \sum_{i \in I} g(s_i) \delta_{s_i}. \quad (4.28)$$

Pour prouver que les δ_s forment une partie libre, nous supposons avoir $\lambda_i \in \mathbb{K}$ tels que

$$g = \sum_{i \in I} \lambda_i \delta_{s_i} = 0 \quad (4.29)$$

Soit $j \in I$. Nous avons

$$0 = f(s_j) = \sum_{i \in I} \lambda_i \underbrace{\delta_{s_i}(s_j)}_{=\delta_{ij}} = \lambda_j. \quad (4.30)$$

Donc les coefficients λ_i sont tous nuls, et nous avons prouvé que la partie est libre. $\square$

Il est parfois pratique d'écrire les éléments de $F(S)$ comme sommes « formelles » d'éléments de S . Cela va encore lorsque S est un ensemble n'ayant aucune somme bien définie.

Mais attention : si $S = \mathbb{R}$, l'élément $4 + 7$ de $F(\mathbb{R})$ n'est pas 11. L'élément 11 de $F(\mathbb{R})$ est un élément complètement différent. Bref, il n'est pas judicieux d'écrire les éléments de $F(S)$ comme des combinaisons linéaires d'éléments de S . Pour $x \in S$ il vaut mieux écrire explicitement δ_x que x . La somme $\delta_x + \delta_y$ est parfaitement bien définie dans l'ensemble des applications de S vers $\mathbb{K}$.

4.2 Applications linéaires

Le lien entre matrice et applications linéaires est la définition 4.63 et toutes les propriétés qui s'en suivent.

4.2.1 Définition

Définition 4.25.

Soient des espaces vectoriels E et F sur le corps $\mathbb{K}$. Soit un sous-corps $\mathbb{L}$ de $\mathbb{K}$. Une application $T : E \rightarrow F$ est dite $\mathbb{L}$ -linéaire si

- $T(x + y) = T(x) + T(y)$ pour tout x et y dans E ,
- $T(\lambda x) = \lambda T(x)$ pour tout λ dans $\mathbb{K}$ et x dans E .

Nous noterons $\mathcal{L}_{\mathbb{L}}(E, F)$ l'espace des applications $\mathbb{L}$ -linéaires de E vers F .

Si vous avez bien suivi, les égalités dans la définition 4.25 sont des égalités dans F .

4.26.

Le plus souvent, si E est un espace vectoriel sur $\mathbb{K}$, alors nous ne considérerons que les applications $\mathbb{K}$ -linéaires. Autrement dit, nous écrirons le plus souvent simplement $\mathcal{L}(E, F)$ sans préciser le corps.

Il pourra pourtant arriver que, pour un espace vectoriel sur $\mathbb{C}$, nous considérons les applications seulement $\mathbb{R}$ -linéaires. Ce sera le cas dans le lemme 27.135.

11. Définition 4.5.

Lemme-Définition 4.27.

L'ensemble de toutes les applications linéaires de E vers F est noté $\mathcal{L}(E, F)$ et devient un espace vectoriel sur $\mathbb{K}$ avec les définitions suivantes :

- (1) $(T_1 + T_2)(x) = T_1(x) + T_2(x)$,
- (2) $(\lambda T)(x) = \lambda T(x)$.

Exemple 4.28.

Pour tout b dans $\mathbb{R}$ la fonction $T_b(x) = bx$ est une application linéaire de $\mathbb{R}$ dans $\mathbb{R}$. En effet,

- $T_b(x + y) = b(x + y) = bx + by = T_b(x) + T_b(y)$,
- $T_b(ax) = b(ax) = abx = aT_b(x)$.

De la même façon on peut montrer que la fonction T_λ définie par $T_\lambda(x) = bx$ est une application linéaire de $\mathbb{R}^m$ dans $\mathbb{R}^m$ pour tout λ dans $\mathbb{R}$ et m dans $\mathbb{N}$. $\triangle$

Exemple 4.29.

Soit $m = n$. On fixe λ dans $\mathbb{R}$ et v dans $\mathbb{R}^m$. L'application U_λ de $\mathbb{R}^m$ dans $\mathbb{R}^m$ définie par $U_\lambda(x) = \lambda x + v$ n'est pas une application linéaire lorsque $v \neq 0$, parce que si a est un réel différent de 0 et 1, alors $av \neq v$, d'où

$$U_\lambda(ax) = \lambda(ax) + v \neq a(\lambda x + v) = aU_\lambda(x).$$

 $\triangle$ **Exemple 4.30.**

Soit A une matrice fixée de $\mathcal{M}_{n \times m}$. La fonction $T_A: \mathbb{R}^m \rightarrow \mathbb{R}^n$ définie par $T_A(x) = Ax$ est une application linéaire. En effet,

- $T_A(x + y) = A(x + y) = Ax + Ay = T_A(x) + T_A(y)$,
- $T_A(ax) = A(ax) = a(Ax) = aT_A(x)$.

 $\triangle$ **Lemme 4.31.**

Si une application linéaire est inversible, alors son inverse est linéaire.

Démonstration. Soient une application linéaire inversible $f: V \rightarrow W$, ainsi que $x, y \in V$. Nous avons

$$f(f^{-1}(x) + f^{-1}(y)) = f(f^{-1}(x)) + f(f^{-1}(y)) = x + y = f(f^{-1}(x + y)). \quad (4.31)$$

En prenant f^{-1} des deux côtés, nous trouvons

$$f^{-1}(x) + f^{-1}(y) = f^{-1}(x + y). \quad (4.32)$$

De même :

$$f(\lambda f^{-1}(x)) = \lambda f(f^{-1}(x)) = \lambda x = f(f^{-1}(\lambda x)), \quad (4.33)$$

ce qui nous donne $\lambda f^{-1}(x) = f^{-1}(\lambda x)$. $\square$

On peut observer que, si on identifie $\mathbb{M}(1, \mathbb{R})$ et $\mathbb{R}$, on obtient le premier exemple comme cas particulier.

Définition 4.32 (Quelques ensembles d'applications linéaires).

Soient E et F des espaces vectoriels.

- L'ensemble des applications linéaires de E vers F est noté $\mathcal{L}(E, F)$, comme déjà dit en 4.27.
- Une application linéaire $E \rightarrow E$ est un **endomorphisme** de E . L'ensemble des endomorphismes de E est noté $\text{End}(E)$.
- Un endomorphisme bijectif est un **automorphisme**. L'ensemble des automorphismes de E est noté $\text{Aut}(E)$.

- Une application linéaire bijective $E \rightarrow F$ est un **isomorphisme** d'espace vectoriel. L'ensemble des isomorphismes $E \rightarrow F$ est noté¹² $\text{GL}(E, F)$. Cela est un groupe par le lemme 4.31.

Remarque 4.33.

Les ensembles définis en 4.32 concernent la structure d'espace vectoriel seulement. Lorsque nous verrons la notion d'espace vectoriel normé, nous demanderons de plus la continuité, laquelle n'est pas automatique en dimension infinie. Voir aussi les définitions 11.76.

Définition 4.34.

Si E est un espace vectoriel, si X est un espace vectoriel, et si $f: X \rightarrow E$ est une application, le **noyau** de f est le noyau de f lorsque E est vu comme un groupe pour l'addition¹³, c'est-à-dire la partie

$$\ker(f) = \{x \in X \text{ tel que } f(x) = 0\}. \quad (4.34)$$

Proposition 4.35.

Le noyau d'une application linéaire est un sous-espace vectoriel.

Démonstration. Soit une application linéaire $f: E \rightarrow F$. Si $x, y \in \ker(f)$ et si $\lambda \in \mathbb{K}$ alors

$$f(x + y) = f(x) + f(y) = 0 + 0 = 0, \quad (4.35)$$

donc $x + y \in \ker(f)$ et

$$f(\lambda x) = \lambda f(x) = 0, \quad (4.36)$$

donc $\lambda x \in \ker(f)$. □

Proposition 4.36.

Si E et F sont des espaces vectoriels de dimension n et si $\{e_i\}_{i=1,\dots,n}$ et $\{f_i\}_{i=1,\dots,n}$ sont des bases respectivement de E et F , alors il existe une unique application linéaire $T: E \rightarrow F$ telle que $T(e_i) = f_i$ pour tout i .

Démonstration. En deux parties.

Existence Soit $v \in E$. Vu que $\{e_i\}$ est une base, il se décompose de façon unique en $v = \sum_i v_i e_i$.

Alors définir

$$T(v) = \sum_i v_i f_i \quad (4.37)$$

est une bonne définition et satisfait aux exigences.

Unicité Soient T et U satisfaisant aux exigences. Alors pour tout i nous avons $T(e_i) = U(e_i)$.

Si $v \in E$ s'écrit de la forme $v = \sum_i v_i e_i$ alors la linéarité impose $T(v) = \sum_i v_i T(e_i) = \sum_i v_i U(e_i) = U(v)$. Donc $T = U$. □

Lemme 4.37 ([1]).

Soient des espaces vectoriels V et W de dimension finie. Soient des bases $\{e_i\}$ de V et $\{f_\alpha\}$ de W . Nous posons

$$\begin{aligned} \varphi_{i\alpha}: V &\rightarrow W \\ v &\mapsto v_i f_\alpha \end{aligned} \quad (4.38)$$

où v_i est défini par la décomposition (unique) $v = \sum_i v_i e_i$.

Alors :

- (1) La partie $\{\varphi_{i\alpha}\}$ est une base de $\mathcal{L}(V, W)$.
- (2) Au niveau des dimensions : $\dim(\mathcal{L}(V, W)) = \dim(V) \dim(W)$.

12. Le fait d'utiliser une notation similaire à celle des matrices inversibles n'est pas anodine : le lecteur en est sans doute conscient.

13. Définition 2.28.

Démonstration. Il faut prouver que $\{\varphi_{i\alpha}\}$ est libre et générateur.

Générateur Soit une application linéaire $b: V \rightarrow W$. En décomposant $b(v)$ dans la base $\{f_\alpha\}$, nous définissons $b_\alpha: V \rightarrow \mathbb{K}$ par

$$b(v) = \sum_{\alpha} b_{\alpha}(v) f_{\alpha}. \quad (4.39)$$

Nous posons $b_{\alpha i} = b_{\alpha}(e_i)$. Ainsi,

$$b(v) = \sum_{\alpha} v_i b_{\alpha i} f_{\alpha} = \sum_{\alpha i} b_{\alpha i} \varphi_{i\alpha}(v). \quad (4.40)$$

Donc b peut être écrit comme combinaison linéaire des $\varphi_{i\alpha}$.

Libre Supposons que $\sum_{i\alpha} a_{i\alpha} \varphi_{i\alpha} = 0$ pour certains coefficients $a_{i\alpha} \in \mathbb{K}$. Nous avons, pour tout $v \in V$:

$$0 = \sum_{i\alpha} a_{i\alpha} \varphi_{i\alpha}(v) = \sum_{i\alpha} a_{i\alpha} v_i f_{\alpha}, \quad (4.41)$$

mais comme les f_{α} forment une base, chaque terme de la somme sur α est nul :

$$\sum_i a_{i\alpha} v_i = 0. \quad (4.42)$$

Et comme cela est valable pour tout v et donc pour tout choix de v_i , nous avons $a_{i\alpha} = 0$ pour tout i et pour tout α .

La formule de dimension est simplement la cardinalité de la base trouvée ; c'est la définition 4.13. $\square$

4.2.2 Linéarité et bases

Proposition 4.38 ([99]).

Soient deux espaces vectoriels E et F . Une application linéaire¹⁴ $f: E \rightarrow F$ est injective si et seulement si $\ker\{f\} = \{0\}$.

Démonstration. Nous supposons que f est injective. Si $x \in \ker(f)$, alors $f(x) = 0$. Or f est linéaire, donc $f(0) = 0$. Nous avons donc $f(x) = f(0)$ et donc $x = 0$ parce que f est injective.

Dans l'autre sens, soient x, y tels que $f(x) = f(y)$. Par linéarité de f nous avons $f(x - y) = 0$, et donc $x - y = 0$ parce que $\ker(f) = \{0\}$. Donc $x = y$ et f est injective. $\square$

Proposition 4.39 ([99]).

Soit $f \in \mathcal{L}(E, F)$ où E et F sont deux espaces vectoriels.

- (1) Si f est injective et si $\{v_i\}_{i \in I}$ est libre, alors $\{f(v_i)\}_{i \in I}$ est libre.
- (2) Si f est surjective et si $\{v_i\}_{i \in I}$ est génératrice, alors $\{f(v_i)\}_{i \in I}$ est génératrice.
- (3) Si f est une bijection, alors l'image d'une base par f est une base.

Démonstration. En trois parties.

(1) Nous devons montrer que $\{f(v_j)\}_{j \in J}$ est libre pour tout J fini dans I . Soit donc une partie finie $J \in I$ et des scalaires¹⁵ tels que $\sum_{j \in J} \lambda_j f(v_j) = 0$. La linéarité de f donne¹⁶

$$f\left(\sum_{j \in J} \lambda_j v_j\right) = 0. \quad (4.43)$$

Par injectivité de f nous avons alors $\sum_j \lambda_j v_j = 0$. Vu que les v_j eux-même forment une partie libre, nous avons $\lambda_j = 0$ pour tout $j \in J$.

14. Définition 4.25.

15. Des éléments du corps de base $\mathbb{K}$.

16. Voir les propriétés de la définition 4.25.

(2) Soit $y \in F$. Vu que f est surjective, il existe $x \in E$ tel que $f(x) = y$. Étant donné que $\{v\beta\}_{i \in I}$ est générateur, il existe une partie finie $J \subset I$ et des scalaires $\lambda_j \in \mathbb{K}$ tels que

$$x = \sum_{j \in J} \lambda_j v_j. \quad (4.44)$$

En appliquant f aux deux côtés, et en tenant compte de la linéarité de f ,

$$y = f(x) = \sum_{j \in J} \lambda_j f(v_j), \quad (4.45)$$

ce qui prouve que y est une combinaison linéaire des $f(v_j)$.

(3) Une base est à la fois libre et génératrice et une bijection est à la fois injective et surjective. Les deux premiers points permettent de conclure. □

Corolaire 4.40 ([1]).

Si E et F sont des espaces vectoriels isomorphes de dimensions finies. Alors leurs dimensions sont égales.

Démonstration. Vu que E et F sont isomorphes, il existe une bijection $f: E \rightarrow F$. Par la proposition 4.39(3), l'image d'une base de E est une base de F . Donc les espaces E et F ont des bases contenant le même nombre d'éléments. □

4.2.3 Rang

La proposition 4.41 et le théorème 4.42 sont valables également en dimension infinie; ce sera une des rares incursions en dimension infinie de ce chapitre.

Proposition-Définition 4.41.

*L'image d'une application linéaire est un espace vectoriel. La dimension de cet espace est le **rang** de ladite application linéaire.*

Démonstration. Soit une application linéaire $f: E \rightarrow F$. Nous considérons v, w dans l'image de f ainsi que λ dans le corps de base commun à E et F .

Soient $v_0 \in E$ et $w_0 \in E$ tels que $v = f(v_0)$ et $w = f(w_0)$. Alors $v + w = f(v_0 + w_0)$ et $\lambda v = f(\lambda v_0)$. Donc l'image est bien un espace vectoriel. □

Théorème 4.42 (Théorème du rang).

Soient E et F deux espaces vectoriels (de dimensions finies ou non) et soit $f: E \rightarrow F$ une application linéaire.

Si $(u_s)_{s \in S}$ est une base de $\ker(f)$ et si $(f(v_t))_{t \in T}$ est une base de $\text{Image}(f)$ alors

$$(u_s)_{s \in S} \cup (v_t)_{t \in T} \quad (4.46)$$

est une base de E .

En dimension finie, nous avons en plus la formule suivante :

$$\text{rang}(f) + \dim(\ker f) = \dim E, \quad (4.47)$$

c'est-à-dire que le rang¹⁷ de f est égal à la codimension¹⁸ du noyau.

17. Définition 4.41.

18. Définition 4.17.

Démonstration. Nous devons montrer que

$$(u_s)_{s \in S} \cup (v_t)_{t \in T} \quad (4.48)$$

est libre et générateur.

Soit $x \in E$. Nous définissons les nombres x_t par la décomposition de $f(x)$ dans la base $(f(v_t))$:

$$f(x) = \sum_{t \in T} x_t f(v_t). \quad (4.49)$$

Ensuite le vecteur $x = \sum_t x_t v_t$ est dans le noyau de f , par conséquent nous le décomposons dans la base (u_s) :

$$x - \sum_t x_t v_t = \sum_{s \in S} x_s u_s. \quad (4.50)$$

Par conséquent

$$x = \sum_s x_s u_s + \sum_t x_t v_t. \quad (4.51)$$

En ce qui concerne la liberté nous écrivons

$$\sum_t x_t v_t + \sum_s x_s u_s = 0. \quad (4.52)$$

En appliquant f nous trouvons que

$$\sum_t x_t f(v_t) = 0 \quad (4.53)$$

et donc que les x_t doivent être nuls. Nous restons avec $\sum_s x_s u_s = 0$ qui à son tour implique que $x_s = 0$. $\square$

Un exemple d'utilisation de ce théorème en dimension infinie sera donné dans le cadre du théorème de Fréchet-Riesz, théorème 25.17.

Proposition 4.43 ([100]).

Soit E , un espace vectoriel de dimension finie sur le corps $\mathbb{K}$. Soient V et W des sous-espaces vectoriels de E . Alors

$$\dim(V + W) = \dim(V) + \dim(W) - \dim(V \cap W). \quad (4.54)$$

Démonstration. Nous considérons l'application

$$\begin{aligned} \varphi: V \times W &\rightarrow E \\ (x, y) &\mapsto x + y. \end{aligned} \quad (4.55)$$

C'est une application linéaire dont l'image est $V + W$. Nous avons donc, pour commencer

$$\dim(V + W) = \dim(\text{Image}(\varphi)). \quad (4.56)$$

Nous appliquons à présent le théorème du rang 4.42 à l'application φ :

$$\dim(V + W) = \dim(\text{Image}(\varphi)) \quad (4.57a)$$

$$= \dim(V \times W) - \dim(\ker(\varphi)) \quad (4.57b)$$

$$= \dim(V) + \dim(W) - \dim(\ker(\varphi)). \quad (4.57c)$$

Nous devons maintenant étudier $\ker(\varphi)$. D'abord, $(v, w) \in V \times W$ appartient à $\ker(\varphi)$ si et seulement si $v + w = 0$. Nous avons donc

$$\ker(\varphi) = \{(x, -x) \text{ tel que } x \in V \cap W\}. \quad (4.58)$$

Nous montrons à partir de cela que $\dim(\ker(\varphi)) = \dim(V \cap W)$ en montrant que l'application

$$\begin{aligned} \psi: V \cap W &\rightarrow \ker(\varphi) \\ x &\mapsto (x, -x) \end{aligned} \quad (4.59)$$

est un isomorphisme d'espaces vectoriels. D'abord ψ est injective parce que si $\psi(x) = \psi(y)$, alors $(x, -x) = (y, -y)$ et donc $x = y$. Ensuite, ψ est surjective parce qu'un élément générique de $\ker(\varphi)$ est $(x, -x) = \psi(x)$ avec $x \in V \cap W$. L'application ψ étant un isomorphisme d'espaces vectoriels, nous avons bien $\dim(\ker(\varphi)) = \dim(V \cap W)$. $\square$

Corolaire 4.44.

Soient deux espaces vectoriels E et F de même dimensions finies¹⁹. Pour une application linéaire $f: E \rightarrow F$, les trois conditions suivantes sont équivalentes :

- (1) f est injective ;
- (2) f est surjective ;
- (3) f est bijective.

Démonstration. Si un endomorphisme $f: E \rightarrow E$ est surjectif, alors $\text{rang}(f) = \dim(E)$, ce qui donne, par le théorème du rang 4.42, $\dim(\ker(f)) = 0$, c'est-à-dire que f est injectif.

De la même façon, si f est injective, alors $\dim(\ker(f)) = 0$, ce qui donne $\text{rang}(f) = \dim(E)$ ou encore que f est surjective. $\square$

Exemple 4.45.

Le corolaire 4.44 n'est pas correct en dimension infinie. Par exemple en prenant $f(e_1) = f(e_2) = e_1$ et ensuite $f(e_k) = e_{k-1}$ pour tout $k \geq 2$. Cette application est surjective mais pas injective. $\triangle$

Une conséquence du théorème du rang est que les endomorphismes ont un inverse à gauche et à droite égaux (lorsqu'ils existent). En résumé, ce que le corolaire 4.46 dit est que si $AB = \mathbb{I}$, alors $BA = \mathbb{I}$.

Corolaire 4.46.

Soit un endomorphisme f d'un espace vectoriel de dimension finie. Si f admet un inverse à gauche, alors

- (1) f est bijective,
- (2) f admet également un inverse à droite,
- (3) les inverses à gauche et à droite sont égaux.

Tout cela tient également en remplaçant « gauche » par « droite ».

Démonstration. Soit g , un inverse à gauche de f : $gf = \text{Id}$. Cela implique que f est injective et que g est surjective, et donc qu'elles sont toutes deux bijectives par le corolaire 4.44. Vu que f est bijective, elle admet également un inverse à droite, soit h . Nous avons : $gf = \text{Id}$ et $fh = \text{Id}$.

Alors $gfh = h$ parce que $gf = \text{Id}$, mais également $gfh = g$ parce que $fh = \text{Id}$. Donc $g = h$.²⁰ $\square$

C'est ce corolaire qui nous permet d'écrire f^{-1} sans plus de précisions dès que f est une bijection.

Exemple 4.47 (Pas en dimension infinie).

Tout cela ne fonctionne pas en dimension infinie. Par exemple avec une base $\{e_k\}_{k \in \mathbb{N}}$ nous pouvons considérer l'opérateur

$$f(e_k) = e_{k+1}. \quad (4.60)$$

19. Les deux mots sont importants : les dimensions doivent être égales et finies.

20. C'est le même argument que celui employé pour la preuve du lemme 1.139 (2), à ceci près que nous devons montrer l'existence de l'inverse à droite.

Il est injectif, mais pas surjectif. Si on pose

$$g(e_k) = \begin{cases} e_{k-1} & \text{si } k \geq 1 \\ 0 & \text{si } k = 0 \end{cases} \quad (4.61)$$

alors nous avons $gf = \text{Id}$, mais pas $fg = \text{Id}$ parce que ce $(fg)(e_0) = 0$. $\triangle$

Lemme 4.48.

Si E et F sont des espaces vectoriels et si $f: E \rightarrow F$ est une application linéaire inversible, alors son inverse est également linéaire.

Démonstration. Nous avons $f^{-1}(x + y) = f^{-1}(x) + f^{-1}(y)$. En effet,

$$f(f^{-1}(x) + f^{-1}(y)) = f(f^{-1}(x)) + f(f^{-1}(y)) = x + y. \quad (4.62)$$

De la même façon,

$$f(\lambda f^{-1}(x)) = \lambda x, \quad (4.63)$$

donc $f^{-1}(\lambda x) = \lambda f^{-1}(x)$. $\square$

Proposition 4.49.

Soient un espace vectoriel E de dimension finie, un endomorphisme $f: E \rightarrow E$ et une partie $\{v_i\}_{i \in I}$ tel que $\{f(v_i)\}_{i \in I}$ soit une base.

Alors $\{v_i\}_{i \in I}$ est une base.

Démonstration. Soit $x \in E$. Il existe une partie finie $J \subset I$ et des scalaires λ_j tels que

$$x = \sum_j \lambda_j f(v_j) = f\left(\sum_j \lambda_j v_j\right), \quad (4.64)$$

ce qui prouve que f est surjective. Le corolaire 4.44 nous dit alors que f est une bijection. L'application inverse est également linéaire par le lemme 4.48.

Une application linéaire bijective (comme f^{-1}) transforme une base en une base par la proposition 4.39. Donc

$$f^{-1}(\{f(v_i)\}) \quad (4.65)$$

est une base. $\square$

Proposition 4.50.

Soit un espace vectoriel E de dimension finie et deux applications linéaires $f, g: E \rightarrow E$ telles que $g \circ f = \text{Id}$. Alors f et g sont bijectives.

Démonstration. En plusieurs étapes

f est injective Si $f(x) = f(y)$, alors en appliquant g nous avons

$$g(f(x)) = g(f(y)), \quad (4.66)$$

ce qui donne $x = y$.

f est surjective C'est maintenant le corolaire 4.44.

g est surjective Pour tout $x \in E$ nous avons $g(f(x)) = x$. Donc l'image de $f(E)$ par g est E .

g est injective C'est maintenant le corolaire 4.44. $\square$

Lemme 4.51 ([101]).

Soit une application linéaire $f: E \rightarrow F$.

(1) L'application f est injective si et seulement s'il existe $g: F \rightarrow E$ telle que $g \circ f = \text{Id}|_E$.

(2) L'application f est surjective si et seulement s'il existe $g: F \rightarrow E$ telle que $f \circ g = \text{Id}|_F$.

Démonstration. Nous démontrons séparément les deux affirmations.

- (1) Si f est injective, alors $f: E \rightarrow \text{Image}(f)$ est un isomorphisme. Si V est un supplémentaire de $\text{Image}(f)$ dans F (c'est-à-dire $F = \text{Image}(f) \oplus V$) alors nous pouvons poser $g(x+v) = f^{-1}(x)$ où $x+v$ est la décomposition (unique) d'un élément de F en $x \in \text{Image}(f)$ et $v \in V$. Avec cela nous avons bien $g \circ f = \text{Id}$.
Inversement, s'il existe $g: F \rightarrow E$ telle que $g \circ f = \text{Id}$ alors $f: E \rightarrow E$ doit être injective. Parce que si $f(x) = 0$ avec $x \neq 0$ alors $(g \circ f)(x) = 0 \neq x$.
- (2) Si f est surjective nous pouvons choisir des éléments $x_1, \dots, x_p$ dans E tels que $\{f(x_i)\}$ soit une base de F . Ensuite nous définissons

$$g: F \rightarrow E$$

$$\sum_k a_k f(x_k) \mapsto \sum_k a_k x_k. \quad (4.67)$$

Cela donne $f \circ g = \text{Id}|_F$ parce que si $v \in F$ alors $v = \sum_k v_k f(x_k)$ avec $v_k \in \mathbb{K}$, et nous avons

$$(f \circ g)(v) = \sum_k v_k (f \circ g)(f(x_k)) = f\left(\sum_k v_k x_k\right) = \sum_k v_k f(x_k) = v. \quad (4.68)$$

Inversement, s'il existe $g: F \rightarrow E$ tel que $f \circ g = \text{Id}$ alors f doit être surjective parce que

$$F = \text{Image}(f \circ g) = f(\text{Image}(g)) \subset \text{Image}(f). \quad (4.69)$$

□

4.3 Matrices

Les matrices et les applications linéaires sont deux choses différentes. Une application linéaire²¹ est une application d'un espace vectoriel vers un autre, et une matrice est un simple tableau de nombres sur lesquels nous définissons des opérations, de telle sorte à fournir une structure d'espace vectoriel. Le lien entre ces opérations et les opérations correspondantes sur les applications linéaires sera fait plus tard. Voir la définition 4.63 et ce qui s'en suit.

4.3.1 Définitions

Les notions topologiques sur les espaces de matrices sont pour plus tard, à commencer par la définition 7.125.

Définition 4.52.

Soit un anneau $\mathbb{A}$ ainsi que des entiers m, n strictement positifs. L'ensemble $\mathbb{M}(n \times m, \mathbb{A})$ est l'ensemble des applications

$$\{1, \dots, n\} \times \{1, \dots, m\} \rightarrow \mathbb{A}, \quad (4.70)$$

et est appelé ensemble des **matrices** $n \times m$ sur $\mathbb{A}$.

Si A est une matrice, nous notons A_{ij} au lieu de $A(i, j)$ l'image de (i, j) par l'application A .

Définition 4.53.

Quelques ensembles de matrices particuliers.

- (1) Si $n = m$, alors :
- nous disons que la matrice est **carrée**,
 - nous notons $\mathbb{M}(n, \mathbb{A})$ pour $\mathbb{M}(n \times n, \mathbb{A})$,
 - n est appelée **ordre** de la matrice.

21. Définition 4.25.

(2) Si $n = 1$, alors la matrice est appelée **matrice-ligne**.

(3) Si $m = 1$, alors la matrice est appelée **matrice-colonne**.

4.54.

On note les isomorphismes naturels $\mathbb{M}(1 \times m, \mathbb{A}) \simeq \mathbb{A}^m$ et $\mathbb{M}(n \times 1, \mathbb{A}) \simeq \mathbb{A}^n$.

Lemme-Définition 4.55.

L'ensemble $\mathbb{M}(n \times m, \mathbb{A})$ muni des opérations

Somme $(A + B)_{ij} = A_{ij} + B_{ij}$,

Produit par un scalaire $(\lambda A)_{ij} = \lambda A_{ij}$,

pour tout $A, B \in \mathbb{M}(n \times m, \mathbb{A})$ et $\lambda \in \mathbb{A}$ est un $\mathbb{A}$ -module (définition 1.212).

Lemme-Définition 4.56.

Avec la multiplication

$$\begin{aligned} \mathbb{M}(n \times p, \mathbb{A}) \times \mathbb{M}(p \times m, \mathbb{A}) &\rightarrow \mathbb{M}(n \times m, \mathbb{A}) \\ (A, B) &\mapsto (AB)_{ij} = \sum_{k=1}^p A_{ik} B_{kj}, \end{aligned} \quad (4.71)$$

l'espace $\mathbb{M}(n, \mathbb{K})$ est une $\mathbb{K}$ -algèbre²².

Définition 4.57.

Pour un élément $A \in \mathbb{M}(n \times m, \mathbb{A})$ nous définissons encore

La transposée $A_{ij}^t = A_{ji}$,

La trace $\text{Tr}(A) = \sum_i A_{ii}$.

Remarque 4.58.

Quelques remarques directes sur les définitions.

- (1) La motivation de cette définition pour le produit apparaîtra plus loin, mais le Frido n'étant pas un livre d'introduction, j'imagine que le lecteur a déjà une idée.
- (2) Nous verrons plus loin en 4.6.2 que la définition de transposée d'une application linéaire n'est pas tout à fait évidente ; elle sera la définition 4.135.

Ici nous avons bien défini la transposée d'une matrice, pas d'une application linéaire.

Remarque 4.59.

Quelques remarques à propos de structures supplémentaires.

- (1) Nous utiliserons (presque) tout le temps des matrices à coefficients dans un corps. Il est clair que, si $\mathbb{K}$ est un corps (commutatif), alors $\mathbb{M}(n \times m, \mathbb{K})$ a une structure d'espace vectoriel sur $\mathbb{K}$.
- (2) Par ailleurs, sur les matrices carrées d'ordre n fixé, le produit de deux matrices est bien défini. Ainsi, $\mathbb{M}(n, \mathbb{A})$ se voit conférer une structure d'anneau, dont le neutre pour la multiplication est la matrice carrée $\mathbb{1}_n$ (notée aussi $\mathbb{1}$ lorsqu'il n'y a pas d'ambiguïté sur la taille), donnée par

$$\mathbb{1}_{ij} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{sinon.} \end{cases} \quad (4.72)$$

Il est vite vu que si A est une matrice carrée d'ordre n , alors $A\mathbb{1} = \mathbb{1}A = A$.

Lemme 4.60 ([1]).

Si A, B et C sont des matrices nous avons

- (1) $(AB)^t = B^t A^t$,

22. Définition 1.228.

$$(2) \operatorname{Tr}(ABC) = \operatorname{Tr}(CAB).$$

Démonstration. La première est un simple calcul :

$$(AB)_{ij}^t = (AB)_{ji} = \sum_k A_{jk} B_{ki} = \sum_k A_{kj}^t B_{ik}^t = (B^t A^t)_{ij}. \quad (4.73)$$

Pour la seconde :

$$\operatorname{Tr}(ABC) = \sum_{ikl} A_{ik} B_{kl} C_{li} = \sum_{ikl} C_{li} A_{ik} B_{kl} = \sum_l (CAB)_{ll} = \operatorname{Tr}(CAB). \quad (4.74)$$

□

4.61.

La seconde égalité est importante et est nommée **invariance cyclique** de la trace. Elle sert entre autres nombreuses choses à prouver que la trace d'une matrice d'une application linéaire ne dépend pas de la base choisie. Ce sera la proposition 9.260.

Lemme 4.62.

Soient des matrices $A, B \in \mathbb{M}(n, \mathbb{K})$. Si pour tout $x, y \in \mathbb{K}^n$ nous avons

$$\sum_{ij} A_{ij} x_i y_j = \sum_{ij} B_{ij} x_i y_j \quad (4.75)$$

alors $A = B$.

Démonstration. Il suffit de choisir $x_i = \delta_{ik}$ et $y_j = \delta_{jl}$, et d'effectuer les sommes ; par exemple

$$\sum_{ij} A_{ij} \delta_{ik} \delta_{jl} = \sum_j A_{kj} \delta_{jl} = A_{kl}. \quad (4.76)$$

Après avoir effectué toutes les sommes nous nous retrouvons avec $A_{kl} = B_{kl}$, ce qui signifie $A = B$. □

4.3.2 Identifier matrices et applications linéaires

Voir dans l'index thématique, -2.1.1.

Soient deux espaces vectoriels de dimension finie E, F sur le corps $\mathbb{K}$. Nous considérons les bases²³ $\{e_i\}$ pour E et $\{f_\alpha\}$ pour F .

Définition 4.63.

Nous considérons l'application

$$\begin{aligned} \psi: \mathbb{M}(n \times m, \mathbb{K}) &\rightarrow \mathcal{L}(E, F) \\ A &\mapsto f_A \end{aligned} \quad (4.77)$$

où f_A est définie par

$$f_A(x) = \sum_{i\alpha} A_{\alpha i} x_i f_\alpha \quad (4.78)$$

si x_i sont les coordonnées de $x \in E$ dans la base $\{e_i\}$.

4.64.

Nous allons prouver un certain nombre de résultats montrant que cette application a toutes les propriétés imaginables permettant d'identifier les matrices aux applications linéaires : elle est un isomorphisme pour toutes les structure que vous pouvez raisonnablement imaginer.

²³. C'est le théorème 4.11 qui nous permet de considérer des bases. Et ce théorème ne fonctionne que parce que nous avons supposé une dimension finie.

À cette application ψ il manque cependant une propriété importante : elle n'est pas canonique. Elle dépend des bases choisies. Autrement dit : nous avons à priori autant d'applications ψ différentes qu'il y a de choix de bases sur E et F ²⁴.

Nous allons prouver maintenant quelques résultats montrant que les matrices et les applications linéaires, dans le cas des espaces vectoriels $\mathbb{K}^n$ sont deux présentations de la même chose.

Le fait que ψ est continue sera la proposition 11.75.

4.65.

Lorsque $A \in \mathbb{M}(n, \mathbb{K})$ est une matrice et $x \in \mathbb{K}^n$ un vecteur, nous notons Ax l'élément de $\mathbb{K}^n$ donné par

$$(Ax)_i = \sum_j A_{ij}x_j. \quad (4.79)$$

Autrement dit, $Ax = f_A(x)$.

Cette convention et de nombreuses autres à propos de matrice sera rappelée dans -2.1.

Proposition-Définition 4.66.

Soient deux espaces vectoriels de dimension finie E, F sur le corps $\mathbb{K}$. Nous considérons les bases $\{e_i\}$ pour E et $\{f_\alpha\}$ pour F .

Nous considérons l'application

$$\begin{aligned} \psi: \mathbb{M}(n \times m, \mathbb{K}) &\rightarrow \mathcal{L}(E, F) \\ A &\mapsto f_A \end{aligned} \quad (4.80)$$

où f_A est définie par

$$f_A(x) = \sum_{i\alpha} A_{\alpha i} x_i f_\alpha \quad (4.81)$$

si x_i sont les coordonnées de $x \in E$ dans la base $\{e_i\}$.

Alors

(1) Nous avons

$$f_A(e_i)_\alpha = A_{\alpha i}. \quad (4.82)$$

(2) Nous avons

$$f_A(e_i) = \sum_\alpha A_{\alpha i} f_\alpha. \quad (4.83)$$

(3) Nous avons

$$(f_A(x))_\alpha = \sum_i A_{\alpha i} x_i. \quad (4.84)$$

(4) L'application ψ est une bijection.

Si f est une application linéaire, alors la matrice $\psi^{-1}(f)$ est la **matrice associée** à f dans les bases choisies.

Remarque : les bases ne sont supposées être canoniques en aucun sens du terme. Les dimensions de E et F ne sont pas non plus supposées identiques.

Démonstration. En nous rappelant que $(e_j)_i = \delta_{ij}$ nous avons

$$f_A(e_j) = \sum_{i\alpha} A_{\alpha i} (e_j)_i f_\alpha = \sum_\alpha A_{\alpha j} f_\alpha, \quad (4.85)$$

donc $f_A(e_i)_\alpha = A_{\alpha i}$. Cela prouve la formule du point (1).

Le point (2) est une simple somme sur α de (1).

La formule ((3)) est simplement la composante f_α de la définition 4.81.

24. Bonne question. Est-ce qu'il y a moyen de construire deux choix de bases donnant la même application ψ ? Écrivez-moi si vous savez la réponse.

Prouvons que ψ est injective. Si $f_A = f_B$, nous avons en particulier $f_A(e_i)_\alpha = f_B(e_i)_\alpha$ et donc $A_{\alpha i} = B_{\alpha i}$.

Prouvons que ψ est surjective. Pour cela nous considérons $f \in \mathcal{L}(E, F)$ et nous posons $A_{\alpha i} = f(e_i)_\alpha$. Nous avons alors $f = f_A$ parce que

$$f_A(x) = \sum_{i\alpha} A_{\alpha i} x_i f_\alpha = \sum_{i\alpha} f(e_i)_\alpha x_i f_\alpha = \sum_{\alpha} f\left(\sum_i x_i e_i\right)_\alpha f_\alpha = \sum_{\alpha} f(x)_\alpha f_\alpha = f(x). \quad (4.86)$$

□

La proposition suivante montre que le produit matriciel correspond à la composition d'applications linéaires, pourvu que l'on travaille avec les bases canoniques sur $\mathbb{K}^n$.

Proposition 4.67 ([1]).

Soit un corps commutatif $\mathbb{K}$. Nous considérons des espaces vectoriels E et F munis de bases $\{e_i\}_{i=1,\dots,n}$ et $\{f_\alpha\}_{\alpha=1,\dots,m}$.

L'application déjà définie²⁵

$$\psi: \mathbb{M}(m \times n, \mathbb{K}) \rightarrow \mathcal{L}(E, F) \quad (4.87)$$

est un isomorphisme d'espaces vectoriels.

Démonstration. Le fait que ψ soit une bijection est la proposition 4.66. Nous devons montrer que c'est linéaire.

Pour $\lambda \in \mathbb{K}$ nous avons le calcul

$$\psi(\lambda A)(e_k) = f_{\lambda A}(e_k) = \sum_{\alpha i} (\lambda A)_{\alpha i} \underbrace{(e_k)_i}_{=\delta_{ki}} f_\alpha = \lambda \sum_{\alpha} A_{\alpha k} f_\alpha = \lambda f_A(e_k). \quad (4.88)$$

Donc $\psi(\lambda A) = \lambda \psi(A)$.

Si $A, B \in \mathbb{M}(n, \mathbb{K})$ nous avons de la même façon $f_{A+B} = f_A + f_B$. □

Proposition 4.68.

Soient des espaces vectoriels E , F et G de dimensions n , m et p munis de bases²⁶ $\{e_i\}$, $\{f_i\}$ et $\{g_i\}$. Nous considérons les deux applications

$$\psi: \mathbb{M}(m \times n, \mathbb{K}) \rightarrow \mathcal{L}(E, F) \quad (4.89)$$

et

$$\psi: \mathbb{M}(p \times m, \mathbb{K}) \rightarrow \mathcal{L}(F, G). \quad (4.90)$$

Nous avons

$$f_A \circ f_B = f_{AB} \quad (4.91)$$

pour toutes matrices $A \in \mathbb{M}(p \times m, \mathbb{K})$ et $B \in \mathbb{M}(m \times n, \mathbb{K})$.

Démonstration. Nous considérons les applications linéaires associées à A et B : $f_A: F \rightarrow G$ et $f_B: E \rightarrow F$ et la composée $f_A \circ f_B: E \rightarrow G$. Et puis c'est le calcul :

$$(f_A \circ f_B)(e_k) = f_A\left(\sum_{ij} B_{ij}(e_k)_j f_i\right) \quad (4.92a)$$

$$= \sum_i B_{ik} f_A(f_i) \quad (4.92b)$$

$$= \sum_i B_{ik} \sum_{rs} A_{rs}(f_i)_s g_r \quad (4.92c)$$

$$= \sum_{ir} B_{ik} A_{ri} g_r \quad (4.92d)$$

$$= \sum_r (AB)_{rk} g_r \quad (4.92e)$$

$$= f_{AB}(e_k). \quad (4.92f)$$

25. Notez la position du n et du m . Sachez noter les bornes des sommes écrites dans la démonstration.

26. Avec trois, nous renonçons à utiliser des alphabets différents pour numéroter les éléments des bases.

Donc $f_A \circ f_B = f_{AB}$ comme il se doit. $\square$

Nous pouvons particulariser au cas où $E = F = G$.

Proposition 4.69.

Si E est un espace vectoriel muni d'une base $\{e_i\}$, alors l'application

$$\psi: \mathbb{M}(n, \mathbb{K}) \rightarrow \text{End}(E) \quad (4.93)$$

est un isomorphisme d'algèbre²⁷ et d'anneaux²⁸.

Démonstration. Le fait que ψ soit un isomorphisme d'algèbre est juste la combinaison entre les propositions 4.67 et 4.68.

En ce qui concerne l'isomorphisme d'anneaux, il faut en plus identifier les neutres. Le neutre pour la composition d'applications linéaires est l'application identité et le neutre pour la multiplication de matrices est la matrice identité. Nous devons donc montrer que $\psi(\delta) = \text{Id}$. Juste un calcul :

$$f_\delta(x) = \sum_{ij} \delta_{ij} x_j e_i = \sum_i x_i e_i = x. \quad (4.94)$$

Donc oui, f_δ est l'identité. $\square$

Le fait que ψ est continue sera la proposition 11.75.

Voilà. Soyez bien conscient que l'application ψ dont nous avons beaucoup parlé est surtout intéressante dans le cas des espaces de la forme $\mathbb{K}^n$. Dans ce cas, nous avons une identification canonique entre $\mathbb{M}(n, \mathbb{K})$ et $\text{End}(\mathbb{K}^n)$ qui est un isomorphisme d'anneaux et d'algèbres.

Nous verrons que ce ψ respecte encore les inverses²⁹ et les déterminants³⁰.

4.70.

Il convient de ne pas confondre matrice et application linéaire (bien que nous le ferons sans vergogne). Une matrice est un bête tableau de nombres, tandis qu'une application linéaire est une application entre deux espaces vectoriels vérifiant certaines propriétés.

Cependant si les espaces vectoriels E et F sont munis de bases, alors il y a une application

$$\psi: \mathbb{M}(m \times n, \mathbb{K}) \rightarrow \mathcal{L}(E, F) \quad (4.95)$$

qui a toutes les propriétés imaginables³¹.

Cette application dépend des bases choisies. Il n'y a donc pas de trucs comme « la matrice de telle application linéaire » ou comme « voici une matrice, nous considérons l'application linéaire associée ».

Cependant, sur des espaces comme $\mathbb{R}^n$ ou plus généralement sur $\mathbb{K}^n$, nous avons une base canonique et toute personne raisonnable utilise toujours la base canonique (sauf mention du contraire). Dans ces cas il est sans danger de dire « la matrice associée à telle application linéaire » sans préciser les bases.

Mais si un jour vous utilisez une base autre que la base canonique sur $\mathbb{R}^n$, précisez-le et plutôt deux fois qu'une³².

4.71.

Tant que nous sommes à parler de matrice et d'applications linéaires, les plus acharnés anti-abus de langage³³ remarqueront qu'il n'est pas vrai que « étant donné une base, une application linéaire a une matrice ».

27. Définition 1.228.

28. Définition 1.31

29. Proposition 4.88.

30. Proposition 9.10.

31. Et elle en aura encore plus lorsque nous aurons vus les déterminants.

32. Au passage, non, les coordonnées polaires ne sont pas une base de $\mathbb{R}^2$. C'est un système de coordonnées, et ce n'est pas la même chose.

33. Dont l'auteur de ces lignes fait partie.

En effet, une base est une partie libre et génératrice (définition 4.5). Or une partie d'un ensemble n'est pas muni d'un ordre. Toutes les permutations de colonnes de la matrice sont encore possible d'après l'ordre que l'on met sur les vecteurs de la base.

Encore une fois, la base canonique n'a pas de problèmes parce que les $\{e_i\}$ de $\mathbb{R}^n$ viennent avec un ordre indiscutable. Plus généralement, très souvent, lorsqu'on construit une base, la construction suggère un ordre.

4.3.3 Déterminant

Définition 4.72.

Si $A \in \mathbb{M}(n, \mathbb{K})$ nous définissons le **déterminant** de A par la formule

$$\det(A) = \sum_{\sigma \in S_n} (-1)^\sigma \prod_{i=1}^n A_{i\sigma(i)} \quad (4.96)$$

où la somme est effectuée sur tous les éléments du groupe symétrique³⁴ S_n et où $(-1)^\sigma$ représente la parité de la permutation σ .

En se souvenant que $|S_n| = n!$, nous sommes frappés de stupeur devant le fait que le nombre de termes dans la somme croît de façon factorielle (c'est plus qu'exponentiel, pour info) en la taille de la matrice. Cette formule est donc sans espoir pour une matrice plus grande que 3×3 ou à la rigueur 4×4 à la main. À l'ordinateur, il est possible de monter plus haut, mais pas tellement.

4.3.4 Déterminant en petite dimension

En dimension deux, le déterminant de la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est le nombre

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - cb. \quad (4.97)$$

Ce nombre détermine entre autres le nombre de solutions que va avoir le système d'équations linéaires associé à la matrice.

Pour une matrice 3×3 , nous avons le même concept, mais un peu plus compliqué ; nous avons la formule

$$\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12} \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13} \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}. \quad (4.98)$$

4.3.5 Manipulations de lignes et de colonnes

Nous voudrions savoir ce qu'il se passe avec le déterminant d'une matrice lorsque nous substituons à une ligne ou une colonne une combinaison des autres lignes et colonnes. Lorsque une matrice est donnée, nous notons C_j sa j^{e} colonne.

Lemme 4.73 ([1]).

Si A et B sont des matrices, alors

$$(AB)^t = B^t A^t. \quad (4.99)$$

Démonstration. Il suffit de calculer les éléments de matrice :

$$(AB)_{ij}^t = (AB)_{ji} = \sum_k A_{jk} B_{ki} = \sum_k B_{ik}^t A_{kj}^t = (B^t A^t)_{ij}. \quad (4.100)$$

□

34. Pour le groupe symétrique, c'est la définition 1.146, le fait que ce soit un groupe fini est le lemme 1.148, et pour la somme sur un groupe fini c'est la définition 1.206..

Lemme 4.74 ([1, 102]).

Si A est une matrice, alors $\det(A) = \det(A^t)$.

Démonstration. Nous commençons par écrire la définition du déterminant :

$$\det(A^t) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^n (A^t)_{i, \sigma(i)} = \sum_{\sigma} \epsilon(\sigma) \prod_i A_{\sigma(i), i}. \quad (4.101)$$

Pour chaque σ séparément, nous utilisons la proposition 1.211 pour ré-indexer le produit :

$$\prod_i A_{\sigma(i), i} = \prod_i A_{i, \sigma^{-1}(i)}. \quad (4.102)$$

Nous profitons du fait que l'application $\varphi: S_n \rightarrow S_n$ donnée par $\varphi(\sigma) = \sigma^{-1}$ soit une permutation de S_n pour appliquer la définition 1.206 et faire la somme sur σ^{-1} :

$$\det(A^t) = \sum_{\sigma} \epsilon(\sigma) \prod_i A_{i, \sigma^{-1}(i)} = \sum_{\sigma} \epsilon(\sigma^{-1}) \prod_i A_{i, \sigma(i)} = \det(A) \quad (4.103)$$

où nous avons utilisé le fait que $\epsilon(\sigma^{-1}) = \epsilon(\sigma)$ (corolaire 1.160). $\square$

Le fait que $\det(A) = \det(A^t)$ permet, dans toutes les propositions du type « ce qui arrive au déterminant si on change telle ligne ou colonnes » de ne donner qu'une preuve pour la partie « ligne » et déduire automatiquement le cas « colonne ». Le lemme suivant donne un exemple d'utilisation.

Lemme 4.75 ([1]).

Soit une matrice A . Nous considérons la matrice B obtenue à partir de A par la permutation de lignes $L_k \leftrightarrow L_l$ ainsi que la matrice C obtenue à partir de A^t par la permutation de colonnes $C_k \leftrightarrow C_l$.

Alors $C^t = B$.

Démonstration. Calculons les éléments de matrice de C :

$$C_{ij} = \begin{cases} (A^t)_{ij} & \text{si } j \neq k, j \neq l \\ (A^t)_{ik} & \text{si } j = l \\ (A^t)_{il} & \text{si } j = k \end{cases} = \begin{cases} A_{ji} & \text{si } j \neq k, j \neq l \\ A_{ki} & \text{si } j = l \\ A_{li} & \text{si } j = k. \end{cases} \quad (4.104)$$

Ensuite nous prouvons que $C^t = B$ en écrivant les éléments de C^t :

$$(C^t)_{ij} = C_{ji} = \begin{cases} A_{ij} & \text{si } i \neq k, i \neq l \\ A_{kj} & \text{si } i = l \\ A_{lj} & \text{si } i = k. \end{cases} \quad (4.105)$$

Cette dernière expression est la matrice A après permutation des lignes $L_k \leftrightarrow L_l$, c'est-à-dire la matrice B . $\square$

Pour la suite nous écrivons δ la matrice « identité », c'est-à-dire celle dont les entrées sont précisément les δ_{ik} . Nous écrivons également E_{ij} la matrice contenant de zéros partout sauf en (i, j) où elle a un 1, c'est-à-dire

$$(E_{ij})_{kl} = \delta_{ik} \delta_{jl}. \quad (4.106)$$

Proposition 4.76 (Permuter des lignes ou des colonnes $L_k \leftrightarrow L_l$ [103, 1]).

Soient une matrice $A \in \mathbb{M}(n, \mathbb{K})$, deux entiers $k \neq l$ inférieurs ou égaux à n .

(1) Si B est la matrice obtenue à partir de A en permutant deux lignes ou deux colonnes, alors

$$\det(A) = -\det(B). \quad (4.107)$$

(2) Si B est la matrice obtenue à partir de A par la permutation de lignes $L_k \leftrightarrow L_l$. Alors

$$B = SA \quad (4.108)$$

avec $S = \delta + E_{kl} + E_{lk} - E_{kk} - E_{ll}$.

Autrement dit : la matrice S est une matrice de permutations de lignes.

(3) La matrice S vérifie $\det(S) = -1$

(4) Nous avons

$$\det(SA) = \det(S) \det(A). \quad (4.109)$$

Démonstration. Point par point

(1) pour les colonnes Soient k et l fixés, et considérons la permutation des colonnes C_k et C_l . Nous notons α la permutation (kl) dans S_n (groupe symétrique, définition 1.146). Nous avons

$$B_{ij} = A_{i\alpha(j)}, \quad (4.110)$$

ou encore : $A_{ij} = B_{i\alpha(j)}$. Par définition,

$$\det(A) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^n A_{i\sigma(i)} \quad (4.111)$$

C'est le moment d'utiliser la proposition 1.209 à propos de somme sur des groupes avec $G = S_n$, $h = \alpha$ et

$$f(\sigma) = \epsilon(\sigma) \prod_i A_{i,\sigma(i)}. \quad (4.112)$$

Nous savons que $\epsilon(\alpha) = -1$ et que ϵ est un homomorphisme par la proposition 1.159(1), donc

$$f(\alpha\sigma) = \epsilon(\alpha\sigma) \prod_i A_{i,(\alpha\sigma)(i)} = -\epsilon(\sigma) \prod_i B_{i,\sigma(i)}. \quad (4.113)$$

Avec ça, nous concluons :

$$\det(A) = \sum_{\sigma \in S_n} f(\sigma) = \sum_{\sigma} f(\alpha\sigma) = - \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^n B_{i\sigma(i)} = -\det(B). \quad (4.114)$$

(1) pour les lignes Que se passe-t-il si nous permutons les lignes L_k et L_l ? Si nous notons B' la matrice obtenue à partir de A par la permutation de lignes $L_k \leftrightarrow L_l$, et C celle obtenue de A^t après permutation de colonnes $C_k \leftrightarrow C_l$ alors nous avons $C^t = B'$. Le lemme 4.75 nous dit que $C^t = B'$. En utilisant le lemme 4.74 sur le déterminant de la transposée,

$$\det(B') = \det(C^t) = \det(C) = -\det(A^t) = -\det(A). \quad (4.115)$$

Voilà qui prouve le résultat pour les permutation de lignes.

(2) Si $k = l$, il n'y a pas de permutations, et il est vite vu que la matrice S est l'identité parce qu'il y a quatre fois le terme E_{kk} . Nous supposons donc que $k \neq l$; en particulier $\delta_{kl} = 0$.

Il s'agit surtout d'un beau calcul :

$$(SA)_{ij} = \sum_m S_{im} A_{mj} = A_{ij} + \sum_m (\delta_{ki}\delta_{lm} + \delta_{li}\delta_{lm} - \delta_{ki}\delta_{km} - \delta_{li}\delta_{lm}) A_{mj} \quad (4.116a)$$

$$= A_{ij} + \delta_{ki}A_{lj} + \delta_{li}A_{kj} - \delta_{ki}A_{kj} - \delta_{li}A_{lj}. \quad (4.116b)$$

Si $i \neq j$ et $i \neq l$, alors $(SA)_{ij} = A_{ij}$. Si $i = k$, alors

$$(SA)_{kj} = A_{kj} + A_{lj} - A_{kj} = A_{lj}, \quad (4.117)$$

c'est-à-dire que la k^{e} ligne de SA est la l^{e} ligne de A .

Avec $i = l$ nous obtenons la k^{e} ligne de A .

Tout cela montre que SA est la matrice A dans laquelle les lignes k et l ont été inversées, c'est-à-dire $SA = B$.

(3) En utilisant la définition du déterminant,

$$\det(S) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^n S_{i\sigma(i)} \quad (4.118a)$$

$$= \sum_{\sigma} \epsilon(\sigma) \prod_i (\delta_{i\sigma(i)} + \delta_{ki}\delta_{l\sigma(i)} + \delta_{li}\delta_{k\sigma(i)} - \delta_{ki}\delta_{k\sigma(i)} - \delta_{li}\delta_{l\sigma(i)}). \quad (4.118b)$$

Nous utilisons l'associativité et la commutativité du produit pour séparer les facteurs $i = k$ et $i = l$ des autres :

$$\det(S) = \sum_{\sigma} \epsilon(\sigma) \prod_{\substack{i \neq k \\ i \neq l}} \delta_{i\sigma(i)} (\delta_{k\sigma(k)} + \delta_{l\sigma(k)} - \delta_{k\sigma(k)}) (\delta_{l\sigma(l)} + \delta_{k\sigma(l)} - \delta_{l\sigma(l)}). \quad (4.119)$$

À cause des facteurs $i \neq k$ et $i \neq l$, les σ pour lesquels le tout n'est pas nuls doivent vérifier $\delta_{i\sigma(i)} = 1$ pour tout i différent de k et l . Les deux seuls sont donc $\sigma = \text{Id}$ et la permutation $\sigma = (k, l)$. Pour $\sigma = \text{Id}$, nous avons

$$\prod_{\substack{i \neq k \\ i \neq l}} \delta_{ii} (\delta_{kk} + \delta_{lk} - \delta_{kk}) (\delta_{ll} + \delta_{kl} - \delta_{ll}) = 0. \quad (4.120)$$

Dernier espoir : $\sigma = (k, l)$. Pour ce terme nous avons $\epsilon(\sigma) = -1$ et

$$\prod_{\substack{i \neq k \\ i \neq l}} \delta_{ii} (\delta_{kl} + \delta_{ll} - \delta_{kl}) (\delta_{lk} + \delta_{kk} - \delta_{lk}) = 1. \quad (4.121)$$

Au final dans $\det(S)$ il n'y a de non nul que le terme $\sigma = (k, l)$ et il vaut -1 . Donc

$$\det(S) = -1. \quad (4.122)$$

(4) Il s'agit de mettre bout à bout les points déjà prouvés :

$$\det(SA) = -\det(A) = \det(S) \det(A). \quad (4.123)$$

□

Corolaire 4.77 ([103]).

Soit une matrice $A \in \mathbb{M}(n, \mathbb{K})$. Si deux lignes ou deux colonnes de A sont égales, alors $\det(A) = 0$.

Démonstration. Si deux colonnes sont égales, la matrice ne change pas lorsqu'on les permute, alors que le déterminant change de signes. La seule possibilité est que $\det(A) = -\det(A)$, ce qui signifie que $\det(A) = 0$. □

Notons que si pour $k \neq l$ nous avons $C_k = \lambda C_l$, alors nous avons aussi $\det(A) = 0$.

La réciproque n'est pas vraie : il existe des matrices dont le déterminant est nul et dont aucune entrée n'est nulle. Par exemple

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}. \quad (4.124)$$

Proposition 4.78 ([103]).

Soient $A \in \mathbb{M}(n, \mathbb{K})$, et $v \in \mathbb{K}^n$. Si B est la matrice A avec la substitution $L_j \rightarrow L_j + v$ et C est la matrice A avec la substitution $L_j \rightarrow v$, alors

$$\det(B) = \det(A) + \det(C). \quad (4.125)$$

Démonstration. En utilisant l'associativité de la multiplication,

$$\det(B) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^n B_{i\sigma(i)} \quad (4.126a)$$

$$= \sum_{\sigma} \epsilon(\sigma) \left(\prod_{i \neq j} B_{i\sigma(i)} \right) B_{j\sigma(j)} \quad (4.126b)$$

$$= \sum_{\sigma} \epsilon(\sigma) \left(\prod_{i \neq j} A_{i\sigma(i)} \right) (A_{j\sigma(j)} + v_{\sigma(j)}) \quad (4.126c)$$

$$= \sum_{\sigma} \epsilon(\sigma) \prod_i A_{i\sigma(i)} + \sum_{\sigma} \epsilon(\sigma) \prod_{i \neq j} C_{i\sigma(i)} v_{\sigma(j)} \quad (4.126d)$$

$$= \det(A) + \sum_{\sigma} \epsilon(\sigma) \prod_{i \neq j} C_{i\sigma(i)} C_{j\sigma(j)} \quad (4.126e)$$

$$= \det(A) + \det(C). \quad (4.126f)$$

Justifications :

- 4.126d parce que pour $i \neq j$ nous avons $A_{i\sigma(i)} = C_{i\sigma(i)}$
- 4.126e parce que $v_{\sigma(j)} = C_{j\sigma(j)}$.

□

Proposition 4.79 (Combinaison de lignes ou colonnes $L_k \rightarrow L_k + \lambda L_l$ [103]).

Soient une matrice $A \in \mathbb{M}(n, \mathbb{K})$, deux entiers $k \neq l$ inférieurs ou égaux à n .

- (1) Si B est la matrice obtenue à partir de A par la substitution $L_k \rightarrow L_k + \lambda L_l$ ou $C_k \rightarrow C_k + \lambda C_l$, alors

$$\det(A) = \det(B). \quad (4.127)$$

- (2) Si B est la matrice A dans laquelle nous avons fait la substitution $L_k \rightarrow L_k + \lambda L_l$, alors

$$B = UA \quad (4.128)$$

avec $U = \delta + \lambda E_{kl}$, c'est-à-dire que U est une matrice de combinaison de lignes.

- (3) La matrice U vérifie $\det(U) = 1$.

- (4) Nous avons

$$\det(UA) = \det(U) \det(A). \quad (4.129)$$

Démonstration. Point par point.

- (1) Soit la matrice C obtenue à partir de A par $L_k \rightarrow \lambda L_l$. En considérant le vecteur $v = \lambda L_l$, nous sommes dans la situation de la proposition 4.78. Donc

$$\det(B) = \det(A) + \det(C). \quad (4.130)$$

Mais dans la matrice C , nous avons $L_k = \lambda L_l$, ce qui implique $\det(C) = 0$ par le corolaire 4.77. Donc $\det(A) = \det(B)$ comme il se devait.

- (2) Encore un calcul :

$$(UA)_{ij} = \sum_m (\delta_{im} + \lambda(E_{kl})_{im}) A_{mj} = A_{ij} + \lambda \sum_m \delta_{ki} \delta_{lm} A_{mj} = A_{ij} + \lambda \delta_{li} A_{kj}. \quad (4.131)$$

Cela donne, pour $i = k$ la ligne

$$(UA)_{kj} = A_{kj} + \lambda A_{lj}, \quad (4.132)$$

ce qui correspond bien à $L_k \rightarrow L_k + \lambda L_l$.

(3) Nous calculons le déterminant de $U = \delta + \lambda E_{kl}$ avec $k \neq l$. Nous avons dans un premier temps :

$$\det(U) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^n (\delta_{i\sigma(i)} + \lambda \delta_{ki} \delta_{l\sigma(i)}). \quad (4.133)$$

Vu que nous avons toujours $\delta_{ki} \delta_{li} = 0$, le terme $\sigma = \text{Id}$ donne 1.

Pour les $\sigma \neq \text{Id}$, le facteur $\lambda \delta_{ki} \delta_{l\sigma(i)}$ ne s'annule pas uniquement si $i = k$ et $\sigma(i) = l$. Donc le seul terme non nul autre que $\sigma = \text{Id}$ peut provenir de $\sigma = (k, l)$. Pour ce terme, nous isolons les termes $i = l$ et $i = k$:

$$(\delta_{k\sigma(k)} + \lambda \delta_{kk} \delta_{k\sigma(k)}) (\delta_{l\sigma(l)} + \lambda \delta_{kl} \delta_{k\sigma(l)}). \quad (4.134)$$

Le dernier facteur est nul.

(4) En mettant bout à bout les résultats prouvés,

$$\det(UA) = \det(A) = \det(U) \det(A). \quad (4.135)$$

□

Proposition 4.80 (Multiplication par un scalaire d'une ligne ou colonne $L_k \rightarrow \lambda L_k$ [103]).

Soient une matrice $A \in \mathbb{M}(n, \mathbb{K})$, un entier $k \neq l$ inférieurs ou égal à n . Soit la matrice B obtenue à partir de A en multipliant la ligne L_k par $\lambda \in \mathbb{K}$.

$$(1) \det(B) = \lambda \det(A)$$

$$(2) \text{ En considérant la matrice } T = \delta + (\lambda - 1)E_{kk}, \text{ nous avons}$$

$$B = TA, \quad (4.136)$$

c'est-à-dire que la matrice T est une matrice de multiplication de ligne par un scalaire.

$$(3) \text{ Nous avons } \det(T) = \lambda.$$

$$(4) \text{ Et aussi : } \det(TA) = \det(T) \det(A)$$

Démonstration. Point par point.

(1) La matrice B est donnée par les éléments

$$B_{ij} = \begin{cases} A_{ij} & \text{si } j \neq k \\ \alpha A_{ij} & \text{si } j = kn \end{cases} \quad (4.137)$$

c'est-à-dire $B_{ij} = (1 + (\alpha - 1)\delta_{jk})A_{ij}$. Nous mettons cela dans la définition du déterminant de B :

$$\det(B) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^n B_{i\sigma(i)} = \sum_{\sigma} \prod_i (1 + (\alpha - 1)\delta_{\sigma(i)k} A_{i\sigma(i)}). \quad (4.138)$$

L'associativité du produit dans $\mathbb{K}$ nous permet de séparer le produit de la façon suivante :

$$\prod_{i=1}^n (1 + (\alpha - 1)\delta_{\sigma(i)k} A_{i\sigma(i)}) = \prod_i (1 + (\lambda - 1)\delta_{\sigma(i)k}) \prod_i A_{i\sigma(i)} = \lambda \prod_i A_{i\sigma(i)}. \quad (4.139)$$

En remettant dans (4.138), nous trouvons $\det(B) = \det(A)$.

(2) C'est un cas particulier de la proposition 4.79(2) en prenant $k = l$ et en adaptant le λ .

(3) Nous calculons le déterminant de la matrice $T = \delta + (\lambda - 1)E_{kk}$. La formule du déterminant donne

$$\det(T) = \sum_{\sigma} \epsilon(\sigma) \prod_{i=1}^n (\delta_{i\sigma(i)} + (\lambda - 1)\delta_{ki} \delta_{k\sigma(i)}). \quad (4.140)$$

Si $i \neq \sigma(i)$, alors non seulement $\delta_{i\sigma(i)} = 0$, mais en plus $\delta_{ki}\delta_{k\sigma(i)} = 0$. Donc seul $\sigma = \text{Id}$ reste dans la somme sur $\sigma \in S_n$. Il reste donc

$$\det(T) = \prod_{i=1}^n (1 + (\lambda - 1)\delta_{ki}) = \left(\prod_{i \neq k} 1 \right) (1 + (\lambda - 1)) = \lambda \quad (4.141)$$

où nous avons utilisé encore l'associativité pour isoler le facteur $i = k$.

(4) Il faut mettre bout à bout les résultats déjà faits :

$$\det(TA) = \lambda \det(A) = \det(T) \det(A). \quad (4.142)$$

□

4.3.6 Réduction de Gauss

Nous avons vu les matrices d'opérations élémentaire sur les lignes et colonnes :

- Permutation de lignes $L_k \leftrightarrow L_l : S(n; k, l) = \delta + E_{kl} + E_{lk} - E_{kk} - E_{ll}$, proposition 4.76.
- Combinaisons de lignes $L_k \rightarrow L_k + \lambda L_l : U(n; k, l, \lambda) = \delta + \lambda E_{kl}$, proposition 4.79.
- Multiplication d'une ligne par un scalaire $L_k \rightarrow \lambda L_k : T = \delta + (\lambda - 1)E_{kk}$, proposition 4.80.

Ces matrices seront dans la suite notées G . Et elles vérifient la grosse propriété

$$\det(GA) = \det(G) \det(A) \quad (4.143)$$

pour toute matrice A .

Proposition 4.81 (Réduction de Gauss[1]).

Soit une matrice $A \in \mathbb{M}(n, \mathbb{K})$ de déterminant non nul : $\det(A) \neq 0$. Alors il existe des matrices $G_1, \dots, G_N$ toutes de type S , U ou T telles que

$$G_1 \dots G_N A = \delta. \quad (4.144)$$

Démonstration. Nous faisons une récurrence sur n . D'abord pour $n = 1$, la matrice A contient un seul élément A_{11} qui est non nul par hypothèse. Nous pouvons multiplier sa ligne par $1/A_{11}$ pour obtenir le résultat. Plus précisément, nous avons l'égalité

$$T(1; 1, \frac{1}{A_{11}})A = \delta \quad (4.145)$$

dans $\mathbb{M}(1, \mathbb{K})$. Notons que $\mathbb{K}$ est un corps (donc A_{11} est inversible) commutatif, ce qui permet d'écrire $1/A_{11}$ sans ambiguïtés.

Supposons le résultat prouvé pour n , et voyons ce qu'il se passe pour $n + 1$. Vu que $\det(A) \neq 0$, aucune de ses colonnes n'est nulle (corolaire 4.77). Il existe donc un k tel que $A_{k1} \neq 0$.

Par la proposition 4.76, la matrice

$$B^{(1)} = S(n + 1; k, 1)A \quad (4.146)$$

est une matrice telle que $B_{11}^{(1)} = A_{k1} \neq 0$. Ensuite, par la proposition 4.80 la matrice

$$B^{(2)} = T(n + 1; 1, \frac{1}{A_{k1}})B^{(1)} \quad (4.147)$$

vérifie $B_{11}^{(2)} = 1$.

Vu que la multiplication par la matrice $U(n + 1; k; l; \lambda)$ fait par la proposition 4.79 la substitution $L_k \rightarrow L_k + \lambda L_l$, la matrice

$$B^{(3)} = \prod_{k=2}^{n+1} U(n + 1; k, 1, -B_{k1}^{(1)})B^{(1)} \quad (4.148)$$

a toute sa première colonne nulle à l'exception de $B_{11}^{(3)} = 1$.

Nous n'avons pas donné de nom ni démontré de théorèmes à propos de la substitution $C_k \rightarrow C_k + \lambda C_l$. En passant éventuellement par les transposées et en utilisant les lemmes 4.73 et 4.74 nous obtenons une matrice $U'(n+1; k, l, \lambda)$ ayant la propriété que la matrice

$$B^{(4)} = \prod_{k=2}^{n+1} U'(n+1; k, 1, -B_{1k}^{(3)}) B^{(3)} \quad (4.149)$$

vérifie $B_{1j}^{(4)} = B_{j1}^{(4)} = 0$ pour tout j sauf $j = 1$. En d'autres termes, la matrice $B^{(4)}$ est de la forme

$$B^{(4)} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix} \quad (4.150)$$

où A' est une matrice de taille n .

Voyons quelques propriétés de A' . Nous savons que

$$B^{(4)} = \prod_i G_i A \quad (4.151)$$

où les G_i sont de type S , T ou U . Vu que $\det(SA) = \det(S)\det(A)$ (et idem pour T et U), nous avons

$$\det(B^{(4)}) = \prod_i \det(G_i) \det(A), \quad (4.152)$$

et comme aucun des $\det(G_i)$ n'est nul, nous avons encore $\det(B^{(4)}) \neq 0$, ce qui implique $\det(A') \neq 0$.

La récurrence peut avoir lieu. Il existe des matrices G'_i telles que

$$G'_1 \dots G'_M A' = \delta \quad (4.153)$$

où les G'_i sont de taille n , ainsi que le δ . En remarquant que

$$S(n+1; k, l) = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & S(n; k-1, l-1) & & \\ 0 & & & \end{pmatrix}, \quad (4.154)$$

et pareillement pour les matrices T et U , nous voyons qu'en prenant

$$G_i = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & G'_i & & \\ 0 & & & \end{pmatrix}, \quad (4.155)$$

nous avons

$$\prod_{i=1}^M G_i B^{(3)} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & \prod_{i=1}^M G'_i A' & & \\ 0 & & & \end{pmatrix} = \delta_{n+1} \quad (4.156)$$

où nous avons mis un indice sur le dernier δ pour être plus explicite. □

Proposition 4.82.

Si $A \in \mathbb{M}(n, \mathbb{K})$ est telle que $\det(A) = 0$, alors il existe des matrices de manipulation de lignes et de colonnes $G_1, \dots, G_N$ telles que $G_1 \dots G_N A$ ait une colonne de zéros.

Démonstration. Si la matrice A elle-même n'a pas de colonnes de zéros, alors nous pouvons faire un pas de réduction de Gauss³⁵ et obtenir des matrices $G_1, \dots, G_{N_1}$ telles que

$$G_1 \dots G_{N_1} A = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A^{(1)} & \\ 0 & & & \end{pmatrix}. \quad (4.157)$$

Si $A^{(1)}$ ne possède pas de colonnes de zéros, nous pouvons continuer.

Si nous parvenons à faire n pas de la sorte, alors nous aurions

$$G_1 \dots G_N A = \delta, \quad (4.158)$$

et donc $\det(G_1 \dots G_N) \det(A) = 1$, ce qui est impossible lorsque $\det(A) = 0$. Nous en concluons que le processus doit s'arrêter et qu'une des matrices $A^{(k)}$ doit avoir une colonne de zéros³⁶. $\square$

4.3.7 Matrices inversibles

Proposition-Définition 4.83.

Soit une matrice $A \in \mathbb{M}(n, \mathbb{K})$. Si les matrices B_1 et B_2 de $\mathbb{M}(n, \mathbb{K})$ vérifient

$$AB_1 = B_1A = \delta \quad (4.159)$$

et

$$AB_2 = B_2A = \delta, \quad (4.160)$$

alors $B_1 = B_2$. Dans ce cas, nous disons que A est inversible et nous notons A^{-1} l'unique matrice telle que $AA^{-1} = A^{-1}A = \delta$.

Démonstration. La preuve est réalisée dans le cas général par le lemme 1.139. Mais si vous en voulez une preuve avec les notations d'ici, en voici une.

Nous avons $AB_1 = AB_2$. En multipliant à gauche par B_1 , nous trouvons $B_1AB_1 = B_1AB_2$. En remplaçant B_1A par δ des deux côtés, il reste $B_1 = B_2$. $\square$

Lemme 4.84 ([103]).

Si $A \in \mathbb{M}(n, \mathbb{K})$, alors il existe au plus une matrice $B \in \mathbb{M}(n, \mathbb{K})$ telle que $AB = \delta$.

Démonstration. Soient des matrices $B, C \in \mathbb{M}(n, \mathbb{K})$ telles que $AB = AC = \delta$. Nous allons montrer que $B = C$.

Pour cela nous considérons les applications linéaires $f_A, f_B, f_C \in \text{End}(\mathbb{K}^n)$ associées par la proposition 4.66. Vu que $AB = \delta$, par la proposition 4.68, nous avons $f_A \circ f_B = f_{AB} = \text{Id}$. La proposition 4.50 nous dit alors que f_A et f_B sont bijectives.

En particulier, vu que $\{e_i\}$ est une base, son image par f_B est une base par la proposition 4.39. La proposition 4.49 dit alors que $\{f_B(e_i)\}$ est une base. Nous décomposons $f_B(e_k) - f_C(e_k)$ dans cette base :

$$f_B(e_k) - f_C(e_k) = \sum_j \alpha_j f_B(e_j) \quad (4.161)$$

où les α_j dépendent à priori de k . Vu que $f_A \circ (f_B - f_C) = 0$, nous avons

$$0 = f_A(f_B(e_k) - f_C(e_k)) = \sum_j (f_A \circ f_B)(e_j) = \sum_j \alpha_j e_j. \quad (4.162)$$

Donc les α_j sont tous nuls.

Nous en déduisons que $f_B(e_k) = f_C(e_k)$, et donc $f_B = f_C$. Cela implique que $B = C$ par la proposition 4.66(4). $\square$

35. La réduction de Gauss est le théorème 9.237, mais le lien avec ce que nous disons ici n'est peut-être pas directement clair.

36. En réalité, le processus tel que nous l'avons décrit ne s'arrête que lorsque la première colonne est remplie de zéros.

Proposition 4.85 ([103]).

Si $A, B \in \mathbb{M}(n, \mathbb{K})$ vérifient $AB = \delta$, alors $BA = \delta$.

Démonstration. L'astuce est de poser $C = BA - \delta + B$ et de montrer que $C = B$. Pour cela, un rapide calcul commence par montrer que

$$AC = ABA - A + AB = AB = \delta. \quad (4.163)$$

Donc C est également un inverse à droite de A . Le lemme 4.84 donne alors $C = B$. $\square$

Corolaire 4.86.

Soit $A \in \mathbb{M}(n, \mathbb{K})$. Si il existe $B \in \mathbb{M}(n, \mathbb{K})$ tel que $AB = \delta$, alors A est inversible et son inverse est B .

Démonstration. Il s'agit d'une paraphrase de la proposition 4.85 et de la définition 4.83. $\square$

Lemme 4.87.

Si une matrice A n'est pas inversible, alors le produit AB n'est inversible pour aucune matrice B .

Démonstration. Supposons que AB soit inversible. Alors

$$AB(AB^{-1}) = \delta, \quad (4.164)$$

ce qui dirait que $B(AB^{-1})$ serait un inverse de A . $\square$

Proposition 4.88.

Une matrice est inversible si et seulement si son application linéaire associée est inversible. Dans ce cas, nous avons

$$f_A^{-1} = f_{A^{-1}}. \quad (4.165)$$

Démonstration. Dans le sens direct, si A est inversible nous avons $AA^{-1} = \delta$. Donc

$$f_A \circ f_{A^{-1}} = f_{AA^{-1}} = f_\delta = \text{Id} \quad (4.166)$$

où nous avons utilisé la proposition 4.68 pour la composition et la proposition 4.69 pour l'identité. L'égalité (4.166) indique que f_A est inversible et que son inverse est $f_{A^{-1}}$.

Dans l'autre sens, l'application f_A^{-1} existe. Soit $B \in \mathbb{M}(n, \mathbb{K})$ sa matrice. Alors nous avons

$$f_\delta = \text{Id} = f_A \circ f_B = f_{AB}. \quad (4.167)$$

Le fait que l'application $\psi: A \rightarrow f_A$ soit une bijection³⁷ implique que $AB = \delta$, c'est-à-dire que A est inversible et que $B = A^{-1}$. $\square$

4.3.8 Inversibilité et déterminant**Proposition 4.89.**

Une matrice au déterminant non nul est inversible.

Démonstration. Si A est une matrice telle que $\det(A) \neq 0$, alors la proposition 4.81 nous donne des matrices $G_1, \dots, G_N$ telles que

$$G_1 \dots G_N A = \delta. \quad (4.168)$$

Donc la matrice $G_1 \dots G_N$ est un inverse de A par le corolaire 4.86. $\square$

Proposition 4.90.

Si une matrice A a une ligne ou une colonne de zéros, alors

(1) $\det(A) = 0$,

(2) A n'est pas inversible.

37. Proposition 4.66(4).

Démonstration. Par définition nous avons

$$\det(A) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^n A_{i\sigma(i)}. \quad (4.169)$$

Si la k^{e} ligne est nulle, alors $A_{k\sigma(k)} = 0$ pour tout σ . Donc tous les produits contiennent un facteur nul. Donc $\det(A) = 0$.

Pour toute matrice B nous avons

$$(AB)_{kk} = \sum_l A_{kl} B_{lk}. \quad (4.170)$$

Si la k^{e} ligne de A est nulle nous avons $(AB)_{kk} = 0$ et donc pas $AB = \delta$. Donc A n'est pas inversible. $\square$

Proposition 4.91.

Une matrice dont le déterminant est nul n'est pas inversible.

Démonstration. Par la proposition 4.82, il existe des matrices de manipulation de lignes et de colonnes $G_1, \dots, G_N$ telles que la matrice $G_1 \dots G_N A$ ait une colonne de zéros. De là, la proposition 4.90 implique que la matrice

$$G_1 \dots G_N A \quad (4.171)$$

n'est pas inversible. Vu les déterminants des matrices G_i , la proposition 4.89 implique que $G_1 \dots G_N$ est inversible. Si A était inversible, nous aurions

$$G_1 \dots G_N A A^{-1} (G_1 \dots G_N)^{-1} = \delta, \quad (4.172)$$

c'est-à-dire que $A^{-1} (G_1 \dots G_N)^{-1}$ serait un inverse de la matrice (4.171). Cette dernière n'ayant pas d'inverse, nous concluons que A n'en a pas non plus. $\square$

Théorème 4.92.

Une matrice sur un corps commutatif est inversible si et seulement si son déterminant est non nul.

Démonstration. Dans un sens c'est la proposition 4.89 et dans l'autre sens c'est la proposition 4.91. $\square$

4.3.9 Quelques ensembles de matrices particuliers

Certains ensembles de matrices ont une importance particulière, que nous développerons plus tard.

Définition 4.93 (Groupe linéaire de matrices).

On note $\text{GL}(n, \mathbb{A})$ l'ensemble des matrices carrées d'ordre n à coefficients dans $\mathbb{A}$, qui sont inversibles. En d'autres termes, $\text{GL}(n, \mathbb{A}) = U(\mathbb{M}(n, \mathbb{A}))$.

Définition 4.94 (Groupe orthogonal de matrices).

On dit qu'une matrice A est **orthogonale** si son inverse est sa transposée, c'est-à-dire si $A^{-1} = A^t$. On note $\text{O}(n, \mathbb{A})$ l'ensemble des matrices carrées d'ordre n à coefficients dans $\mathbb{A}$, qui sont orthogonales.

4.3.10 Déterminant et combinaisons de lignes et colonnes

Proposition 4.95.

Soient des matrices $A, B \in \mathbb{M}(n, \mathbb{K})$ telles que $\det(A) \neq 0 \neq \det(B)$. Alors

$$\det(AB) = \det(A) \det(B). \quad (4.173)$$

Démonstration. La proposition 4.81 nous donne des matrices de permutations de lignes et de colonnes $G_1, \dots, G_N$ et $G'_1, \dots, G'_N$ telles que³⁸

$$G_1 \dots G_N A = \delta \quad (4.174a)$$

$$G'_1 \dots G'_N B = \delta. \quad (4.174b)$$

Nous avons

$$(G'_1 \dots G'_N) \underbrace{(G_1 \dots G_N) A B}_{=\delta} = \delta. \quad (4.175)$$

En prenant le déterminant des deux côtés et en tenant compte de (4.143),

$$1 = \det(\delta) = \det(G'_1 \dots G'_N G_1 \dots G_N AB) = \det(G'_1 \dots G'_N) \det(G_1 \dots G_N) \det(AB). \quad (4.176)$$

Mais en même temps, les équations 4.174 donnent

$$\det(G_1 \dots G_N) = \det(A)^{-1} \quad (4.177a)$$

$$\det(G'_1 \dots G'_N) = \det(B)^{-1}. \quad (4.177b)$$

Cela pour dire que

$$1 = \det(A)^{-1} \det(B)^{-1} \det(AB), \quad (4.178)$$

et donc ce qu'il nous fallait. $\square$

Proposition 4.96.

Soient des matrices $A, B \in \mathbb{M}(n, \mathbb{K})$ telles que $\det(A) = 0$ et $\det(B) \neq 0$. Alors

$$\det(AB) = \det(BA) = \det(A) \det(B). \quad (4.179)$$

Démonstration. Il existe des matrices de manipulations de lignes et de colonnes $G_1, \dots, G_N$ telles que $G_1 \dots G_N B = \delta$. Donc

$$0 = \det(A) = \det(G_1 \dots G_N BA) = \det(G_1 \dots G_N) \det(BA). \quad (4.180)$$

Donc $\det(BA) = 0$. $\square$

Proposition 4.97.

Soient des matrices A et B sur un corps commutatif. Alors

$$\det(AB) = \det(A) \det(B). \quad (4.181)$$

Démonstration. Les propositions 4.95 et 4.96 ont déjà fait une grosse partie du travail. Il ne reste que le cas où $\det(A) = \det(B) = 0$.

Dans ce cas, les matrices A et B ne sont pas inversibles (proposition 4.92). Le produit AB n'est alors pas inversible non plus³⁹. La proposition 4.92, utilisée dans le sens inverse, nous dit alors que $\det(AB) = 0$.

Au final dans le cas $\det(A) = \det(B) = 0$ nous avons $0 = \det(AB) = \det(A) \det(B) = 0$. $\square$

Faisons maintenant le cas général des manipulations de lignes et colonnes.

Proposition 4.98.

Soit une matrice carré $A \in \mathbb{M}(n, \mathbb{K})$. La matrice B obtenue par la substitution simultanée

$$C_j \rightarrow \sum_k a_{kj} C_k \quad (4.182)$$

a pour déterminant

$$\det(B) = \det(a) \det(A). \quad (4.183)$$

38. Les plus acharnés préciseront que pour avoir le même N des deux côtés, il a fallu compléter avec des matrices δ là où il y en avait le moins.

39. Citez le lemme 4.87 si vous voulez justifier ça.

Démonstration. L'élément B_{ij} de la matrice B est une combinaison linéaire de tous les éléments de sa ligne :

$$B_{ij} = \sum_k a_{kj} A_{ik} = (Aa)_{ij}. \quad (4.184)$$

Donc $B = Aa$. La proposition 4.97 nous dit alors que $\det(B) = \det(a) \det(A)$. $\square$

4.3.11 Transvections

Nous nommons E_{ij} la matrice remplie de zéros sauf à la case ij qui vaut 1. Autrement dit

$$(E_{ij})_{kl} = \delta_{ik} \delta_{jl}. \quad (4.185)$$

Définition 4.99.

Une **matrice de transvection** est une matrice de la forme

$$T_{ij}(\lambda) = \text{Id} + \lambda E_{ij} \quad (4.186)$$

avec $i \neq j$.

Une **matrice de dilatation** est une matrice de la forme

$$D_i(\lambda) = \text{Id} + (\lambda - 1) E_{ii}. \quad (4.187)$$

Ici le $(\lambda - 1)$ sert à avoir λ et non $1 + \lambda$. C'est donc une matrice qui dilate d'un facteur λ la direction i tout en laissant le reste inchangé.

Si σ est une permutation (un élément du groupe symétrique S_n) alors la **matrice de permutation** associée est la matrice d'entrées

$$(P_\sigma)_{ij} = \delta_{i\sigma(j)}. \quad (4.188)$$

Lemme 4.100.

La matrice $T_{ij}(\lambda)A = (\mathbb{1} + \lambda E_{ij})A$ est la matrice A à qui on a effectué la substitution

$$L_i \rightarrow L_i + \lambda L_j. \quad (4.189)$$

La matrice $AT_{ij}(\lambda)$ est la substitution

$$C_j \rightarrow C_j + \lambda C_i. \quad (4.190)$$

La matrice AP_σ est la matrice A dans laquelle nous avons permuté les colonnes avec σ .

La matrice $P_\sigma A$ est la matrice A dans laquelle nous avons permuté les lignes avec σ^{-1} .

Démonstration. Calculons la composante kl de la matrice $E_{ij}A$:

$$(E_{ij}A)_{kl} = \sum_m (E_{ij})_{km} A_{ml} \quad (4.191a)$$

$$= \sum_m \delta_{ik} \delta_{jm} A_{ml} \quad (4.191b)$$

$$= \delta_{ik} A_{jl}. \quad (4.191c)$$

C'est donc la matrice pleine de zéros, sauf la ligne i qui est donnée par la ligne j de A . Donc effectivement la matrice

$$A + \lambda E_{ij}A \quad (4.192)$$

est la matrice A à laquelle on a substitué la ligne i par la ligne i plus λ fois la ligne j .

En ce qui concerne l'autre assertion sur les transvections, le calcul est le même et nous obtenons

$$(AE_{ij})_{kl} = A_{ki} \delta_{jl}. \quad (4.193)$$

Pour les matrices de permutation, nous avons

$$(AP_\sigma)_{kl} = A_{k\sigma(l)} \quad (4.194)$$

et

$$(P_\sigma A)_{kl} = \sum_m \delta_{k\sigma(m)} A_{ml} = \sum_m \delta_{\sigma^{-1}(k)m} A_{ml} = A_{\sigma^{-1}(k)l}. \quad (4.195)$$

$\square$

4.3.12 Mineur, rang

Pour la définition du rang d'une matrice, nous en donnons une qui est clairement inspirée de l'application linéaire associée.

Définition 4.101 ([103]).

Le **rang** d'une matrice de $\mathbb{M}(n, \mathbb{K})$ est la dimension de la partie de $\mathbb{K}^n$ engendrée par ses colonnes.

Il est possible d'exprimer le rang d'une matrice de façon plus « intrinsèque » via le concept de mineur.

Définition 4.102 ([104]).

Les mineurs d'une matrice sont les déterminants de ses sous-matrices carrées.

Dans la suite nous désignerons souvent par le mot « mineur » la sous-matrice carrée elle-même au lieu de son déterminant.

Lorsque A est une matrice, nous notons f_A l'application linéaire associée à la matrice A par l'application (4.77).

Lemme 4.103.

Soit $\mathbb{K}$ un corps commutatif⁴⁰. Si A est une matrice carrée d'ordre n et de rang r à coefficients dans $\mathbb{K}$, alors il existe des vecteurs $(x_i)_{i=1, \dots, n}$ formant une base de $\mathbb{K}^n$ tels que

$$f_A(x_i) \neq 0 \quad (4.196)$$

pour $x \leq r$ et

$$f_A(x_i) = 0 \quad (4.197)$$

pour $i > r$.

Démonstration. Soit V le sous-espace de $\mathbb{K}^n$ engendré par les colonnes de A . Nous considérons la base canonique $\{e_i\}$ de $\mathbb{K}^n$, ainsi que v_i le vecteur créé par la i^{e} colonne de A . Nous avons

$$v_i = f_A(e_i). \quad (4.198)$$

Les vecteurs v_i engendrent V , donc nous pouvons en extraire une base par le théorème 4.15(1). Soit donc $\{v_j\}_{j \in J}$ une base de V avec $J \subset \{1, \dots, n\}$.

La base de $\mathbb{K}^n$ que nous cherchons commence par les vecteurs $\{e_j\}_{j \in J}$. Ces vecteurs vérifient $f_A(e_j) = v_j \neq 0$ parce que des vecteurs d'une base ne sont jamais nuls.

Pour la suite de la base, nous pourrions penser au théorème de la base incomplète⁴¹, mais les vecteurs ainsi complétant la base ne sont pas garantis de s'annuler par f_A . Voir l'exemple 4.104.

L'idée est d'utiliser le noyau de f_A qui est un sous-espace vectoriel par la proposition 4.35. Soit une base⁴² $\{z_k\}$ de $\ker(f)$. Les vecteurs $\{e_j\}_{j \in J}$ forment une base de $\text{Image}(f_A)$. Vu que les z_i forment une base de $\ker(f_A)$, le théorème du rang 4.42 dit alors que $\{e_j\}_{j \in J} \cup \{z_k\}$ est une base de $\mathbb{K}^n$.

Il y a r éléments dans J parce que l'espace engendré par les colonnes de A est de dimension r par hypothèse. Donc il y a $n - r$ éléments dans les z_k pour que le tout ait le bon nombre d'éléments. $\square$

Exemple 4.104.

Soit la matrice

$$A = \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}. \quad (4.199)$$

Elle est de rang 1. En suivant l'idée de la démonstration, nous commençons la base de $\mathbb{R}^2$ par le vecteur e_1 qui vérifie

$$f_A(e_1) = \begin{pmatrix} 1 \\ 2 \end{pmatrix}. \quad (4.200)$$

40. Comme toujours.

41. Théorème 4.11(2).

42. Cette base contient $n - r$ éléments, mais ce n'est pas très important pour la suite.

L'utilisation du théorème de la base incomplète ne permet pas de trouver un second vecteur de base v tel que $f_A(v) = 0$. En effet ce théorème donne juste l'existence d'une completion de la base, mais pas de propriétés particulières de la base obtenue. Elle pourrait donner $v = e_2$ comme second vecteur de base. Mais alors

$$f_A(v) = f_A(e_2) = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \neq 0. \quad (4.201)$$

Au contraire, le noyau de f_A est donné par le sous-espace engendré par $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$. Une base convenable est donc $\{e_1, e_1 - e_2\}$. $\triangle$

Proposition 4.105.

Le rang d'une application linéaire⁴³ est égal au rang de sa matrice⁴⁴ dans n'importe quelle base.

4.3.13 Matrices équivalentes et semblables

Définition 4.106.

Deux relations d'équivalence entre les matrices.

- (1) Deux matrices A et B sont **équivalentes** dans $\mathbb{M}(n, \mathbb{K})$ s'il existe $P, Q \in \text{GL}(n, \mathbb{K})$ telles que $A = PBQ^{-1}$.
- (2) Deux matrices sont **semblables** s'il existe une matrice $P \in \text{GL}(n, \mathbb{K})$ telle que $A = PBP^{-1}$.

Lemme 4.107.

Une matrice de rang⁴⁵ r dans $\mathbb{M}(n, \mathbb{K})$ est équivalente à la matrice par blocs

$$J_r = \begin{pmatrix} \mathbb{1}_r & 0 \\ 0 & 0 \end{pmatrix}. \quad (4.202)$$

Démonstration. Nous devons prouver que pour toute matrice $A \in \mathbb{M}(n, \mathbb{K})$ de rang r , il existe $P, Q \in \text{GL}(n, \mathbb{K})$ telles que $QAP = J_r$. Soit $\{e_i\}$ la base canonique de $\mathbb{K}^n$, puis $\{f_i\}$ une base telle que $Af_i = 0$ dès que $i > r$, qui existe par le lemme 4.103.

Nous considérons la matrice inversible P telle que $Pe_i = f_i$; ses colonnes sont donc précisément les f_i , si bien que

$$APe_i = Af_i = \begin{cases} 0 & \text{si } i > r \\ \neq 0 & \text{sinon.} \end{cases} \quad (4.203)$$

La matrice AP se présente donc sous la forme

$$AP = \begin{pmatrix} M & 0 \\ * & 0 \end{pmatrix} \quad (4.204)$$

où M est une matrice $r \times r$. Nous considérons maintenant une base $\{g_i\}_{i=1, \dots, n}$ dont les r premiers éléments sont les r premières colonnes de AP et une matrice inversible Q telle que $Qg_i = e_i$. Alors

$$QAPe_i = \begin{cases} e_i & \text{si } i < r \\ 0 & \text{sinon.} \end{cases} \quad (4.205)$$

Cela signifie que QAP est la matrice J_r . $\square$

Corolaire 4.108 (Équivalence et rang).

Deux matrices sont équivalentes⁴⁶ si et seulement si elles sont de même rang.

43. Définition 4.41.

44. Définition 4.101.

45. Définition 4.101.

46. Définition 4.106(1).

Démonstration. D'abord il y a des implicites dans l'énoncé. Vu que nous voulons soit par hypothèse soit par conclusion que les matrices A et B soient équivalentes, nous supposons qu'elles ont même dimension. Soient donc A et B deux matrices carrées d'ordre n .

Par le lemme 4.107, deux matrices de même rang r sont équivalentes à J_r . Elles sont donc équivalentes entre elles.

Inversement, supposons que A et B soient deux matrices équivalentes : $A = PBQ^{-1}$ avec P et Q inversibles. Alors

$$\text{Image}(PBQ^{-1}) = \{PBQ^{-1}v \text{ tel que } v \in \mathbb{K}^n\} \quad (4.206a)$$

$$= PB \underbrace{\{Q^{-1}v \text{ tel que } v \in \mathbb{K}^n\}}_{=\mathbb{K}^n} \quad (4.206b)$$

$$= P(B(\mathbb{K}^n)). \quad (4.206c)$$

L'ensemble $B(\mathbb{K}^n)$ est un sous-espace vectoriel de $\mathbb{K}^n$. Vu que le rang de P est maximum, la dimension de $P(B(\mathbb{K}^n))$ est la même que celle de $B(\mathbb{K}^n)$. Par conséquent

$$\dim(\text{Image}(PBQ^{-1})) = \dim(B(\mathbb{K}^n)) = \text{rang}(B). \quad (4.207)$$

Le membre de gauche de cela n'est autre que $\text{rang}(A) = \dim(\text{Image}(PBQ^{-1}))$. $\square$

4.3.14 Algorithme des facteurs invariants

Proposition 4.109 (Algorithme des facteurs invariants[79]).

Soit $(\mathbb{A}, \delta)$ un anneau euclidien muni de son stathme et $U \in \mathbb{M}(n \times m, \mathbb{A})$. Alors il existe $d_1, \dots, d_s \in \mathbb{A}^*$ et des matrices $P \in \text{GL}(m, \mathbb{A})$, $Q \in \text{GL}(n, \mathbb{A})$ tels que nous ayons

$$U = P \begin{pmatrix} d_1 & & & 0 \\ & \ddots & & \\ & & d_s & \\ & 0 & & 0 \end{pmatrix} Q \quad (4.208)$$

avec $d_i \mid d_{i+1}$ pour tout i .

Démonstration. Nous allons donner la preuve plus ou moins sous forme d'algorithme.

D'abord si $U = 0$ c'est bon, on a la réponse. Sinon, nous prenons l'élément (i_0, j_0) dont le stathme est le plus petit et nous l'aménon en $(1, 1)$ par les permutations

$$\begin{aligned} C_1 &\leftrightarrow C_{j_0} \\ L_1 &\leftrightarrow L_{i_0} \end{aligned} \quad (4.209)$$

Ensuite nous traitons la première colonne jusqu'à amener des zéros partout en dessous de u_{11} de la façon suivante : pour chaque ligne successivement nous calculons la division euclidienne

$$u_{i1} = qu_{11} + r_i, \quad (4.210)$$

et nous faisons

$$L_i \rightarrow L_i - qL_1, \quad (4.211)$$

c'est-à-dire que nous enlevons le maximum possible et il reste seulement r_i en u_{i1} . Vu que le but est de ne laisser que des zéros dans la première colonne, si le reste n'est pas zéro nous ne sommes pas content⁴⁷. Dans ce cas nous permutons $L_1 \leftrightarrow L_i$, ce qui aura pour effet de strictement diminuer le stathme de u_{11} parce qu'on va mettre en u_{11} le nombre r_i dont le stathme est strictement plus petit que celui de u_{11} .

47. S'il est zéro, nous passons à la ligne suivante

En faisant ce jeu de division euclidienne puis échange, on diminue toujours le stathme de u_{11} , donc ça finit par s'arrêter, c'est-à-dire qu'à un certain moment la division euclidienne de u_{i1} par u_{11} va donner un reste zéro et nous serons content.

Une fois la première colonne ramenée à la forme

$$C_1 = \begin{pmatrix} u_{11} \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad (4.212)$$

nous faisons tout le même jeu avec la première ligne en faisant maintenant des sommes divisions et permutations de colonnes. Notons que ce faisant nous ne changeons plus la première colonne.

En fin de compte nous trouvons une matrice ⁴⁸

$$U = \begin{pmatrix} u_{11} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A & \\ 0 & & & \end{pmatrix} \quad (4.213)$$

Si l'élément u_{11} ne divise pas un des éléments de A , disons a_{ij} , alors nous faisons

$$C_1 \rightarrow C_1 - C_j. \quad (4.214)$$

Cela nous détruit un peu la première colonne, mais ne change pas u_{11} . Nous avons maintenant

$$U = \begin{pmatrix} u_{11} & 0 & \dots & 0 \\ 0 & & & \\ * & & & \\ u_{ij} & & A & \\ * & & & \\ 0 & & & \end{pmatrix} \quad (4.215)$$

Et nous refaisons tout le jeu depuis le début. Cependant lorsque nous allons nous attaquer à la ligne i , u_{11} ne divisera pas u_{ij} , ce qui donnera lieu à une division euclidienne et un échange $L_1 \leftrightarrow L_i$. L'échange consistant à mettre r_i à la place de u_{11} et inversement diminuera encore strictement le stathme. Encore une fois nous allons travailler jusqu'à avoir la matrice sous la forme

$$U = \begin{pmatrix} u_{11} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A & \\ 0 & & & \end{pmatrix}, \quad (4.216)$$

sauf que cette fois le stathme de u_{11} est strictement plus petit que la fois précédente. Si u_{11} ne divise toujours pas tous les éléments de A , nous recommençons encore et encore. En fin de compte nous finissons par avoir une matrice de la forme (4.216) avec u_{11} qui divise tous les éléments de A .

Une fois que cela est fait, il faut continuer en recommençant tout sur la matrice A . Nous avons maintenant

$$U = \begin{pmatrix} u_{11} & & 0 \\ & u_{22} & \\ 0 & & B \end{pmatrix}. \quad (4.217)$$

Sous cette forme nous avons $u_{11} \mid u_{22}$ et u_{11} divise tous les éléments de B . En effet u_{11} divisant tous les éléments de A , il divise toutes les combinaisons de ces éléments. Or tout l'algorithme ne consiste qu'à prendre des combinaisons d'éléments.

Nous finissons donc bien sûr une matrice comme annoncée. De plus n'ayant effectué que des combinaisons de lignes, nous avons seulement multiplié par des matrices inversibles (lemme 4.100).

□

48. Nous nommons toujours par la même lettre U la matrice originale et la modifiée, comme il est d'usage en informatique.

4.4 Changement de base

Soit un espace vectoriel V muni de deux bases $(e_i)_{i=1,\dots,n}$ et $(f_\alpha)_{\alpha=1,\dots,n}$. Les deux bases sont liées entre elles par

$$f_\alpha = \sum_i Q_{i\alpha} e_i. \quad (4.218)$$

Ici Q n'est pas une application linéaire $V \rightarrow V$: Q est seulement un tableau de nombres, donnant les coordonnées des vecteurs f_α dans la base de e_i . Éventuellement Q peut être vu comme une application linéaire $\mathbb{K}^n \rightarrow \mathbb{K}^n$.

Dans la suite nous nommerons Q^{-1} la matrice inverse de Q . Inverse au sens des bêtes tableaux de nombres, sans interprétations en tant qu'application linéaire. De même pour Q^t qui est la transposée de Q .

4.4.1 Changement de base : vecteurs de base

Lemme 4.110.

Soit un espace vectoriel V sur $\mathbb{K}$ ainsi que deux bases $(e_i)_{i=1,\dots,n}$, $(f_\alpha)_{\alpha=1,\dots,n}$ de V liées par $f_\alpha = \sum_i Q_{i\alpha} e_i$. Alors

$$e_i = \sum_\alpha Q_{\alpha i}^{-1} f_\alpha. \quad (4.219)$$

Démonstration. Nous multiplions l'égalité $f_\alpha = \sum_i Q_{i\alpha} e_i$ par le nombre⁴⁹ $Q_{\alpha j}^{-1} \in \mathbb{K}$ et nous sommes sur α :

$$\sum_\alpha Q_{\alpha j}^{-1} f_\alpha = \sum_{i\alpha} (A_{i\alpha} Q_{\alpha j}^{-1}) e_i = e_j. \quad (4.220)$$

□

4.4.2 Changement de base : coordonnées

Proposition 4.111.

Soit un espace vectoriel V sur $\mathbb{K}$. Soient deux bases $(e_i)_{i=1,\dots,n}$ et $(f_\alpha)_{\alpha=1,\dots,n}$ liées par $f_\alpha = \sum_i Q_{i\alpha} e_i$. Nous considérons un même vecteur dans les deux bases : $\sum_i x_i e_i = \sum_\alpha y_\alpha f_\alpha$. Alors

$$(1) \ y_\alpha = \sum_i Q_{\alpha i}^{-1} x_i$$

$$(2) \ x_i = \sum_\alpha Q_{i\alpha} y_\alpha.$$

Démonstration. Soit un vecteur $x \in V$. Il peut être écrit dans les deux bases :

$$x = \sum_i x_i e_i = \sum_\alpha y_\alpha f_\alpha. \quad (4.221)$$

En remplaçant e_i par sa valeur (4.219) nous avons l'égalité

$$\sum_{i\alpha} x_i Q_{\alpha i}^{-1} f_\alpha = \sum_\alpha y_\alpha f_\alpha. \quad (4.222)$$

Vu que les f_α sont linéairement indépendants, l'égalité des sommes donne l'égalité de chacun de termes :

$$y_\alpha = \sum_i x_i Q_{\alpha i}^{-1}. \quad (4.223)$$

En identifiant $x \in V$ au vecteur dans $\mathbb{K}^n$ de ses coordonnées dans la base $\{e_i\}$ nous pouvons écrire

$$y_\alpha = (Q^{-1}x)_\alpha, \quad (4.224)$$

Le point (1) est prouvé.

⁴⁹. Attention à la bonne interprétation de ce nombre : on fait bien référence à l'élément situé en (α, j) de la matrice Q^{-1} , et pas autre chose.

En ce qui concerne le point (2), nous repartons encore de (4.221), mais nous y substituons la définition des f_α :

$$\sum_i x_i e_i = \sum_{\alpha} y_\alpha Q_{i\alpha} e_i. \quad (4.225)$$

Vous voulez des détails ? Allez, une étape de plus que le strict nécessaire : nous écrivons

$$\sum_i (x_i - \sum_{\alpha} y_\alpha Q_{i\alpha}) e_i = 0. \quad (4.226)$$

Par linéarité indépendante des e_i , nous avons annulation de tous les coefficients, c'est à dire

$$x_i = \sum_{\alpha} Q_{i\alpha} y_\alpha, \quad (4.227)$$

comme annoncé. $\square$

4.112.

Attention à l'ordre des indices dans la dernière égalité : la matrice Q vient avec les indices dans l'ordre $i\alpha$, tandis que la matrice Q^{-1} vient avec les indices dans l'ordre opposé : αi . C'est pour cela qu'il est intéressant de noter avec des lettres latines les indices se rapportant à la première base et avec des lettres grecques ceux se rapportant à la seconde base.

4.113.

Les formules de changement de coordonnées de la proposition 4.111 s'écrivent souvent de la façon suivante :

- (1) $y_\alpha = (Q^{-1}x)_\alpha$
- (2) $y = Q^{-1}x$.
- (3) $x_i = (Qy)_i$
- (4) $x = Qy$

Ces égalités reposent sur un petit paquet d'abus de notations qu'il convient de bien comprendre. Ici, x et y sont les éléments de $\mathbb{K}^n$ donnés par les composantes de x dans les bases $\{e_i\}$ et $\{f_\alpha\}$, et Q est vu comme une matrice, un opérateur linéaire sur $\mathbb{K}^n$. Autrement dit, le choix des bases permet d'identifier V avec $\mathbb{K}^n$ et la matrice Q avec l'application linéaire f_Q de la proposition 4.66.

4.4.3 Changement de base : matrice d'une application linéaire

Proposition 4.114.

Soit une application linéaire $t: V \rightarrow V$ de matrices A et B dans les bases $\{e_i\}$ et $\{f_\alpha\}$. Si les bases sont liées par

$$f_\alpha = \sum_i Q_{i\alpha} e_i, \quad (4.228)$$

alors les matrices A et B sont liées par

$$B = Q^{-1}AQ. \quad (4.229)$$

Démonstration. L'hypothèse sur le fait que A et B sont les matrices de t signifie que pour tout $x \in V$,

$$t(x) = \sum_{ij} A_{ji} x_i e_j = \sum_{\alpha\beta} B_{\alpha\beta} y_\beta f_\alpha. \quad (4.230)$$

En remplaçant e_j par son expression (4.219) en termes des f_α et x_i par son expression $x_i = (Qy)_i$ (proposition 4.111), nous avons

$$(By)_\alpha = \sum_{ij\alpha} A_{ji} (Qy)_i Q_{\alpha j}^{-1} f_\alpha \quad (4.231a)$$

$$= \sum_{i\alpha} (Q^{-1}A)_{\alpha i} (Qy)_i f_\alpha \quad (4.231b)$$

$$= \sum_{\alpha} (Q^{-1}AQy)_\alpha f_\alpha. \quad (4.231c)$$

Vu que les f_α forment une base nous en déduisons $Q^{-1}AQy = By$. Et vu que y est un élément quelconque de $\mathbb{K}^n$, nous en déduisons l'égalité de matrices

$$B = Q^{-1}AQ. \quad (4.232)$$

□

Il s'agit bien d'une égalité de matrices, ou à la limite d'applications linéaires sur $\mathbb{K}^n$, et non d'une égalité d'application linéaire sur V .

4.5 Espaces de polynômes

Attention : les polynômes en soi sont définis par la définition 1.240.

Pour chaque $k > 0$ donné nous définissons

$$\mathcal{P}_{\mathbb{R}}^k = \{p : \mathbb{R} \rightarrow \mathbb{R} \mid p : x \mapsto a_0 + a_1x + a_2x^2 + \cdots + a_kx^k, a_i \in \mathbb{R}, \forall i = 0, \dots, k\}. \quad (4.233)$$

Il est facile de se convaincre que la somme de deux polynômes de degré inférieur ou égal à k est encore un polynôme de degré inférieur ou égal à k . En outre il est clair que la multiplication par un scalaire ne peut pas augmenter le degré d'un polynôme. L'ensemble $\mathcal{P}_{\mathbb{R}}^k$ est donc un espace vectoriel muni des opérations héritées de $\mathcal{P}_{\mathbb{R}}$.

La base canonique de l'espace $\mathcal{P}_{\mathbb{R}}^k$ est donné par les monômes $\mathcal{B} = \{x \mapsto x^j \mid j = 0, \dots, k\}$. Le fait que cela soit une base est vraiment facile à démontrer et est un exercice très utile si vous ne l'avez pas encore vu dans un cours précédent.

Nous allons maintenant étudier trois applications linéaires de $\mathcal{P}_{\mathbb{R}}^k$ vers des autres espaces vectoriels

L'isomorphisme canonique $\phi : \mathcal{P}_{\mathbb{R}}^k \rightarrow \mathbb{R}^{k+1}$ Nous définissons ϕ par les relations suivantes

$$\phi(x^j) = e_{j+1}, \quad \forall j \in \{0, \dots, k\}.$$

Cela veut dire que pour tout p dans $\mathcal{P}_{\mathbb{R}}^k$, avec $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_kx^k$, l'image de p par ϕ est

$$\phi(p) = \phi\left(\sum_{j=0}^k a_j x^j\right) = \sum_{j=0}^k a_j e_{j+1}.$$

Exemple 4.115.

Soit $k = 5$ on a

$$\phi(-8 - 7x - 4x^2 + 4x^3 + 2x^5) = \begin{pmatrix} -8 \\ -7 \\ -4 \\ 4 \\ 0 \\ 2 \end{pmatrix}. \quad (4.234)$$

△

Cette application est clairement bijective et respecte les opérations d'espace vectoriel, donc elle est un isomorphisme d'espaces vectoriels. L'existence d'un isomorphisme entre $\mathcal{P}_{\mathbb{R}}^k$ et $\mathbb{R}^{k+1}$ est un cas particulier du théorème qui dit que pour chaque m dans $\mathbb{N}_0$ fixée, tous les espaces vectoriels sur $\mathbb{R}$ de dimension m sont isomorphes à $\mathbb{R}^m$. Vous connaissez peut être déjà ce théorème depuis votre cours d'algèbre linéaire.

La dérivation $d : \mathcal{P}_{\mathbb{R}}^k \rightarrow \mathcal{P}_{\mathbb{R}}^{k-1}$ L'application de dérivation d fait exactement ce qu'on s'attend d'elle

$$d(x^0) = d(1) = 0, \quad d(x^j) = jx^{j-1}, \quad \forall j \in \{1, \dots, k\}.$$

Cette application n'est pas injective, parce que l'image de p ne dépend pas de la valeur de a_0 , donc si deux polynômes sont les mêmes à une constante près ils auront la même image par d .

Exemple 4.116.

Soit $k = 3$ on a

$$d(-8 - 12x + 4x^3) = -12(1) + 4(3x^2) = -12 + 12x^2. \quad (4.235)$$

Noter que $d(-30 - 12x + 4x^3) = d(-8 - 12x + 4x^3)$. Cela confirme, comme mentionné plus haut, que la dérivée n'est pas injective. $\triangle$

L'intégration $I : \mathcal{P}_{\mathbb{R}}^k \rightarrow \mathcal{P}_{\mathbb{R}}^{k+1}$ Nous pouvons définir une application que est «à une constante près» l'application inverse de la dérivation. Cette application est définie sur les éléments de base par

$$I(x^j) = \frac{x^{j+1}}{j+1}. \quad (4.236)$$

Bien entendu la raison d'être et la motivation de cette définition apparaîtra lorsque nous développerons une théorie générale de l'intégration.

Exemple 4.117.

Soit $k = 4$ on a

$$I(6 + 2x + x^2 + x^4) = 6x + x^2 + \frac{x^3}{3} + \frac{x^5}{5}. \quad (4.237)$$

$\triangle$

Remarquez que, étant donné que dans la définition de I nous avons décidé d'intégrer entre zéro et x , tous les polynômes dans $\mathcal{P}_{\mathbb{R}}^{k+1}$ qui sont l'image par I d'un polynôme de $\mathcal{P}_{\mathbb{R}}^k$ ont $a_0 = 0$. Cela veut dire que nous pouvons générer toute l'image de I en utilisant un sous-ensemble de la base canonique de $\mathcal{P}_{\mathbb{R}}^{k+1}$, en particulier $\mathcal{B}_1 = \{x \mapsto x^j \mid j = 1, \dots, k\} \subset \mathcal{B}$ nous suffira. Cela n'est guère surprenant, parce que l'image par une application linéaire d'un espace vectoriel de dimension finie ne peut pas être un espace de dimension supérieure.

Les applications de dérivation et intégration correspondent évidemment à des applications linéaires de $\mathcal{P}_{\mathbb{R}}$ dans lui-même.

L'espace de tous les polynômes étant de dimension infinie, il peut servir de contre-exemple assez simple. Dans la sous-section 11.3.2, nous verrons que toutes les normes ne sont pas équivalentes sur l'espace des polynômes.

4.5.1 Projection et orthogonalité

Proposition 4.118 (Produit scalaire dans $\mathbb{R}^n$).

Si $x, y \in \mathbb{R}^n$, nous définissons

$$x \cdot y = \sum_{i=1}^n x_i y_i. \quad (4.238)$$

Cela est un produit scalaire qui vérifie

Symétrie $X \cdot Y = Y \cdot X$;

Linéarité $(\lambda X + \mu X') \cdot Y = \lambda(X \cdot Y) + \mu(X' \cdot Y)$ pour tout λ et μ dans $\mathbb{R}$;

Défini positif $X \cdot X \geq 0$ et $X \cdot X = 0$ si et seulement si $X = 0$.

Ce produit scalaire est le **produit scalaire** qui sera toujours considéré. C'est de lui qui découle toujours la norme, et la topologie de $\mathbb{R}^n$.

Proposition 4.119.

Soit une application linéaire $A : \mathbb{R}^n \rightarrow \mathbb{R}^n$. Nous considérons le produit scalaire usuel sur $\mathbb{R}^n$. Alors :

(1) Les éléments de matrice de A sont donnés par $A_{ij} = e_i \cdot Ae_j$.

(2) Nous avons la formule $x \cdot Ay = \sum_{kl} A_{kl} x_k y_l$.

Démonstration. Pour Ae_j nous utilisons la formule 4.83 avec des notations plus décontractées : $Ae_j = \sum_k A_{kj}e_k$. Ensuite nous faisons un calcul avec la formule (4.238) :

$$e_i \cdot Ae_j = e_i \cdot \sum_k A_{kj}e_k = \sum_k A_{kj}\delta_{ik} = A_{ij}. \quad (4.239)$$

La seconde formule à prouver est du même tonneau, en utilisant cette fois la formule (4.84) :

$$x \cdot Ay = \sum_k x_k(Ay)_k = \sum_{kl} x_k A_{kl}y_l = \sum_{kl} A_{kl}x_k y_l. \quad (4.240)$$

□

Définition 4.120.

La **norme** du vecteur X , notée $\|X\|$, est définie par

$$\|X\| = \sqrt{X \cdot X} = \sqrt{x^2 + y^2 + z^2} \quad (4.241)$$

si $X = (x, y, z)$. Cette norme sera parfois nommée « norme euclidienne ».

Cette définition est motivée par le théorème de Pythagore. Le nombre $X \cdot X$ est bien la longueur de la « flèche » X . Plus intrigante est la définition suivante :

Définition 4.121.

Deux vecteurs X et Y sont **orthogonaux** si $X \cdot Y = 0$.

Cette définition de l'orthogonalité est motivée par la proposition suivante.

Proposition 4.122.

Si nous écrivons proj_Y l'opération de projection sur la droite qui sous-tend Y , alors nous avons

$$\|\text{proj}_Y X\| = \frac{X \cdot Y}{\|Y\|}. \quad (4.242)$$

Démonstration. Les vecteurs X et Y sont des flèches dans l'espace. Nous pouvons choisir un système d'axe orthogonal tel que les coordonnées de X et Y soient

$$X = \begin{pmatrix} x \\ y \\ 0 \end{pmatrix}, \quad Y = \begin{pmatrix} l \\ 0 \\ 0 \end{pmatrix} \quad (4.243)$$

où l est la longueur du vecteur Y . Pour ce faire, il suffit de mettre le premier axe le long de Y , le second dans le plan qui contient X et Y , et enfin le troisième axe dans le plan perpendiculaire aux deux premiers.

Un simple calcul montre que $X \cdot Y = xl + y \cdot 0 + 0 \cdot 0 = xl$. Par ailleurs, nous avons $\|\text{proj}_Y X\| = x$. Par conséquent,

$$\|\text{proj}_Y X\| = \frac{X \cdot Y}{l} = \frac{X \cdot Y}{\|Y\|}. \quad (4.244)$$

□

Corolaire 4.123.

Si la norme de Y est 1, alors le nombre $X \cdot Y$ est la longueur de la projection de X sur Y .

Démonstration. Poser $\|Y\| = 1$ dans la proposition 4.122.

□

4.6 Dualité

Proposition 4.124.

Si A est la matrice d'une application linéaire, alors le rang de cette application linéaire est égal au rang de A , c'est-à-dire à la taille de la plus grande matrice carrée de déterminant non nul contenue dans A .

Définition 4.125.

Soit E un espace vectoriel sur $\mathbb{K}$.

Une **forme linéaire** sur E est une application linéaire de E sur son corps de base $\mathbb{K}$.

Le **dual algébrique** de E , noté E^* , l'ensemble des formes linéaires sur E . Ainsi, $E^* = \text{GL}(E, \mathbb{K})$.

Nous verrons plus tard qu'en dimension infinie, les applications linéaires ne sont pas toujours continues. Nous définirons donc aussi un concept de dual topologique. Voir la proposition 11.73, la remarque 11.87 et la définition 11.89.

Définition 4.126.

Si E est un espace vectoriel et si $\{e_i\}$ est une base de E , alors nous définissons la **base duale** de E^* par

$$e_i^*(e_j) = \delta_{ij} \quad (4.245)$$

est sa prolongation par linéarité.

Notons que si $v \in E$ est un vecteur, ça n'a aucun sens à priori de parler de v^* . Il s'agit bien de définir toute la base $\{e_i^*\}$ à partir de toute la base $\{e_i\}$.

Lemme 4.127 ([105]).

Soit un espace vectoriel E de dimension finie.

- (1) Si α est une forme linéaire non nulle sur E , alors il existe $x \in E$ tel que $\alpha(x) = 1$.
- (2) Si $x \neq 0$ dans E , il existe une forme linéaire α sur E telle que $\alpha(x) = 1$.

Démonstration. En deux parties.

Pour (1) Vu que α est non nulle nous pouvons considérer $v \in E$ tel que $\alpha(v) \neq 0$. Alors en posant $x = \alpha(v)^{-1}v$, nous avons le résultat.

Pour (2) Soit un vecteur non nul que nous écrivons sous la forme $x = \sum_{i=1}^n x_i e_i$ (pour une certaine base $(e_i)_{i=1, \dots, n}$ de E). Supposons que $x_k \neq 0$. Alors la forme

$$\begin{aligned} \alpha: E &\rightarrow \mathbb{K} \\ y &\mapsto y_k/x_k \end{aligned} \quad (4.246)$$

fait l'affaire.

□

Lemme 4.128.

Soit un espace vectoriel de dimension finie E sur le corps $\mathbb{K}$. Si $(\alpha_1, \dots, \alpha_n)$ est une base de E^* , alors l'application

$$\begin{aligned} \Phi: E &\rightarrow \mathbb{K}^n \\ x &\mapsto (\alpha_1(x), \dots, \alpha_n(x)) \end{aligned} \quad (4.247)$$

est un isomorphisme d'espaces vectoriels.

Démonstration. En deux parties.

Φ est injective Soit $z \in \ker(\Phi)$. Nous avons $\alpha_i(z) = 0$ pour tout i . Si $z \neq 0$, alors le lemme 4.127 dit qu'il existe $\beta \in E^*$ tel que $\beta(z) \neq 0$.

Décomposons ce β dans la base de (α_i) :

$$\beta = \sum_{i=1}^n \beta_i \alpha_i. \quad (4.248)$$

Alors nous avons

$$0 = \beta(z) = \sum_{i=1}^n \beta_i \underbrace{\alpha_i(z)}_{=0} = 0. \quad (4.249)$$

Contradiction. Donc $\ker(\Phi) = \{0\}$ et Φ est injective.

Φ est surjective Les espaces vectoriels E , E^* et $\mathbb{K}^n$ ont tout trois dimension n . Donc Φ est une application linéaire injective entre deux espaces de même dimension. Elle est donc surjective par le corolaire 4.44.

□

Proposition-Définition 4.129 ([105]).

*Soit un espace vectoriel E de dimension finie sur le corps $\mathbb{K}$. Toute base du dual E^* est duale d'une unique base de E . Cette base est dite **préduale**.*

Démonstration. Nous considérons une base $\mathcal{F} = (\alpha_1, \dots, \alpha_n)$ de E^* . Nous devons prouver qu'il existe une unique base de E dont la base duale est $\mathcal{F}$.

Existence Le lemme 4.128 nous indique que l'application

$$\begin{aligned} \Phi: E &\rightarrow \mathbb{K}^n \\ x &\mapsto (\alpha_1(x), \dots, \alpha_n(x)) \end{aligned} \quad (4.250)$$

est un isomorphisme d'espaces vectoriels.

Soit la base canonique de $\mathbb{K}^n : (\epsilon_1, \dots, \epsilon_n)$. Vu que Φ est un isomorphisme, $(\Phi^{-1}(\epsilon_i))_{i=1, \dots, n}$ est une base de E . Nous allons montrer qu'elle est préduale de (α_i) . Nous posons $e_i = \Phi^{-1}(\epsilon_i)$ et nous calculons :

$$\alpha_i(e_j) = \alpha_i(\Phi^{-1}(\epsilon_j)) \quad (4.251a)$$

$$= \Phi(\Phi^{-1}(\epsilon_i))_j \quad (4.251b)$$

$$= (\epsilon_j)_i \quad (4.251c)$$

$$= \delta_{ij} \quad (4.251d)$$

Justifications :

- Pour 4.251b, nous remarquons que $\alpha_i(x) = \Phi(x)_i$.
- Pour 4.251d, nous utilisons le fait que les ϵ_j forment la base canonique de $\mathbb{K}^n$.

Unicité Soit une base préduale (e_i) de (α_i) . Nous avons, par définition, que $\alpha_i(e_j) = \delta_{ij}$. Donc

$$(\alpha_1(e_j), \dots, \alpha_n(e_j)) = \epsilon_j. \quad (4.252)$$

Nous appliquons Φ^{-1} à cette dernière équation pour obtenir $e_j = \Phi^{-1}(\epsilon_j)$. Donc les e_j sont déterminés de façon unique à partir des α_i .

□

4.6.1 Orthogonal

Définition 4.130.

*Soit E , un espace vectoriel, et F une sous-espace de E . L'**orthogonal** de F est la partie $F^\perp \subset E^*$ donnée par*

$$F^\perp = \{\alpha \in E^* \text{ tel que } \forall x \in F, \alpha(x) = 0\}. \quad (4.253)$$

Cette définition d'orthogonal via le dual n'est pas du pur snobisme. En effet, la définition « usuelle » qui ne parle pas de dual,

$$F^\perp = \{y \in E \text{ tel que } \forall x \in F, y \cdot x = 0\}, \quad (4.254)$$

demande la donnée d'un produit scalaire. Évidemment dans le cas de $\mathbb{R}^n$ munie du produit scalaire usuel et de l'identification usuelle entre $\mathbb{R}^n$ et $(\mathbb{R}^n)^*$ via une base, les deux notions d'orthogonal coïncident.

La définition 4.130, au contraire, est intrinsèque : elle ne dépend que de la structure d'espace vectoriel.

Si $B \subset E^*$, on note B° son orthogonal :

$$B^\circ = \{x \in E \text{ tel que } \omega(x) = 0 \forall \omega \in B\}. \quad (4.255)$$

Notons qu'on le note B° et non $B^\perp$ parce qu'on veut un peu s'abstraire du fait que $(E^*)^* = E$. Du coup on impose que B soit dans un dual et on prend une notation précise pour dire qu'on remonte au pré-dual et non qu'on va au dual du dual.

Proposition 4.131.

Soient un espace vectoriel E et un sous-espace vectoriel F . Nous avons

$$\dim F + \dim F^\perp = \dim E. \quad (4.256)$$

Démonstration. Soit $\{e_1, \dots, e_p\}$ une base de F que nous complétons en une base $\{e_1, \dots, e_n\}$ de E par le théorème 4.11. Soit $\{e_1^*, \dots, e_n^*\}$ la base duale. Alors nous prouvons que $\{e_{p+1}^*, \dots, e_n^*\}$ est une base de $F^\perp$.

Déjà c'est une partie libre en tant que partie d'une base.

Ensuite ce sont des éléments de $F^\perp$ parce que si $i \leq p$ et si $k \geq 1$, nous avons $e_{p+k}^*(e_i) = 0$; donc oui, $e_{p+k}^* \in F^\perp$.

Enfin $F^\perp \subset \text{Span}\{e_k^*, k \in \{p+1, \dots, n\}\}$ parce que si $\omega = \sum_{k=1}^n \omega_k e_k^*$, alors $\omega(e_i) = \omega_i$, mais nous savons que si $\omega \in F^\perp$, alors $\omega(e_i) = 0$ pour $i \leq p$. Donc $\omega = \sum_{k=p+1}^n \omega_k e_k^*$. $\square$

La proposition 9.266 donnera une version plus terre à terre de la proposition 4.131 en disant que si nous avons un produit scalaire, alors $V = F \oplus F^\perp$ où $F^\perp$ est cette fois défini comme l'orthogonal pour le produit scalaire.

4.6.2 Transposée : pas d'approche naïve

Il est légitime, si $t: E \rightarrow E$ est une application linéaire, de dire que sa transposée soit l'application linéaire $t^t: E \rightarrow E$ dont la matrice est la matrice transposée de celle de t . Lorsque nous travaillons sur $\mathbb{R}^n$ muni de la base canonique, cela ne pose pas de problèmes et nous pouvons écrire des égalités du type $\langle x, Ay \rangle = \langle A^t x, y \rangle$.

Proposition 4.132 (Matrice transposée et produit scalaire).

Soit une matrice réelle A . En utilisant l'application linéaire associée⁵⁰ $f_A: \mathbb{R}^n \rightarrow \mathbb{R}^n$, nous avons

$$x \cdot f_A(y) = f_{A^t}(x) \cdot y. \quad (4.257)$$

Cette formule est souvent écrite $x \cdot Ay = A^t x \cdot y$ ou $\langle x, Ay \rangle = \langle A^t x, y \rangle$.

Démonstration. Il s'agit d'un calcul utilisant la formule (4.78) et le produit scalaire (4.238) :

$$x \cdot f_A(y) = \sum_i x_i (f_A(y))_i = \sum_i x_i \sum_j A_{ij} y_j = \sum_{ij} A_{ji}^t x_i y_j = \sum_j f_{A^t}(x)_j y_j = f_{A^t}(x) \cdot y. \quad (4.258)$$

$\square$

50. Définition 4.63. Ici nous considérons la base canonique sur $\mathbb{R}^n$

Hélas nous allons voir que cette façon de définir une transposée est mauvaise.

Soit une application linéaire $t: E \rightarrow E$ de matrice A dans la base $\{e_i\}_{i=1,\dots,n}$ et de matrice B dans la base $\{f_\alpha\}_{\alpha=1,\dots,n}$.

Nous nommons t_1 l'application linéaire associée à A^t dans la base $\{e_i\}$ et t_2 l'application linéaire associée à la matrice B^t dans la base $\{f_\alpha\}$. Définir la transposée d'une application linéaire comme étant l'application linéaire associée à la transposée de sa matrice ne sera une bonne définition que si $t_1 = t_2$.

La première chose facile à voir est

$$t_1(e_i)_j = \sum_k (A^t)_{jk} (e_i)_k = A_{ji}^t = A_{ij}. \quad (4.259)$$

Pour calculer $t_2(e_i)_j$, c'est un peu plus laborieux :

$$t_2(e_i) = \sum_\alpha Q_{\alpha i}^{-1} t_2(f_\alpha) = \sum_{\beta\gamma\alpha} Q_{\alpha i}^{-1} B_{\gamma\beta}^t \underbrace{(t_\alpha)_\beta}_{\delta_{\alpha\beta}} f_\gamma = \sum_{\beta\gamma} Q_{\beta i}^{-1} B_{\gamma\beta}^t f_\gamma \quad (4.260a)$$

$$= (B^t Q^{-1})_{\gamma i} Q_{j\gamma} e_j \quad (4.260b)$$

$$= \sum_j (Q B^t Q^{-1})_{ji} e_j. \quad (4.260c)$$

Donc $t_2(e_i)_j = (Q B^t Q^{-1})_{ji}$. En tenant compte du fait que $B = Q^{-1} A Q$ nous avons

$$t_2(e_i)_j = (Q Q^t A^t (Q^{-1})^t Q^{-1})_{ji}. \quad (4.261)$$

Cela est égal à l'expression (4.259) lorsque $Q^t = Q^{-1}$. Nous voyons que confondre transposée d'une application linéaire avec transposée de la matrice associée n'est valable que si nous sommes certain de ne considérer que des changements de base par des matrices orthogonales.

Cela est la situation typique dans laquelle nous nous trouvons lorsque nous considérons des applications linéaires sur $\mathbb{R}^n$ muni de la base canonique et que nous n'avons aucune intention de changer de base, et encore moins de chercher une base non orthonormale. Cette situation est clairement la situation la plus courante.

Exemple 4.133 ([68]).

Soit la base canonique $\{e_1, e_2\}$ de $\mathbb{R}^2$. Nous considérons l'application linéaire $t: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ définie par

$$t(e_1) = e_1 \quad (4.262a)$$

$$t(e_2) = 0. \quad (4.262b)$$

La matrice de t dans cette base est

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}. \quad (4.263)$$

Elle est symétrique : elle vérifie $A^t = A$. Si nous comptons sur la transposée de matrice pour définir la transposée de t , nous aurions $t^t = t$.

Soit maintenant la base $f_1 = e_1$, $f_2 = e_1 + e_2$. Nous avons $t(f_1) = f_1$ et

$$t(f_2) = t(e_1) + t(e_2) = e_1 = f_1. \quad (4.264)$$

Donc la matrice de t dans cette base est

$$B = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}. \quad (4.265)$$

Et là, nous avons $B^t \neq B$. Donc en comptant sur cette base pour définir la transposée de t nous aurions $t^t \neq t$. $\triangle$

4.134.

Autrement dit, la façon « usuelle » de voir la transposée d'une application linéaire ne fonctionne dans les livres pour enfant uniquement parce qu'on n'y considère toujours $\mathbb{R}^n$ muni de la base canonique ou de bases orthonormées.

Notons que nous avons tout de même les notions d'opérateur adjoint et autoadjoint pour parler d'application orthogonale sans passer par la transposée, voir 9.38.

4.6.3 Transposée : la bonne approche**Définition 4.135.**

Si $f: E \rightarrow F$ est une application linéaire entre deux espaces vectoriels, la **transposée** est l'application $f^t: F^* \rightarrow E^*$ donnée par

$$f^t(\omega)(x) = \omega(f(x)). \quad (4.266)$$

pour tout $\omega \in F^*$ et $x \in E$.

Lemme 4.136.

Soit E muni de la base $\{e_i\}$ et F muni de la base $\{g_i\}$ et une application $f: E \rightarrow F$. Si A est la matrice de f dans ces bases, alors A^t est la matrice de f^t dans les bases $\{e_i^*\}$ et $\{g_i^*\}$ de E^* et F^* .

Démonstration. Nous allons montrer que les formes $f^t(g_i^*)$ et $\sum_k (A^t)_{ik} g_k^*$ sont égales en les appliquant à un vecteur.

Par définition de la matrice d'une application linéaire dans une base,

$$f^t(g_i^*) = \sum_j (f^t)_{ij} e_j^*, \quad (4.267)$$

et

$$f(e_k) = \sum_l A_{kl} g_l. \quad (4.268)$$

Du coup, si $x = \sum_k x_k e_k$, nous avons

$$f^t(g_i^*)x = \sum_{kl} x_k g_i^* A_{kl} g_l = \sum_{kl} x_k A_{kl} \delta_{il} = \sum_k x_k A_{ki} = \sum_k (A^t)_{ik} x_k. \quad (4.269)$$

D'autre part,

$$\sum_k (A^t)_{ik} g_k^* x = \sum_{kl} (A^t)_{ik} g_k^* x_l e_l = \sum_k (A^t)_{ik} x_k. \quad (4.270)$$

Le fait que (4.269) et (4.270) donnent le même résultat prouve le lemme. $\square$

En corolaire, les rangs de f et de f^t sont égaux parce que le rang est donné par la plus grande matrice carrée de déterminant non nul. Nous prouvons cependant ce résultat de façon plus intrinsèque.

Lemme 4.137 ([106]).

Si $f: E \rightarrow F$ est une application linéaire, alors

$$\text{rang}(f) = \text{rang}(f^t). \quad (4.271)$$

Démonstration. Nous posons $\dim \ker(f) = p$ et donc $\text{rang}(f) = n - p$. Soit $\{e_1, \dots, e_p\}$ une base de $\ker(f)$ que l'on complète en une base $\{e_1, \dots, e_n\}$ de E . Nous considérons maintenant les vecteurs

$$g_i = f(e_{p+i}) \quad (4.272)$$

pour $i = 1, \dots, n - p$. C'est-à-dire que les g_i sont les images des vecteurs qui ne sont pas dans le noyau de f . Prouvons qu'ils forment une famille libre. Si

$$\sum_{k=1}^{n-p} a_k f(e_{p+k}) = 0, \quad (4.273)$$

alors $f(\sum_k a_k e_{p+k}) = 0$, ce qui signifierait que $\sum_k a_k e_{p+k}$ se trouve dans le noyau de f , ce qui est impossible par construction de la base $\{e_i\}_{i=1,\dots,n}$. Étant donné que les vecteurs $g_1, \dots, g_{n-p}$ sont libres, nous les complétons en une base

$$\underbrace{\{g_1, \dots, g_{n-p}\}}_{\text{images}} \underbrace{\{g_{n-p+1}, \dots, g_r\}}_{\text{complétion}} \quad (4.274)$$

de F .

Nous prouvons maintenant que $\text{rang}(f^t) \geq n - p$ en montrant que les formes $\{g_i^*\}_{i=1,\dots,n-p}$ forment une partie libre (et donc l'espace image de f^t est au moins de dimension $n - p$). Pour cela nous prouvons que $f^t(g_i^*) = e_{i+p}^*$. En effet

$$f^t(g_i^*)e_k = g_i^*(fe_k), \quad (4.275)$$

Si $k = 1, \dots, p$, alors $fe_k = 0$ et donc $g_i^*(fe_k) = 0$; si $k = p + l$ alors

$$f^t(g_i^*)e_k = g_i^*(fe_{k+l}) = g_i^*(g_l) = \delta_{i,l} = \delta_{i,k-p} = \delta_{k,i+p}. \quad (4.276)$$

Donc $f^t(g_i^*) = e_{i+p}^*$. Cela prouve que les formes $f^t(g_i^*)$ sont libres et donc que

$$\text{rang}(f^t) \geq n - p = \text{rang}(f). \quad (4.277)$$

En appliquant le même raisonnement à f^t au lieu de f , nous trouvons

$$\text{rang}((f^t)^t) \geq \text{rang}(f^t) \quad (4.278)$$

et donc, vu que $(f^t)^t = f$, nous obtenons $\text{rang}(f) = \text{rang}(f^t)$. □

Proposition 4.138 ([107]).

Si f est une application linéaire entre les espaces vectoriels E et F , alors nous avons

$$\text{Image}(f^t) = \ker(f)^\perp. \quad (4.279)$$

Démonstration. Soient donc l'application $f: E \rightarrow F$ et sa transposée $f^t: F^* \rightarrow E^*$. Nous commençons par prouver que $\text{Image}(f^t) \subset (\ker f)^\perp$. Pour cela nous prenons $\omega \in \text{Image}(f^t)$, c'est-à-dire $\omega = \alpha \circ f$ pour un certain élément $\alpha \in F^*$. Si $z \in \ker(f)$, alors $\omega(z) = (\alpha \circ f)(z) = 0$, c'est-à-dire que $\omega \in (\ker f)^\perp$.

Pour prouver qu'il y a égalité, nous n'allons pas démontrer l'inclusion inverse, mais plutôt prouver que les dimensions sont égales. Après, on sait que si $A \subset B$ et si $\dim A = \dim B$, alors $A = B$. Nous avons

$$\dim(\text{Image}(f^t)) = \text{rang}(f^t) \quad (4.280a)$$

$$= \text{rang}(f) \quad \text{lemme 4.137} \quad (4.280b)$$

$$= \dim(E) - \dim \ker(f) \quad \text{théorème 4.42} \quad (4.280c)$$

$$= \dim((\ker f)^\perp) \quad \text{proposition 4.131.} \quad (4.280d)$$

□

Lemme 4.139 ([101]).

Soit $\mathbb{K}$ un corps, E et F deux $\mathbb{K}$ -espaces vectoriels de dimension finie et une application linéaire $f: E \rightarrow F$. L'application f est injective si et seulement si sa transposée⁵¹ f^t est surjective.

51. Définition 4.135.

Démonstration. Supposons que f soit injective. Alors par le lemme 4.51, il existe $g: F \rightarrow E$ tel que $g \circ f = \text{Id}|_E$. Nous avons alors aussi $(g \circ f)^t = \text{Id}|_{E^*}$, mais $(g \circ f)^t = f^t \circ g^t$, donc f^t est surjective.

Inversement, nous supposons que $f^t: F^* \rightarrow E^*$ est surjective. Alors en nous souvenant que E et F sont de dimension finie et en faisant jouer les identifications $(f^t)^t = f$ et $(E^*)^* = E$ nous savons qu'il existe $s: E^* \rightarrow F^*$ tel que $f^t \circ s = \text{Id}|_{E^*}$. En passant à la transposée,

$$s^t \circ f = \text{Id}|_E, \quad (4.281)$$

qui implique que f est injective. $\square$

4.6.4 Polynômes de Lagrange

Soit $E = \mathbb{R}_n[X]$ l'ensemble des polynômes à coefficients réels de degré au plus n . Soient les $n+1$ réels distincts $a_0, \dots, a_n$. Nous considérons les formes linéaires associées $f_i \in E^*$,

$$f_i(P) = P(a_i). \quad (4.282)$$

Lemme 4.140.

Ces formes forment une base de E^* .

Démonstration. Nous prouvons que l'orthogonal est réduit au nul :

$$\text{Span}\{f_0, \dots, f_n\}^\perp = \{0\} \quad (4.283)$$

pour que la proposition 4.131 conclue. Si $P \in \text{Span}\{f_i\}^\perp$, alors $f_i(P) = 0$ pour tout i , ce qui fait que $P(a_i) = 0$ pour tout $i = 0, \dots, n$. Un polynôme de degré au plus n qui s'annule en $n+1$ points est automatiquement le polynôme nul. $\square$

Les **polynômes de Lagrange** sont les polynômes de la base (pré)duale de la base $\{f_i\}$.

Proposition 4.141.

Les polynômes de Lagrange sont donnés par

$$P_i = \prod_{k \neq i} \frac{X - a_k}{a_i - a_k}. \quad (4.284)$$

Démonstration. Il suffit de vérifier que $f_j(P_i) = \delta_{ij}$. Nous avons

$$f_j(P_i) = P_i(a_j) = \prod_{k \neq i} \frac{a_j - a_k}{a_i - a_k}. \quad (4.285)$$

Si $j \neq i$ alors un des termes est nul. Si au contraire $i = j$, tous les termes valent 1. $\square$

4.6.5 Dual de $\mathbb{M}(n, \mathbb{K})$

Proposition 4.142 ([79]).

Soit $\mathbb{K}$, un corps. Les formes linéaires sur $\mathbb{M}(n, \mathbb{K})$ sont les applications de la forme

$$\begin{aligned} f_A: \mathbb{M}(n, \mathbb{K}) &\rightarrow \mathbb{K} \\ M &\mapsto \text{Tr}(AM). \end{aligned} \quad (4.286)$$

Démonstration. Nous considérons l'application

$$\begin{aligned} f: \mathbb{M}(n, \mathbb{K}) &\rightarrow \mathbb{M}(n, \mathbb{K})^* \\ A &\mapsto f_A \end{aligned} \quad (4.287)$$

et nous voulons prouver que c'est une bijection. Étant donné que nous sommes en dimension finie, nous avons égalité des dimensions de $\mathbb{M}(n, \mathbb{K})$ et $(\mathbb{M}(n, \mathbb{K}))^*$, et il suffit de prouver que f est injective. Soit donc A telle que $f_A = 0$. Nous l'appliquons à la matrice $(E_{ij})_{kl} = \delta_{ik}\delta_{jl}$:

$$0 = f_A(E_{ij}) = \sum_k (AE_{ij})_{kk} = \sum_{kl} A_{kl}(E_{ij})_{lk} = \sum_{kl} A_{kl}\delta_{il}\delta_{jk} = A_{ij}. \quad (4.288)$$

Donc $A = 0$. □

Corolaire 4.143 ([79]).

Soient un corps $\mathbb{K}$ ainsi qu'une matrice $\phi \in \mathbb{M}(n, \mathbb{K})^*$ telle que pour tout $M, N \in \mathbb{M}(n, \mathbb{K})$ on ait

$$\phi(MN) = \phi(NM). \quad (4.289)$$

Alors il existe $\lambda \in \mathbb{K}$ tel que $\phi = \lambda \text{Tr}$.

Démonstration. La proposition 4.142 nous donne une matrice $A \in \mathbb{M}(n, \mathbb{K})$ telle que $\phi = f_A$. L'hypothèse nous dit que $f_A(MN) = f_A(NM)$, c'est-à-dire

$$\text{Tr}(AMN) = \text{Tr}(ANM) \quad (4.290)$$

pour toutes matrices $M, N \in \mathbb{M}(n, \mathbb{K})$. L'invariance cyclique de la trace⁵² appliqué au membre de droite nous donne $\text{Tr}(AMN) = \text{Tr}(MAN)$, ce qui signifie que

$$\text{Tr}((AM - MA)N) = 0 \quad (4.291)$$

ou encore que $f_{AM-MA} = 0$, et ce, pour toute matrice M . La fonction f étant injective nous en déduisons que la matrice A doit satisfaire

$$AM = MA \quad (4.292)$$

pour tout $M \in \mathbb{M}(n, \mathbb{K})$. En particulier, en prenant pour M les fameuses matrices E_{ij} et en calculant un peu,

$$A_{li}\delta_{jm} = \delta_{il}A_{jm} \quad (4.293)$$

pour tout i, j, l, m . Cela implique que $A_{ll} = A_{mm}$ pour tout l et m et que $A_{jm} = 0$ dès que $j \neq m$. Il existe donc $\lambda \in \mathbb{K}$ tel que $A = \lambda \mathbb{1}$. En fin de compte,

$$\phi(X) = f_{\lambda \mathbb{1}}(X) = \lambda \text{Tr}(X). \quad (4.294)$$

□

Corolaire 4.144 ([79]).

Soit $\mathbb{K}$ un corps. Tout hyperplan de $\mathbb{M}(n, \mathbb{K})$ coupe $\text{GL}(n, \mathbb{K})$.

Démonstration. Soit $\mathcal{H}$ un hyperplan de $\mathbb{M}$. Il existe une forme linéaire ϕ sur $\mathbb{M}(n, \mathbb{K})$ telle que $\mathcal{H} = \ker(\phi)$. Encore une fois la proposition 4.142 nous donne $A \in \mathbb{M}$ telle que $\phi = f_A$; nous notons r le rang de A . Par le lemme 4.107 nous avons $A = PJ_rQ$ avec $P, Q \in \text{GL}(n, \mathbb{K})$ et

$$J_r = \begin{pmatrix} \mathbb{1}_r & 0 \\ 0 & 0 \end{pmatrix}. \quad (4.295)$$

Pour tout $M \in \mathbb{M}$ nous avons

$$\phi(M) = \text{Tr}(AM) = \text{Tr}(PJ_rQM) = \text{Tr}(J_rQMP), \quad (4.296)$$

⁵². Lemme 4.60.

la dernière égalité découlant de l'invariance cyclique de la trace⁵³. Ce que nous cherchons est $M \in \text{GL}(n, \mathbb{K})$ telle que $\phi(M) = 0$. Nous commençons par trouver $N \in \text{GL}(n, \mathbb{K})$ telle que $\text{Tr}(J_r N) = 0$. Celle-là est facile : c'est

$$N = \begin{pmatrix} 0 & 1 \\ \mathbb{1}_{n-1} & 0 \end{pmatrix}. \quad (4.297)$$

Les éléments diagonaux de $J_r N$ sont tous nuls. Par conséquent en posant $M = Q^{-1} N P^{-1}$ nous avons notre matrice inversible dans le noyau de ϕ . $\square$

4.7 Représentation de groupe

Définition 4.145 (Représentation).

Soit un groupe G et un espace vectoriel V . Nous disons qu'une application $\rho: G \rightarrow \text{GL}(V)$ est une **représentation** de G sur V si pour tout $g, h \in G$ nous avons

$$\rho(g) \circ \rho(h) = \rho(gh). \quad (4.298)$$

Très souvent, nous disons que la représentation est le couple (V, ρ) .

Définition 4.146.

Une représentation⁵⁴ est **fidèle** si elle est injective en tant que application $G \rightarrow \text{GL}(V)$. Ce ne sont pas chacun des $\rho(g)$ qui doivent être injectifs. La dimension de V est le **degré** de la représentation (V, ρ) .

Proposition 4.147.

Soit un corps $\mathbb{K}$. Si G est un groupe dans $\mathbb{M}(n, \mathbb{K})$ (c'est-à-dire un groupe de matrices à coefficients dans $\mathbb{K}$), alors l'application

$$\begin{aligned} \rho: G &\rightarrow \text{GL}(\mathbb{K}^n) \\ A &\mapsto f_A \end{aligned} \quad (4.299)$$

où f_A est l'application linéaire associée à A est une représentation de G .

4.8 Somme directe d'espaces vectoriels

Si V et W sont des espaces vectoriels, ce que nous notons $V \oplus W$ n'est rien d'autre que l'espace vectoriel de l'ensemble $V \times W$.

Proposition-Définition 4.148 ([108, 109]).

Si V et W sont des espaces vectoriels sur le même corps $\mathbb{K}$, alors les définitions

- (1) $(v_1, w_1) + (v_2, w_2) = (v_1 + v_2, w_1 + w_2)$
- (2) $\lambda(v, w) = (\lambda v, \lambda w)$

donnent une structure d'espace vectoriel sur $V \times W$.

Cet espace sera noté $V \oplus W$ et est appelé **somme directe** de V et W .

Définition 4.149 (Sous-espaces en somme directe[110]).

Soient un espace vectoriel E ainsi que des sous-espaces vectoriels $\{F_i\}_{i \in I}$ (I est un ensemble fini ou infini). Nous disons que les F_i sont **en somme directe** si pour tout élément $u \in \sum_{i \in I} F_i$, il existe un unique ensemble $\{u_i\}_{i \in I}$ tel que

- (1) $u = \sum_{i \in I} u_i$
- (2) $u_i \in F_i$ pour tout i ,

⁵³. Lemme 4.60.

⁵⁴. Définition 4.145.

(3) $\{j \in I \text{ tel que } u_j \neq 0\}$ est fini.

Lemme 4.150 ([1, 110]).

Soient un espace vectoriel E ainsi que des sous-espaces vectoriels F_i . Nous avons équivalence entre les choses suivantes.

(1) Les F_i sont en somme directe⁵⁵.

(2) Si $\sum_{i \in I} u_i = 0$ avec $u_i \in F_i$ et si $\{j \in I \text{ tel que } u_j \neq 0\}$ est fini, alors tous les u_i sont nuls.

Proposition 4.151 ([111]).

Soient un espace vectoriel de dimension finie V et deux sous-espaces M_1 et M_2 satisfaisant

(1) $M_1 \cap M_2 = \{0\}$,

(2) $\dim(M_1) + \dim(M_2) \geq \dim(V)$.

Alors $V = M_1 \oplus M_2$.

Démonstration. Soient une base $\{e_i\}_{i \in I}$ de M_1 et $\{f_\alpha\}$ de M_2 . Nous commençons par prouver que la partie $B = \{e_i\} \cup \{f_\alpha\}$ est libre.

Supposons en effet avoir des coefficients a_i et b_α tels que

$$\sum_i a_i e_i + \sum_\alpha b_\alpha f_\alpha = 0. \quad (4.300)$$

Cela implique que $\sum_i a_i e_i = -\sum_\alpha b_\alpha f_\alpha$. Or $\sum_i a_i e_i \in M_1$ et $-\sum_\alpha b_\alpha f_\alpha \in M_2$. Donc les éléments $\sum_i a_i e_i$ et $\sum_\alpha b_\alpha f_\alpha$ sont dans $M_1 \cap M_2 = \{0\}$. Nous avons alors les égalités

$$\sum_i a_i e_i = 0 \quad (4.301)$$

et

$$\sum_\alpha b_\alpha f_\alpha = 0. \quad (4.302)$$

La première implique $a_i = 0$ pour tout i et la seconde implique $b_\alpha = 0$ pour tout α .

Donc B est une partie libre de V contenant $\dim(M_1) + \dim(M_2) \geq \dim(V)$ éléments. La proposition 4.16(1) nous indique alors qu'en réalité $\dim(M_1) + \dim(M_2) = \dim(V)$. Vu que B est une partie libre contenant $\dim(V)$ éléments, c'est une base par la proposition 4.16(2). $\square$

4.8.1 Structure réelle

Proposition-Définition 4.152 ([112, 109, 1]).

Soit un espace vectoriel V sur $\mathbb{C}$. Il existe une application $\sigma: V \rightarrow V$ telle que

(1) $\sigma^2 = \text{id}$ (involution)

(2) Pour tout $\alpha, \beta \in \mathbb{R}$, $f(\alpha x + \beta y) = \alpha \sigma(x) + \beta \sigma(y)$.

Une telle application est une **structure réelle** sur V .

Démonstration. La proposition 4.21 nous permet de considérer une base $\{e_i\}_{i \in I}$ de V . Alors nous définissons

$$\sigma\left(\sum_{i \in I} \lambda_i e_i\right) = \sum_{i \in I} \bar{\lambda}_i e_i. \quad (4.303)$$

Notez que la somme est toujours finie. $\square$

Proposition 4.153.

Soit un espace vectoriel V sur $\mathbb{C}$ et une structure réelle⁵⁶ σ sur V . Nous posons

$$V_{\mathbb{R}} = \{v \in V \text{ tel que } \sigma(v) = v\}. \quad (4.304)$$

Alors

55. Définition 4.149.

56. Définition 4.152.

- (1) La partie $V_{\mathbb{R}}$ est un espace vectoriel réel.
 (2) Nous avons la décomposition en somme directe⁵⁷

$$V = V_{\mathbb{R}} \oplus iV_{\mathbb{R}}. \quad (4.305)$$

Démonstration. En plusieurs parties.

Espace vectoriel réel Si $v, w \in V_{\mathbb{R}}$, alors

$$\sigma(v + w) = \sigma(v) + \sigma(w) = v + w, \quad (4.306)$$

et si $\lambda \in \mathbb{R}$,

$$\sigma(\lambda x) = \lambda \sigma(x) = \lambda x. \quad (4.307)$$

Donc $V_{\mathbb{R}}$ est un espace vectoriel réel.

Première somme directe Nous définissons

$$V^+ = \{v \in V \text{ tel que } \sigma(v) = v\}, \quad (4.308a)$$

$$V^- = \{v \in V \text{ tel que } \sigma(v) = -v\} \quad (4.308b)$$

Nous prouvons que

$$\begin{aligned} \psi: V^+ \times V^- &\rightarrow V \\ a, b &\mapsto a + b \end{aligned} \quad (4.309)$$

est un isomorphisme d'espaces vectoriels.

Vu que ψ est linéaire, il suffit de prouver qu'elle est bijective.

Subjectif Si $v \in V$, alors en posant $v_+ = \frac{1}{2}(v + \sigma(v))$, $v_- = \frac{1}{2}(v - \sigma(v))$, nous avons

$$v = v_+ + v_-, \quad v_+ \in V^+, \quad v_- \in V^-, \quad (4.310)$$

et donc $v = \psi(v_+, v_-)$.

Injectif Supposons $\psi(a, b) = \psi(\alpha, \beta)$. Alors $a + b = \alpha + \beta$ et donc $a - \alpha = \beta - b$. Vu que $a - \alpha \in V^+$ et $\beta - b \in V^-$, nous savons que $a - \alpha = \beta - b \in V^+ \cap V^-$. Étant donné que $V^+ \cap V^- = \{0\}$, nous avons $a - \alpha = \beta - b = 0$.

Nous avons donc la somme directe $V = V^+ \oplus V^-$.

Conclusion Par définition, $V^+ = V_{\mathbb{R}}$. Il nous reste à voir que $V^- = iV^+$. Nous faisons les inclusions dans les deux sens.

$V^- \subset iV^+$ Soit $v \in V^-$. Nous avons $iv \in V^+$; en effet

$$\sigma(iv) = -i\sigma(v) = iv. \quad (4.311)$$

Donc $v = i(-iv)$ avec $-iv \in V^+$.

$iV^+ \subset V^-$ Soit $v \in V^+$, et voyons que $iv \in V^-$. En effet,

$$\sigma(iv) = -i\sigma(v) = -iv. \quad (4.312)$$

□

4.154.

Lorsque nous avons une structure réelle σ sur un espace vectoriel complexe V , nous écrivons $V = V_{\mathbb{R}} \oplus iV_{\mathbb{R}}$ sans préciser dans la notation « $V_{\mathbb{R}}$ » que cet ensemble dépend du choix de σ . En particulier si W est un sous-espace de V , nous utiliserons la notation $W_{\mathbb{R}}$ relativement à la même involution que celle de V .

57. Définition 4.148.

Lemme 4.155.

Soit un espace vectoriel complexe V muni d'une structure réelle σ . Si W est un sous-espace de V alors $W_{\mathbb{R}} = V_{\mathbb{R}} \cap W$.

Démonstration. Par définition,

$$W_{\mathbb{R}} = \{w \in W \text{ tel que } \sigma(w) = w\}. \quad (4.313)$$

$W_{\mathbb{R}} \subset W$ C'est défini en tant que sous-ensemble.

$W_{\mathbb{R}} \subset V_{\mathbb{R}}$ Si $w \in W_{\mathbb{R}}$, alors $\sigma(w) = w$. Mais cette égalité est précisément également l'égalité pour être dans $V_{\mathbb{R}}$.

□

Vous remarquerez que ce lemme ne fonctionne que parce que nous avons choisi la même structure réelle sur W que sur V .

Chapitre 5

Classification de certains groupes

5.1 Théorèmes de Sylow

Lemme 5.1.

Soient H et K des sous-groupes finis de G . Alors

$$\text{Card}(HK) = \frac{|H| \cdot |K|}{|H \cap K|}. \quad (5.1)$$

Attention : dans ce lemme, l'ensemble HK n'est pas spécialement un groupe. Ce serait le cas si H normaliserait K , c'est-à-dire si nous avons $hkh^{-1} \in K$, $\forall h, k \in H \times K$.

Théorème 5.2 (Théorème de Cauchy[113]).

Soit G un groupe fini et p un nombre premier divisant $|G|$. Alors

- (1) G contient un élément d'ordre p .
- (2) Si G est un p -groupe, il existe un élément central d'ordre p dans G .

Lemme 5.3 (Théorème de Cayley).

Si G est un groupe d'ordre n alors il est isomorphe à un sous-groupe du groupe symétrique S_n .

Démonstration. L'action à gauche de G sur lui-même

$$\begin{aligned} \varphi: G &\rightarrow S_n \\ \varphi(x)g &\mapsto xg \end{aligned} \quad (5.2)$$

est une permutation des éléments de G . Cela donne un morphisme injectif parce que si $\varphi(x) = \varphi(y)$ nous avons $xg = yg$ pour tout g et en particulier pour $g = e$ nous trouvons $x = y$. $\square$

Lemme 5.4.

Soit p un diviseur premier de n . Alors le groupe symétrique S_n se plonge dans $\text{GL}_n(\mathbb{F}_p)$.

Démonstration. Soit $\{e_i\}$ la base canonique de $\mathbb{F}_p$. Nous avons le morphisme injectif $\varphi: S_n \rightarrow \text{GL}(n, \mathbb{F})$ donné par $\varphi(\sigma)e_i = e_{\sigma(i)}$. $\square$

Remarque 5.5.

En mettant bout à bout les lemmes 5.3 et 5.4, nous trouvons que si p est un diviseur premier de $|G|$, alors G peut être vu comme un sous-groupe de $\text{GL}(n, \mathbb{F}_p)$.

Définition 5.6.

Soit p un nombre premier. Un **p -groupe** est un groupe dont tous les éléments sont d'ordre p^m pour un certain m (dépendant de l'élément).

Soit G un groupe fini et p , un diviseur premier de $|G|$. Un **p -Sylow** dans G est un p -sous-groupe d'ordre p^n où p^n est la plus grande puissance de p divisant $|G|$.

Notons que si p est un nombre premier, alors tout groupe d'ordre p^m est un p -groupe.

Lemme 5.7.

Soit G un groupe fini et P, Q des p -sous-groupes. Nous supposons que Q normalise P . Alors PQ est un p -sous-groupe de G .

Si S est un p -Sylow, alors p ne divise pas le nombre $|G : S| = |G|/|S|$.

Proposition 5.8.

Soit le corps fini $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (p premier). Soit T le sous-ensemble de $\mathrm{GL}_n(\mathbb{F}_p)$ formé des matrices triangulaires supérieures de rang¹ n et dont les éléments diagonaux sont 1. Alors T est un p -Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$.

Démonstration. Nous commençons par étudier le cardinal de $\mathrm{GL}_n(\mathbb{F}_p)$. Pour la première colonne, la seule contrainte à vérifier est qu'elle ne soit pas nulle. Il y a donc $p^n - 1$ possibilités. Pour la seconde, il faut ne pas être multiple de la première. Il y a donc $p^n - p$ possibilités (parce qu'il y a p multiples possibles de la première colonne). Pour la k -ième colonne, il faut éviter toutes les combinaisons linéaires des $(k-1)$ premières colonnes. Il y a p^{k-1} telles combinaisons et donc $p^n - p^{k-1}$ possibilités pour la k -ième colonne. Nous avons donc

$$\mathrm{Card}(\mathrm{GL}(n, \mathbb{F}_p)) = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1}) \quad (5.3a)$$

$$= p \cdot p^2 \dots p^{n-1} (p^n - 1)(p^{n-1} - 1) \dots (p - 1) \quad (5.3b)$$

$$= p^{\frac{n(n-1)}{2}} m \quad (5.3c)$$

où m est un entier qui ne divise pas p .

En ce qui concerne le cardinal de T , le calcul est plus simple : pour la première ligne nous avons p^{n-1} choix (parce qu'il y a un 1 qui est imposé sur la diagonale), pour la seconde p^{n-2} , etc. En tout nous avons alors

$$|T| = p^{\frac{n(n-1)}{2}}, \quad (5.4)$$

et T est un p -Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$. □

Proposition 5.9.

Soit p un nombre premier. Un groupe fini G est un p -groupe si et seulement l'ordre de G est p^n pour un certain n .

Démonstration. Supposons que G est un p -groupe. Soit q un nombre premier divisant $|G|$. Par le théorème de Cauchy (5.2), le groupe G contient un élément d'ordre q , soit g un tel élément. Étant donné que G est un p -groupe, $g^{p^n} = g^q = e$ pour un certain n . Donc $q = p^n$ et $q = p$ parce que q est premier. Nous venons de prouver que p est le seul nombre premier qui divise $|G|$. L'ordre de G est par conséquent une puissance de p .

Nous nous intéressons maintenant à l'implication inverse. Nous supposons que $|G| = p^n$ pour un certain entier $n \geq 0$. Soit $g \in G$; nous notons r l'ordre de G . Le sous-groupe $\mathrm{gr}(g)$ est d'ordre r , donc r divise $|G|$ (par le théorème 2.35 de Lagrange). Le nombre r est alors une puissance de p . □

Lemme 5.10.

Soit G , un groupe fini de cardinal $|G| = n$ et p , un diviseur premier de n . Nous notons $n = p^m \cdot r$ où p ne divise pas r . Soit H un sous-groupe de G et S , un p -Sylow de G . Alors il existe $g \in G$ tel que

$$gSg^{-1} \cap H \quad (5.5)$$

soit un p -Sylow de H .

1. Définition 4.41.

Démonstration. Nous considérons l'ensemble G/S sur lequel H agit. Si $a \in G$, le stabilisateur de $[a]$ dans G/S est

$$\text{Fix}([a]) = \{h \in H \text{ tel que } [ha] = [a]\} \quad (5.6a)$$

$$= \{h \in H \text{ tel que } a^{-1}ha \in S\} \quad (5.6b)$$

$$= aSa^{-1} \cap H. \quad (5.6c)$$

Nous cherchons $a \in G$ tel que l'entier

$$\frac{\text{Card}(H)}{\text{Card}(aSa^{-1} \cap H)} \quad (5.7)$$

soit premier avec p . En effet, dans ce cas le groupe $\text{Fix}([a])$ est un p -Sylow de H parce que $|H : aSa^{-1} \cap H|$ ne divise pas p . La formule des orbites (équation (2.92)) nous dit que

$$\frac{|H|}{|aSa^{-1} \cap H|} = \text{Card}(\mathcal{O}_{[a]}). \quad (5.8)$$

Supposons que toutes les orbites aient un cardinal divisible par p . Étant donné que G/S est une réunion disjointe de ses orbites, nous aurions

$$p \mid \text{Card}(G/S) = \frac{|G|}{|S|} \quad (5.9)$$

alors que S étant un p -Sylow, p ne peut pas diviser $|G|/|S|$. Toutes les orbites n'ont donc pas un cardinal divisible par p , et il existe un $a \in G$ tel que (5.7) soit vérifiée. $\square$

Théorème 5.11 (Théorème de Sylow).

Soit G un groupe fini et p , un diviseur premier de $|G|$. Alors

- (1) G possède au moins un p -Sylow².
- (2) Tout p -sous-groupe de G est contenu dans un p -Sylow.
- (3) Les p -Sylow de G sont conjugués.
- (4) Si n_p est le nombre de p -Sylow de G , alors n_p divise $|G|$ et $n_p \in [1]_p$.

Démonstration. En plusieurs points.

- (1) Nous savons de la remarque 5.5 que G est un sous-groupe de $\text{GL}_n(\mathbb{F}_p)$ et que ce dernier a un p -Sylow par la proposition 5.8. Par conséquent G possède un p -Sylow par le lemme 5.10.
- (2) Soit H un p -sous-groupe de G et S , un p -Sylow de G (qui existe par le point précédent). Par le lemme 5.10 il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p -Sylow de H . Mais H est un p -groupe et un p -Sylow dans un p -groupe est automatiquement le groupe entier. Par conséquent,

$$H = aSa^{-1} \cap H \quad (5.10)$$

et $H \subset aSa^{-1}$, ce qui signifie que H est inclus dans un p -Sylow.

- (3) Soit H un p -Sylow. Nous venons de voir que si S est un p -Sylow quelconque, alors H est inclus au p -Sylow aSa^{-1} pour un certain $a \in G$. Donc H est un p -Sylow inclus dans le p -Sylow aSa^{-1} , donc $H = aSa^{-1}$.
- (4) Le fait que n_p divise n est parce que tous les p -Sylow ont le même nombre d'éléments (ils sont conjugués) et sont deux à deux disjoints. Donc ils forment une partition de G et $|G| = n_p|S|$ si S est un p -Sylow quelconque.

Montrons maintenant que n_p est congru à un modulo p . Soit E l'ensemble des p -Sylow de G . Le groupe G agit sur E par conjugaison. Soit S un p -Sylow et considérons l'ensemble

$$E_S = \{T \in E \text{ tel que } s \cdot T = T \forall s \in S\}. \quad (5.11)$$

2. Définition 5.6.

où l'action est celle par conjugaison. C'est l'ensemble des points fixes de E sous l'action de S . L'ensemble E est la réunion des orbites sous S et chacune de ces orbites a un cardinal qui divise $|S| = p^m$. Par conséquent $|\mathcal{O}_T|$ vaut 1 lorsque $T \in E_S$ et est un multiple de p sinon. Nous avons donc

$$|E| \equiv |E_S| \pmod{p}. \quad (5.12)$$

Nous voulons obtenir $|E_S| = 1$. Évidemment $S \in E_S$ parce que si $s \in S$ alors $sSs^{-1} = S$. Nous voudrions montrer que S est le seul élément de E_S . Soit $T \in E_S$, c'est-à-dire que T est un p -Sylow de G tel que

$$sTs^{-1} = T \quad (5.13)$$

pour tout $s \in S$. Soit N le groupe engendré par S et T . Montrons que T est normal dans N . Un élément g dans N s'écrit

$$g = s_1 t_1 \cdots s_r t_r \quad (5.14)$$

avec $s_i \in S$ et $t_i \in T$. Si $t \in T$, en utilisant le fait que T est un groupe et le fait que S le normalise, nous avons

$$gtg^{-1} = s_1 t_1 \dots s_r t_r t t_r^{-1} s_r^{-1} \dots t_1^{-1} s_1^{-1} \in T. \quad (5.15)$$

Donc T est un sous-groupe normal de N . Mais S et T sont conjugués dans N (parce que ils sont des p -Sylow de N), donc il existe un élément $a \in N$ tel que $aTa^{-1} = S$. Mais étant donné que T est normal,

$$S = aTa^{-1} = T. \quad (5.16)$$

Ceci achève la démonstration des théorèmes de Sylow. □

Proposition 5.12.

Si S est un p -Sylow dans le groupe G alors pour tout $g \in G$, l'ensemble gSg^{-1} est encore un p -groupe.

Démonstration. Si les éléments de S sont d'ordre p^n , alors nous avons

$$(gsg^{-1})^q = gs^qg^{-1} = e. \quad (5.17)$$

Pour avoir $gs^qg^{-1} = e$, il faut et suffit que $gs^q = g$, alors $s^q = e$, c'est-à-dire $q = p^n$. Donc gSg^{-1} est encore un p -Sylow. □

Lemme 5.13 ([114]).

Soit G , un groupe fini et p , un nombre premier. Si H et K sont des groupes distincts d'ordre p , alors $H \cap K = \{e\}$.

Démonstration. L'ensemble $H \cap K$ est un sous-groupe de H . Par conséquent son ordre divise celui de H qui est un nombre premier. Par conséquent soit $|H \cap K| = 1$, soit $|H \cap K| = |H|$. Dans le second cas nous aurions $H = K$, alors que nous avons supposé que H et K étaient distincts. □

Proposition 5.14 ([114]).

Soit G un groupe fini et n le nombre de sous-groupes d'ordre p dans G . Alors le nombre d'éléments d'ordre p dans G vaut $n(p-1)$.

Démonstration. Si g est un élément d'ordre p dans G , le groupe H engendré par g est d'ordre p . Réciproquement si H est un groupe d'ordre p , tous les éléments de $H \setminus \{e\}$ sont d'ordre p (parce que l'ordre d'un élément divise l'ordre du groupe). Donc l'ensemble des éléments d'ordre p dans G est la réunion des ensembles $H \setminus \{e\}$ où H parcourt les sous-groupes d'ordre p dans G . Chacun de ces ensembles possède $p-1$ éléments et le lemme 5.13 nous assure qu'ils sont disjoints. Par conséquent nous avons $n(p-1)$ éléments d'ordre p dans G . □

Corolaire 5.15.

Un groupe d'ordre premier est cyclique.

Démonstration. Soit p l'ordre de G . Le nombre de sous-groupes d'ordre p est $n = 1$ (et c'est G lui-même). La proposition 5.14 nous dit alors que le nombre d'éléments d'ordre p dans G est $p - 1$. Donc tout élément est générateur. $\square$

5.2 Groupe monogène

Le théorème suivant donne quelques informations à propos de groupes monogènes. Il impliquera dans le corolaire 19.16 qu'un groupe monogène d'ordre n possède $\varphi(n)$ générateur où φ est la fonction indicatrice d'Euler définie en 19.11.

Théorème 5.16.

Un groupe monogène est abélien. Plus précisément,

- (1) *un groupe monogène infini est isomorphe à $\mathbb{Z}$,*
- (2) *un groupe monogène fini est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ pour un certain n .*

Démonstration. Le groupe est abélien parce que $g = a^n$, $g' = a^{n'}$ implique $gg' = a^{n+n'} = g'g$. Nous considérons un générateur a de G (qui existe parce que G est monogène) et le morphisme surjectif

$$\begin{aligned} f: \mathbb{Z} &\rightarrow G \\ p &\mapsto a^p. \end{aligned} \tag{5.18}$$

Si G est infini, alors f est injective parce que si $a^n = a^{n'}$, alors $a^{n-n'} = e$, ce qui rendrait G cyclique et par conséquent non infini. Nous concluons que si G est infini, alors f est une bijection et donc un isomorphisme $\mathbb{Z} \simeq G$.

Si G est fini, alors f n'est pas injective et a un noyau $\ker f$. Étant donné que $\ker f$ est un sous-groupe de G , il existe un (unique) n tel que $\ker f = n\mathbb{Z}$ et le premier théorème d'isomorphisme (théorème 2.29) nous indique que

$$\mathbb{Z}/\ker f = \mathbb{Z}/n\mathbb{Z} = \text{Image } f = G. \tag{5.19}$$

$\square$

Le lemme suivant donne une démonstration alternative, avec une construction plus explicite de l'isomorphisme.

Lemme 5.17 ([1]).

À propos de groupes monogènes³

- (1) *Soit un groupe monogène G d'ordre fini n dont g est un générateur. Alors il existe un isomorphisme*

$$\phi: G \rightarrow (\mathbb{Z}/n\mathbb{Z}, +) \tag{5.20}$$

tel que $\phi(g) = 1$.

- (2) *Si G est un groupe monogène d'ordre infini et si g est un générateur, alors il existe un isomorphisme*

$$\phi: G \rightarrow (\mathbb{Z}, +) \tag{5.21}$$

tel que $\phi(g) = 1$.

- (3) *Soient G et H deux groupes monogènes de même ordre. Soient g un générateur de G et h , un générateur de H . Il existe un isomorphisme de G sur H qui envoie g sur h .*

3. Définition 2.14.

Démonstration. Commençons par enfoncer une porte ouverte : vu que le groupe est monogène, l'ordre du groupe est égal à l'ordre de son générateur. Nous séparons les cas selon quel l'ordre soit fini ou non.

L'ordre de G est fini et vaut n Si $k \in \mathbb{Z}$, nous notons $[k]_n$ la classe de k modulo n , c'est-à-dire l'ensemble $\{k + pn \mid p \in \mathbb{Z}\}$.

Nous construisons l'isomorphisme $\phi: G \rightarrow \mathbb{Z}/n\mathbb{Z}$ de la façon suivante :

$$\phi(g^m) = [m]_n. \quad (5.22)$$

Cela est une bonne définition parce que une égalité du type $g^m = g^{m'}$ implique que m et m' soient dans la même classe modulo n . Nous vérifions que cela est une isomorphisme entre G et $\mathbb{Z}/n\mathbb{Z}$.

Morphisme Pour l'identité, si $x = e$ alors $m = 0$ et $\phi(e) = [0]_n$. Et si $x = g^k$, $y = g^l$ alors $\phi(xy) = \phi(g^{k+l}) = [k+l]_n = [k]_n + [l]_n = \phi(x) + \phi(y)$.

Injectif Supposons $\phi(g^k) = \phi(g^l)$ avec $k \geq l$. Nous avons $h^k = h^l$, dont $h^{k-l} = e$, ce qui donne $k - l \in [0]_n$ ou encore $[k]_n = [l]_n$. En particulier $g^k = g^l$.

Surjectif La classe $[k]_n$ est l'image de g^k .

L'ordre de G est infini Si l'ordre de G est infini alors un élément $x \in G$ s'écrit de façon unique sous la forme $x = g^m$ avec $m \in \mathbb{Z}$. Dans ce cas nous définissons directement $\phi(g^m) = m$.

Le reste de la preuve est alors identique au cas d'ordre fini, mais sans les complications liées au modulo.

La dernière assertion s'obtient des précédentes par composition d'isomorphismes. □

5.3 Automorphismes du groupe $\mathbb{Z}/n\mathbb{Z}$

Notons que $\mathbb{Z}/n\mathbb{Z} = \mathbb{F}_n$ est un groupe pour l'addition tandis que $(\mathbb{Z}/n\mathbb{Z})^*$ est un groupe pour la multiplication. Il ne peut donc pas y avoir d'équivoque.

Théorème 5.18 ([115]).

Pour chaque $x \in (\mathbb{Z}/n\mathbb{Z})^*$ nous considérons l'application

$$\begin{aligned} \sigma_x: \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/n\mathbb{Z} \\ y &\mapsto xy. \end{aligned} \quad (5.23)$$

L'application

$$\sigma: ((\mathbb{Z}/n\mathbb{Z})^*, \cdot) \rightarrow \text{Aut}(\mathbb{Z}/n\mathbb{Z}, +) \quad (5.24)$$

ainsi définie est un isomorphisme de groupes.

L'énoncé de ce théorème s'écrit souvent rapidement par

$$\text{Aut}(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^*, \quad (5.25)$$

mais il faut bien garder à l'esprit qu'à gauche on considère le groupe additif et à droite celui multiplicatif.

Démonstration. Nous notons $[x]$ la classe de x dans $\mathbb{Z}/n\mathbb{Z}$. Nous avons $\mathbb{Z}/n\mathbb{Z} = [1]$. Soit f un automorphisme de $(\mathbb{Z}/n\mathbb{Z}, +)$; pour tout $r \in \mathbb{Z}$ nous avons

$$f([r]) = f(r[1]) = rf([1]) = [r]f([1]). \quad (5.26)$$

En particulier, vu que f est surjective, il existe un r tel que $f([r]) = [1]$. Pour un tel r nous avons $[1] = [r]f([1])$, c'est-à-dire que nous avons montré que $f([1])$ est inversible dans $((\mathbb{Z}/n\mathbb{Z})^*, \cdot)$. Nous montrons à présent que⁴

$$\begin{aligned} \sigma: \text{Aut}((\mathbb{Z}/n\mathbb{Z}, +)) &\rightarrow ((\mathbb{Z}/n\mathbb{Z})^*, \cdot) \\ f &\mapsto f([1]) \end{aligned} \quad (5.27)$$

est un isomorphisme.

Nous commençons par la surjectivité. Soit $[a] \in (\mathbb{Z}/n\mathbb{Z})^*$. Les éléments $[a]$ et $[1]$ étant tous deux des générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$, il existe un automorphisme de $\mathbb{Z}/n\mathbb{Z}$ qui envoie $[1]$ sur $[a]$ par le lemme 5.17. Cela prouve la surjectivité de σ .

En ce qui concerne l'injectivité, considérons des automorphismes f_1 et f_2 de $(\mathbb{Z}/n\mathbb{Z}, +)$ tels que $f_1([1]) = f_2([1])$. Les automorphismes f_1 et f_2 prennent la même valeur sur un générateur et donc sur tout le groupe. Donc $f_1 = f_2$.

Enfin nous prouvons que σ est un morphisme, c'est-à-dire que $\sigma(f \circ g) = \sigma(f)\sigma(g)$. Nous avons

$$f(g([1])) = f(g([1])[1]) = g([1])f([1]) = \sigma(f)\sigma(g). \quad (5.28a)$$

□

Ce dernier résultat s'étend aux groupes cycliques.

Proposition 5.19.

Si G est un groupe cyclique⁵ d'ordre n , alors

$$\text{Aut}(G) = (\mathbb{Z}/n\mathbb{Z})^*. \quad (5.29)$$

Corolaire 5.20.

Si p divise $q - 1$ alors $\text{Aut}(\mathbb{F}_q)$ possède un unique sous-groupe d'ordre p .

Démonstration. Si a est un générateur de $\mathbb{F}_q^*$ alors le groupe

$$\text{gr} \left(a^{\frac{q-1}{p}} \right) \quad (5.30)$$

est un sous-groupe d'ordre p . En ce qui concerne l'unicité, soit S un sous-groupe d'ordre p . Il est donc d'indice $(q-1)/p$ dans $\mathbb{F}_q^*$ et le lemme 3.29 nous enseigne que le groupe donné en (5.30) est contenu dans S . Il est donc égal à S parce qu'il a l'ordre de S . Le fait que S soit normal est dû au fait que $\mathbb{F}_q^*$ est abélien. □

5.4 Groupes abéliens finis

Source : [66].

Nous rappelons que l'exposant d'un groupe fini est le ppcm des ordres de ses éléments. Dans le cas des groupes abéliens finis, l'exposant joue un rôle important du fait qu'il existe un élément dont l'ordre est l'exposant. Cela est le théorème suivant.

Théorème 5.21 (Exposant dans un groupe abélien fini).

Un groupe abélien fini contient un élément dont l'ordre est l'exposant du groupe.

Démonstration. Soit G un groupe abélien fini et $x \in G$, un élément d'ordre maximum m . Nous montrons par l'absurde que l'ordre de tous les éléments de G divise m . Soit donc $y \in G$, un élément dont l'ordre ne divise pas m ; nous notons q son ordre. Vu que q ne divise pas m , le

4. Le σ donné ici est l'inverse de celui donné dans l'énoncé. Cela ne change évidemment rien à la validité de l'énoncé et de la preuve.

5. Définition 2.15.

nombre q possède au moins un facteur premier plus de fois que m : soit p premier tel que la décomposition de q contienne p^β et celle de m contienne p^α avec $\beta > \alpha$. Autrement dit,

$$m = p^\alpha m' \quad (5.31a)$$

$$q = p^\beta q' \quad (5.31b)$$

où m' et q' ne contiennent plus le facteur p . L'élément x étant d'ordre m , l'élément x^{p^α} est d'ordre m' . De la même manière, l'élément $y^{q'}$ est d'ordre p^β . Étant donné que p^β et m' sont premiers entre eux, l'élément $x^{p^\alpha} y^{q'}$ est d'ordre $p^\alpha m' > m$. D'où une contradiction avec le fait que x était d'ordre maximal.

Par conséquent l'ordre de tous les éléments de G divise celui de x qui est alors le ppcm des ordres de tous les éléments de G , c'est-à-dire l'exposant de G . $\square$

Proposition 5.22.

Soit G un groupe abélien fini et $x \in G$, un élément d'ordre maximum. Alors

(1) Il existe un morphisme $\varphi: G \rightarrow \text{gr}(x)$ tel que $\varphi(x) = x$.

(2) Il existe un sous-groupe K de G tel que $G = \text{gr}(x) \oplus K$.

Démonstration. Nous notons a l'ordre de x qui est également l'exposant du groupe G .

Nous allons prouver la première partie par récurrence sur l'ordre du groupe. Si $G = \text{gr}(x)$, alors c'est évident. Soit H un sous-groupe propre de G contenant x et tel que le problème soit déjà résolu pour H : il existe un morphisme $\varphi: H \rightarrow \text{gr}(x)$ tel que $\varphi(x) = x$. Soit $y \in G \setminus H$, d'ordre b . Nous allons trouver un morphisme $\hat{\varphi}: \text{gr}(H, y) \rightarrow \text{gr}(x)$ telle que $\hat{\varphi}(x) = x$.

Pour cela nous commençons par construire les applications suivantes :

$$\begin{aligned} \tilde{\varphi}: \mathbb{Z}/b\mathbb{Z} \times H &\rightarrow \text{gr}(x) \\ (\bar{k}, h) &\mapsto x^{kl} \varphi(h) \end{aligned} \quad (5.32)$$

où l est encore à déterminer, et

$$\begin{aligned} p: \mathbb{Z}/b\mathbb{Z} \times H &\rightarrow \text{gr}(y, H) \\ (\bar{k}, h) &\mapsto y^k h. \end{aligned} \quad (5.33)$$

Pour que $\tilde{\varphi}$ soit bien définie, il faut que a divise bl . L'application p est bien définie parce que $\bar{k}$ est pris dans $\mathbb{Z}/b\mathbb{Z}$ et que b est l'ordre de y .

Nous allons construire le morphisme $\hat{\varphi}$ en considérant le diagramme

$$\begin{array}{ccccc} \ker(p) & \hookrightarrow & \mathbb{Z}/b\mathbb{Z} \times H & \xrightarrow{p} & \text{gr}(y, H) \\ & & \downarrow \tilde{\varphi} & \swarrow \hat{\varphi} & \\ & & \text{gr}(x) & & \end{array} \quad (5.34)$$

que l'on voudra être commutatif. Vu que p est surjective, les théorèmes d'isomorphismes nous disent que

$$\text{gr}(y, H) \simeq \frac{\mathbb{Z}/b\mathbb{Z} \times H}{\ker p}. \quad (5.35)$$

Si $[\bar{k}, h]$ est la classe de $(\bar{k}, h)$ modulo $\ker(p)$ alors nous voudrions définir $\hat{\varphi}$ par

$$\hat{\varphi}([\bar{k}, h]) = \tilde{\varphi}(\bar{k}, h). \quad (5.36)$$

Pour que cela soit bien défini, il faut que si $(\bar{r}, z) \in \ker p$,

$$\hat{\varphi}([\bar{k}\bar{r}, hz]) = \hat{\varphi}([\bar{k}, h]), \quad (5.37)$$

c'est-à-dire que $\tilde{\varphi}(\bar{r}, z) = e$. Du coup la définition (5.36) n'est bonne que si et seulement si

$$\ker(p) \subset \ker(\tilde{\varphi}). \quad (5.38)$$

Nous pouvons obtenir cela en choisissant bien l .

Déterminons d'abord le noyau de p . Pour cela nous considérons un nombre β divisant b tel que $\text{gr}(y) \cap H = \text{gr}(y^\beta)$. Nous aurons $p(\bar{k}, h) = e$ si et seulement si $y^h = e$. En particulier $h = y^{-k} \in \text{gr}(y) \cap H = \text{gr}(y^\beta)$. Si $h = (y^\beta)^m = y^{m\beta}$, alors $k = -m\beta$ et nous avons

$$\ker(p) = \{(-m\beta, y^{m\beta}) \text{ tel que } m \in \mathbb{Z}\}. \quad (5.39)$$

En plus court : $\ker(p) = \text{gr}(\beta, y^{-\beta})$. Nous devons donc fixer l de telle sorte que $\tilde{\varphi}(\beta, y^{-\beta}) = e$. Étant donné que φ prend ses valeurs dans $\text{gr}(x)$, il existe un entier α tel que $\varphi(y^{-\beta}) = x^\alpha$; en utilisant cet α , nous écrivons

$$\tilde{\varphi}(\beta, y^{-\beta}) = x^{\beta l} \varphi(y^{-\beta}) = x^{\beta l + \alpha}. \quad (5.40)$$

Par conséquent nous choisissons $l = -\alpha/\beta$. Nous devons maintenant vérifier que ce choix est légitime, c'est-à-dire que a divise βl et que α/β est un entier.

Étant donné que y est d'ordre b ,

$$e = \varphi(y^b) = \varphi(y^{-\beta b/\beta}) = \varphi(y^{-\beta})^{b/\beta} = x^{b\beta/\alpha}. \quad (5.41)$$

Par conséquent a divise $\frac{b\alpha}{\beta} = -\beta l$.

Pour voir que l est entier, nous nous rappelons que a est l'exposant de G (parce que x est d'ordre maximum) et que par conséquent b divise a . Mais a divise $\alpha \frac{b}{\beta}$. Donc α/β est entier.

Nous passons maintenant à la seconde partie de la preuve. Nous considérons un morphisme $\varphi: G \rightarrow \text{gr}(x)$ tel que $\varphi(x) = x$. La première partie nous en assure l'existence. Nous montrons que

$$\begin{aligned} \psi: G &\rightarrow \text{gr}(x) \oplus \ker(\varphi) \\ g &\mapsto (\varphi(g), g\varphi(g)^{-1}) \end{aligned} \quad (5.42)$$

est un isomorphisme. D'abord $g\varphi(g)^{-1}$ est dans le noyau de φ parce que $\varphi(g)^{-1}$ étant dans $\text{gr}(x)$, et φ étant un morphisme,

$$\varphi(g\varphi(g)^{-1}) = \varphi(g)\varphi(g)^{-1} = e. \quad (5.43)$$

L'application ψ est un morphisme parce que, en utilisant le fait que G est abélien,

$$\psi(g_1 g_2) = (\varphi(g_1 g_2), g_1 g_2 \varphi(g_1 g_2)^{-1}) \quad (5.44a)$$

$$= (\varphi(g_1)\varphi(g_2), g_1 \varphi(g_1)^{-1} g_2 \varphi(g_2)^{-1}) \quad (5.44b)$$

$$= \psi(g_1)\psi(g_2). \quad (5.44c)$$

L'application ψ est injective parce que si $\psi(g) = (e, e)$ alors $\varphi(g) = e$ et $g\varphi(g)^{-1} = e$, ce qui implique $g = e$.

Enfin ψ est surjective parce qu'elle est injective et que les ensembles de départ et d'arrivée ont même cardinal. En effet par le premier théorème d'isomorphisme (théorème 2.29) appliqué à φ nous avons

$$|G| = |\text{gr}(x)| \cdot |\ker(\varphi)|. \quad (5.45)$$

□

Théorème 5.23.

Tout groupe abélien fini (non trivial) se décompose en

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/d_r\mathbb{Z} \quad (5.46)$$

avec $d_1 \geq 1$ et d_i divise d_{i+1} pour tout $i = 1, \dots, r-1$.

De plus la liste $(d_1, \dots, d_r)$ vérifiant ces propriétés est unique.

Démonstration. Soit x_1 un élément d'ordre maximal dans G . Soit n_1 son ordre et

$$H_1 = \text{gr}(x_1) = \mathbb{F}_{n_1}. \quad (5.47)$$

D'après la proposition 5.22(2), il existe un supplémentaire K_1 tel que $G = \mathbb{F}_{n_1} \oplus K_1$. Si $K_1 = \{1\}$ on s'arrête et on garde $G = \mathbb{F}_{n_1}$. Sinon on continue de la sorte en prenant x_2 d'ordre maximal dans K_1 etc.

Nous devons maintenant prouver l'unicité de cette décomposition. Soit

$$G = \mathbb{F}_{d_1} \oplus \dots \oplus \mathbb{F}_{d_r} = \mathbb{F}_{s_1} \oplus \dots \oplus \mathbb{F}_{s_q}. \quad (5.48)$$

L'exposant de G est d_r et s_q . Donc $d_r = s_q$. Les complémentaires étant égaux nous avons

$$\mathbb{F}_{d_1} \oplus \dots \oplus \mathbb{F}_{d_{r-1}} = \mathbb{F}_{s_1} \oplus \dots \oplus \mathbb{F}_{s_{q-1}}. \quad (5.49)$$

En continuant nous trouvons $r = q$ et $d_i = s_i$. $\square$

5.5 Groupes d'ordre pq

Lemme 5.24.

Soit G un groupe d'ordre pq où p et q sont des nombres premiers distincts. Nous supposons que $p < q$.

- (1) Le groupe G possède un unique q -Sylow.
- (2) Cet unique q -Sylow est normal dans G .
- (3) Il n'est ni $\{e\}$ ni G .
- (4) Le groupe G n'est pas un groupe simple⁶.

Démonstration. Soit n_q le nombre de q -Sylow; par le théorème de Sylow 5.11(1) le groupe G possède des q -Sylow et par 5.11(4),

$$n_q \in [1]_q. \quad (5.50)$$

De plus le nombre n_q divise $|G| = pq$. Donc n_q vaut p , q ou 1 . Avoir $n_q = p$ n'est pas possible parce que $n_q \in [1]_q$ et $p < q$. Avoir $n_q = q$ n'est pas possible non plus, pour la même raison. Donc $n_q = 1$. Notons H l'unique q -Sylow de G .

Le fait que H soit normal est une conséquence de 5.11(3) parce que le conjugué de H est encore un q -Sylow alors que H est l'unique q -Sylow.

Vu que

$$1 < p = |H| < pq = |G|, \quad (5.51)$$

le sous-groupe H n'est ni réduit à l'identité ni le groupe entier.

Par conséquent G n'est pas simple parce qu'il contient un sous-groupe normal non trivial. $\square$

Avant le lire le théorème suivant, n'oubliez pas de lire la définition d'un produit semi-direct 2.64.

Théorème 5.25 ([116]).

Soient deux nombres premiers distincts⁷ p et q avec $q > p$.

- (1) Si p ne divise pas $q - 1$ alors tout groupe d'ordre pq est cyclique et plus précisément le seul groupe (à isomorphisme près) d'ordre pq est $\mathbb{Z}/pq\mathbb{Z}$.
- (2) Si $p \mid q - 1$, alors il n'existe que deux groupes d'ordre pq :
 - Le groupe abélien et cyclique $\mathbb{Z}/pq\mathbb{Z}$.
 - Le produit semi-direct non abélien

$$G = \mathbb{Z}/q\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/p\mathbb{Z} \quad (5.52)$$

où $\varphi(\bar{1})$ est d'ordre p dans $\text{Aut}(\mathbb{Z}/q\mathbb{Z})$.

6. Pas de sous-groupes normaux non triviaux, 2.6.

7. Le cas $p = q$ sera traité par la proposition 5.28.

(3) Si p et q sont premiers entre eux, le produit est direct⁸.

Démonstration. Division de la preuve en plusieurs parties.

Préliminaires avec Sylow Soit un groupe G d'ordre pq . Soient H , un q -Sylow et K , un p -Sylow de G . Ils existent parce que p et q sont des diviseurs premiers de $|G|$ (théorème de Sylow 5.11). Si n_q est le nombre de q -Sylow dans G alors n_q divise $|G|$ et $n_q \equiv 1 \pmod{q}$. Donc d'abord n_q vaut 1, p ou q . Ensuite $n_q = q$ est exclu par la condition $n_q \equiv 1 \pmod{q}$; la possibilité $n_q = p$ est également impossible parce que $p \equiv 1 \pmod{q}$ est impossible avec $p < q$. Donc $n_q = 1$ et H est normal dans G .

L'ensemble $H \cap K$ est un sous-groupe à la fois de H et de K , ce qui entraîne que (théorème de Lagrange 2.35) $|H \cap K|$ divise à la fois p et q . Nous en déduisons que $|H \cap K| = 1$ et donc que $H \cap K = \{e\}$.

Étant donné que H est normal, l'ensemble HK est un sous-groupe de G . De plus l'application

$$\begin{aligned} \psi: H \times K &\rightarrow HK \\ (h, k) &\mapsto hk \end{aligned} \quad (5.53)$$

est un bijection. Nous ne devons vérifier seulement l'injectivité. Supposons que $hk = h'k'$. Alors $e = h^{-1}h'k'k^{-1}$, et donc

$$h^{-1}h' = (k'k^{-1})^{-1} \in H \cap K = \{e\}. \quad (5.54)$$

Par conséquent $|pq| = |H \times K| = |HK|$, et $HK = G$. Le corolaire 2.66 nous indique que

$$G = H \rtimes_{\varphi} K \quad (5.55)$$

où φ est l'action adjointe. Nous devons maintenant identifier cette action. En d'autres termes, nous savons que $H = \mathbb{Z}/q\mathbb{Z}$ et $K = \mathbb{Z}/p\mathbb{Z}$ et que $\varphi: \mathbb{Z}/p\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/q\mathbb{Z})$ est un morphisme. Nous devons déterminer les possibilités pour φ .

Soit n_p le nombre de p -Sylow de G . Comme précédemment, n_p vaut 1, p ou q et la possibilité $n_p = p$ est exclue. Donc n_p est 1 ou q .

Si p ne divise pas $q - 1$ Si p ne divise pas $q - 1$ alors il n'est pas possible d'avoir $n_p = q$ parce que $n_p \in [1]_p$. Or dire $n_p = q$ demanderait $q \in [1]_p$, c'est-à-dire $q = kp + 1$, qui impliquerait que p divise $q - 1$.

La seule possibilité est que $n_p = 1$. Dans ce cas, K est également normal dans G . Du coup le produit semi-direct (5.55) est en réalité un produit direct (φ est triviale) et nous avons

$$G = \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/pq\mathbb{Z}. \quad (5.56)$$

Si p divise $q - 1$ Cette fois $n_p = 1$ et $n_p = q$ sont tous deux possibles. Ce que nous savons est que $\varphi(\mathbb{Z}/p\mathbb{Z})$ est un sous-groupe de $\text{Aut}(\mathbb{Z}/q\mathbb{Z})$. Par le premier théorème d'isomorphisme 2.29, nous avons

$$|\varphi(\mathbb{Z}/p\mathbb{Z})| = \frac{|\mathbb{Z}/p\mathbb{Z}|}{|\ker \varphi|}, \quad (5.57)$$

ce qui signifie que $|\varphi(\mathbb{Z}/p\mathbb{Z})|$ divise $|\mathbb{Z}/p\mathbb{Z}| = p$. Par conséquent, $|\varphi(\mathbb{Z}/p\mathbb{Z})|$ est égal à 1 ou p . Si c'est 1, alors l'action est triviale et le produit est direct.

Nous supposons que $|\varphi(\mathbb{Z}/p\mathbb{Z})| = p$. Le corolaire 5.20 nous indique que $\text{Aut}(\mathbb{Z}/q\mathbb{Z})$ possède un unique sous-groupe d'ordre p que nous notons Γ ; c'est-à-dire que $\Gamma = \text{Image}(\varphi)$. Vu que $\varphi: \mathbb{Z}/p\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/q\mathbb{Z})$ est un morphisme, Γ est généré par $\varphi(\bar{1})$ qui est alors un élément d'ordre p , comme annoncé.

8. Cette affirmation me semble très bizarre. Comment deux nombres premiers distincts pourraient ne pas être premiers entre eux ???

Unicité Nous nous attaquons maintenant à l'unicité. Soient φ et φ' deux morphismes non triviaux $\mathbb{Z}/p\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/q\mathbb{Z})$. Étant donné que $\text{Aut}(\mathbb{Z}/q\mathbb{Z})$ ne possède qu'un seul sous-groupe d'ordre p , nous savons que $\text{Image}(\varphi) = \text{Image}(\varphi') = \Gamma$. Nous pouvons donc parler de φ'^{-1} en tant qu'application de $\mathbb{Z}/p\mathbb{Z}$ dans Γ . Nous montrons que

$$\begin{aligned} f: \mathbb{Z}/q\mathbb{Z} \times_{\varphi} \mathbb{Z}/p\mathbb{Z} &\rightarrow \mathbb{Z}/q\mathbb{Z} \times_{\varphi'} \mathbb{Z}/p\mathbb{Z} \\ (h, k) &\mapsto (h, \alpha(k)) \end{aligned} \quad (5.58)$$

où $\alpha = \varphi'^{-1} \circ \varphi$ est un isomorphisme de groupes. Le calcul est immédiat :

$$f(h_1, k_1)f(h_2, k_2) = (h_1, \alpha(k_1))(h_2, \alpha(k_2)) \quad (5.59a)$$

$$= (h_1\varphi'(\alpha(k_1))h_2, \alpha(k_1k_2)) \quad (5.59b)$$

$$= f(h_1\varphi(k_1)h_2, k_1k_2) \quad (5.59c)$$

$$= f((h_1, k_1), (h_2, k_2)). \quad (5.59d)$$

Par conséquent $\mathbb{Z}/q\mathbb{Z} \times_{\varphi} \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/q\mathbb{Z} \times_{\varphi'} \mathbb{Z}/p\mathbb{Z}$. □

Note : il existe des nombres premiers p et q tels que $q \equiv 1 \pmod{p}$. Par exemple $7 \equiv 1 \pmod{3}$.

Proposition 5.26 ([34]).

Soit G un groupe fini d'ordre pq où p et q sont deux nombres premiers distincts vérifiant

$$\begin{cases} p \not\equiv 1 \pmod{q} \\ q \not\equiv 1 \pmod{p} \end{cases} \quad (5.60a)$$

$$\quad (5.60b)$$

Alors G est cyclique, abélien et

$$G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}. \quad (5.61)$$

Démonstration. Soient n_p et n_q les nombres de p -Sylow et q -Sylow. Par le théorème de Sylow 5.11, n_p divise pq et $n_p \equiv 1 \pmod{p}$. Le second point empêche n_p de diviser p . Par conséquent n_p divise q et donc n_p vaut 1 ou q . La possibilité $n_p = q$ est exclue par l'hypothèse $q \not\equiv 1 \pmod{p}$. Donc $n_p = 1$, et de la même façon nous obtenons $n_q = 1$.

Soient S l'unique p -Sylow et T , l'unique q -Sylow. Pour les mêmes raisons que celles exposées plus haut, ce sont deux sous-groupes normaux dans G . Étant donné que S est d'ordre p^n pour un certain n et que l'ordre de S doit diviser celui de G , nous avons $|S| = p$. De la même façon, $|T| = q$. Par conséquent S est un groupe cyclique d'ordre p et nous considérons x , un de ses générateurs. De la même façon soit y , un générateur de T .

Nous montrons maintenant que x et y commutent, puis que xy engendre G . Nous savons que $S \cap T$ est un sous-groupe à la fois de S et de T , de telle façon que $|S \cap T|$ divise à la fois $|S| = p$ et $|T| = q$. Nous avons donc $|S \cap T| = 1$ et donc $S \cap T$ se réduit au neutre. Par ailleurs, S et T sont normaux, donc

$$(xyx^{-1})y^{-1} \in T \quad (5.62a)$$

$$x(yx^{-1})y^{-1} \in S, \quad (5.62b)$$

donc $xyx^{-1}y^{-1} = e$, ce qui montre que $xy = yx$.

Montrons que xy engendre G . Soit $m > 0$ tel que $(xy)^m = e$. Pour ce m nous avons $x^m = y^{-m}$ et $y^{-m} = x^m$, ce qui signifie que x^m et y^m appartiennent à $S \cap T$ et donc $x^m = y^m = e$. Les nombres p et q divisent donc tous deux m ; par conséquent $\text{ppcm}(p, q) = pq$ divise m . Nous en concluons que xy est d'ordre pq (il ne peut pas être plus) et qu'il est alors générateur.

Pour la suite nous allons d'abord prouver que $G = ST$ puis que $G \simeq S \times T$. Nous savons déjà que $|S \cap T| = 1$, ce qui nous amène à dire que $|ST| = |S||T|$. En effet si $s, s' \in S$ et $t, t' \in T$ et si $st = s't'$, alors $t = s^{-1}s't'$, ce qui voudrait dire que $s^{-1}s' \in T$ et donc que $s^{-1}s' = e$. Au final nous avons

$$|ST| = |S||T| = pq = |G|. \quad (5.63)$$

Par conséquent $G = ST$. En nous rappelant du fait que $S \cap T = \{e\}$ et que S et T sont normaux, le lemme 2.20 nous dit que $G \simeq S \times T$. Le groupe S étant cyclique d'ordre p nous avons $S = \mathbb{Z}/p\mathbb{Z}$ et pour T , nous avons la même chose : $T = \mathbb{Z}/q\mathbb{Z}$. Nous concluons que

$$G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}. \quad (5.64)$$

□

Théorème 5.27 (Théorème de Burnside[66]).

Le centre d'un p -groupe non trivial est non trivial.

Démonstration. Soit G un p -groupe non trivial. Nous considérons l'action adjointe G sur lui-même. Les points fixes de cette action sont les éléments du centre :

$$\mathcal{Z}_G = \{z \in G \text{ tel que } \sigma_x(z) = z \forall x \in G\} = \text{Fix}_G(G). \quad (5.65)$$

Nous utilisons l'équation aux classes (2.57) pour dire que $|G| = |\mathcal{Z}_G| \pmod p$. Mais $|\mathcal{Z}_G|$ n'est pas vide parce qu'il contient l'identité. Donc $|\mathcal{Z}_G|$ est au moins d'ordre p . □

Proposition 5.28.

Si p est un nombre premier, tout groupe d'ordre p ou p^2 est abélien.

Rappel : un groupe d'ordre p ou p^2 est automatiquement un p -groupe.

Démonstration. Si $|G| = p$, alors le théorème de Cauchy 5.2 nous donne l'existence d'un élément d'ordre p . Cet élément est alors automatiquement générateur, G est cyclique et donc abélien.

Si par contre G est d'ordre p^2 , alors les choses se compliquent (un peu). D'après le théorème de Burnside 5.27, le centre $\mathcal{Z}$ n'est pas trivial ; il est alors d'ordre p ou p^2 . Supposons qu'il soit d'ordre p et prenons $x \in G \setminus \mathcal{Z}$. Alors le stabilisateur de x pour l'action adjointe contient au moins $\mathcal{Z}$ et x , c'est-à-dire que $|\text{Fix}_G(x)| \geq p + 1$. Étant donné que $\text{Fix}_G(x)$ est un sous-groupe, son ordre est automatiquement 1, p ou p^2 . En l'occurrence, il doit être p^2 (parce que plus grand que p), et donc x doit être central, ce qui est une contradiction. □

5.6 Groupe symétrique, groupe alterné

La définition des permutations et du groupe symétrique sont 1.146. Voir aussi le thème 64.

5.6.1 Le groupe alterné

Définition 5.29.

*Le groupe A_n des permutations paires⁹ dans S_n est la **groupe alterné**.*

Proposition 5.30.

À propos du groupe alterné dans le groupe symétrique.

- (1) *Le groupe alterné A_n est un sous-groupe caractéristique¹⁰ de S_n*
- (2) *Le sous-groupe A_n est d'indice 2 dans S_n .*
- (3) *Le sous-groupe A_n est l'unique sous-groupe d'indice¹¹ 2 de S_n .*

Démonstration. Soit $\alpha \in \text{Aut}(S_n)$. Étant donné que $\epsilon \circ \alpha$ est un homomorphisme surjectif sur $\{-1, 1\}$, par unicité de cet homomorphisme, nous avons $\epsilon \circ \alpha = \epsilon$, et donc $\alpha(A_n) = A_n$. Par le premier théorème d'isomorphisme 2.29, il existe un isomorphisme

$$f: S_n / \ker(\epsilon) \rightarrow \text{Image}(\epsilon). \quad (5.66)$$

9. Définition 1.157.

10. Définition 2.4.

11. Définition 2.34.

En égalant le nombre d'éléments nous avons $|S_n : \ker \epsilon| = |S_n : A_n| = 2$.

Nous prouvons maintenant l'unicité. Soit H un sous-groupe d'indice 2 dans S_n . Par le lemme 3.28, H est distingué et nous pouvons considérer le groupe S_n/H . Ce dernier ayant 2 éléments, il est isomorphe à $\{-1, 1\}$. Soit θ l'isomorphisme. On note φ le morphisme canonique $\varphi : S_n \rightarrow S_n/H$:

$$S_n \xrightarrow{\varphi} S_n/H \xrightarrow{\theta} \{-1, 1\}. \quad (5.67)$$

La composition $\varphi \circ \theta$ est alors un homomorphisme surjectif de S_n sur $\{-1, 1\}$ et nous avons $\varphi \circ \theta = \epsilon$ par la proposition 1.159. L'enchaînement (5.67) nous montre que $H = \ker(\theta \circ \varphi) = \ker(\epsilon) = A_n$. $\square$

Proposition 5.31 ([117]).

Le groupe symétrique S_n peut être écrit comme un produit semi-direct¹² du groupe alterné :

$$S_n = A_n \rtimes_{\varphi} \mathbb{Z}/2\mathbb{Z} \quad (5.68)$$

où l'action de $\mathbb{Z}/2\mathbb{Z}$ sur A_n est la conjugaison par $\sigma = (12)$, c'est-à-dire $\rho(-1)\tau = \sigma\tau\sigma^{-1}$.

Démonstration. Nous avons la suite exacte

$$1 \xrightarrow{i} A_n \xrightarrow{i} S_n \xrightarrow{\epsilon} \{\pm 1\} \longrightarrow 1 \quad (5.69)$$

où les i représentent des inclusions et ϵ est la signature définie en 1.151. Grâce à cette suite et au fait que la signature soit un isomorphisme à partir de la partie $\{\text{Id}, \sigma\}$ (pour σ d'ordre 2, par exemple $\sigma = (12)$), le théorème 2.65 nous dit que

$$S_n \simeq A_n \rtimes_{\varphi} \{\text{Id}, \sigma\} \quad (5.70)$$

où φ est l'action adjointe de $\{\text{Id}, \sigma\}$ sur A_n . $\square$

Proposition 5.32.

Si $\beta \in S_n$ est une transposition, nous avons les égalités suivantes d'ensembles :

$$S_n = A_n \cup A_n\beta = A_n \cup \beta A_n. \quad (5.71)$$

Démonstration. Les parties A_n et βA_n ont le même nombre d'éléments. En effet, l'application

$$\begin{aligned} \varphi : A_n &\rightarrow A_n\beta \\ \sigma &\mapsto \sigma\beta \end{aligned} \quad (5.72)$$

est une bijection.

De plus ces deux ensembles sont disjoints à cause de la proposition 1.159. En effet si $\sigma \in A_n$, alors $\epsilon(\sigma) = 1$. Mais un élément de $A_n\beta$ est de la forme $\sigma\beta$ avec $\sigma \in A_n$. Or ϵ est une homomorphisme, donc $\epsilon(\sigma\beta) = \epsilon(\sigma)\epsilon(\beta) = -1$.

Enfin, la proposition 5.30(2) dit que A_n est d'indice deux dans S_n . Donc la partie

$$A_n \cup A_n\beta \quad (5.73)$$

contient $|S_n|/2 + |S_n|/2 = |S_n|$ éléments. C'est donc S_n . $\square$

Lemme 5.33.

Le groupe dérivé du groupe symétrique est le groupe alterné : $D(S_n) = A_n$.

Démonstration. Tout élément de $D(S_n)$ s'écrit sous la forme $ghg^{-1}h^{-1}$. Quel que soit le nombre de transpositions dans g et h , le nombre de transpositions dans $[g, h]$ est pair. $\square$

Proposition 5.34 ([118]).

Soit $n \geq 3$. Les 3-cycles $c_i = (1, 2, i)$ avec $i = 3, \dots, n$ engendrent le groupe alterné A_n .

12. Définition 2.64.

Démonstration. Soit H , le groupe engendré par les c_i . D'abord nous avons

$$c_i = (1, 2, i) = (1, 2)(2, i), \quad (5.74)$$

de telle sorte que $\epsilon(c_i) = 1$. Par conséquent nous avons $H \subset A_n$. Nous montrons par récurrence que $A_n \subset H$.

Pour $n = 3$ il suffit de vérifier que $A_3 = \{\text{Id}, c_3, c_3^2\}$. Supposons avoir obtenu le résultat pour A_{n-1} , et prouvons le pour A_n . Soit $s \in A_n$.

Si $s(n) = n$, alors s se décompose de la même manière que sa restriction s' à $\{1, \dots, n-1\}$. Par l'hypothèse de récurrence, cette restriction, appartenant à A_{n-1} , se décompose en produit des $c_3, \dots, c_{n-1}$ et de leurs inverses.

Si $s(n) = k$ alors nous considérons l'élément $c_n^2 c_k s$. Cet élément envoie n sur n et peut donc être décomposé avec les c_i ($i = 1, \dots, n-1$) en vertu du point précédent. $\square$

Proposition 5.35.

Lorsque $n \geq 5$, tous les 3-cycles de A_n sont conjugués. Autrement dit, la classe de conjugaison d'un 3-cycle est l'ensemble des 3-cycles.

Démonstration. Soient les 3-cycles $\sigma = (i_1, i_2, i_3)$ et $\varphi = (j_1, j_2, j_3)$. Nous considérons une bijection α de $\{1, \dots, n\}$ telle que $\alpha(i_s) = j_s$. Nous avons immédiatement que $\alpha \in S_n$ et que $\alpha\sigma\alpha^{-1} = \varphi$. Donc les 3-cycles sont conjugués dans S_n . Il reste à prouver qu'ils le sont dans A_n .

Si α est une permutation paire, la preuve est terminée. Si α est impaire, alors nous devons un peu la modifier. Vu que $n \geq 5$, nous pouvons prendre s et t , des éléments distincts dans $\{1, \dots, n\} \setminus \{j_1, j_2, j_3\}$ et poser $\tau = (st)$. Vu que la signature est un homomorphisme et que τ et α sont impairs, l'élément $\tau\alpha$ est pair (lemme et proposition 1.158 et 1.156) et est donc dans A_n . Les supports de τ et φ étant disjoints, ces derniers commutent et nous avons

$$(\tau\alpha)\sigma(\tau\alpha)^{-1} = \tau(\alpha\sigma\alpha^{-1})\tau^{-1} = \tau\varphi\tau^{-1} = \varphi. \quad (5.75)$$

Donc σ et φ sont conjugués par $\tau\alpha$ qui est dans A_n . $\square$

Théorème 5.36 ([34]).

Le groupe alterné A_n est simple¹³ pour $n \geq 5$.

Démonstration. Soit N , un sous-groupe normal de A_n non réduit à l'identité. Étant donné que les 3-cycles engendrent A_n (proposition 5.34) et que tous les 3-cycles sont conjugués dans A_n (proposition 5.35), il suffit de montrer que N contient un 3-cycle. En effet si N contient un 3-cycle, le fait qu'il soit normal implique (par conjugaison) qu'il les contienne tous et donc qu'il contient une partie génératrice de A_n .

Soit donc $\sigma \in N$ différent de l'identité. Nous prenons i dans le support de σ et $j = \sigma(i)$. Nous choisissons ensuite $k \in \{1, \dots, n\} \setminus \{i, j, \sigma^{-1}(i)\}$ et $m = \sigma(k)$. Nous considérons la permutation $\alpha = (ijk)$. Étant donné que N est normal l'élément

$$\theta = (\alpha^{-1}\sigma\alpha)\sigma^{-1} \quad (5.76)$$

est dans N . De plus en utilisant le lemme 1.152 et le fait que $\alpha^{-1} = (ikj)$ nous avons

$$\theta = (ikj)(j\sigma(j)m). \quad (5.77)$$

Cela n'est pas spécialement un 3-cycle, mais nous allons en construire un. Nous allons déterminer que θ est soit un 5-cycle, soit un 3-cycle, soit un 2×2 -cycle suivant les valeurs de $\sigma(j)$ et m .

Souvenons-nous que nous avons :

- $i \neq j = \sigma(i)$, puisque i est dans le support de σ ;
- $k \neq i$ et $k \neq j$, par définition de k (rappelons aussi que $k \neq \sigma^{-1}(i)$) ;

13. Pas de sous-groupes normaux non triviaux, définition 2.6.

— $m \neq i$, $m \neq j$ et $m \neq \sigma(j)$ puisque $m = \sigma(k)$.

Il ne nous reste alors seulement les deux possibilités suivantes :

- (1) soit $m = k$, soit $m \neq k$, d'une part ;
- (2) soit $\sigma(j) = i$, soit $\sigma(j) = k$, soit $\sigma(j)$ n'est ni i , ni k , ni m , d'autre part.

Supposons dans un premier temps que $m = k$; alors

$$\theta = (ik)(j\sigma(j)). \quad (5.78)$$

C'est à priori un 2×2 -cycle. Mais si de plus $\sigma(j) = i$, alors

$$\theta = (ijk) \quad (5.79)$$

qui est un 3-cycle ; et si $\sigma(j) = k$, alors

$$\theta = (ikj) \quad (5.80)$$

qui est un autre 3-cycle.

Supposons à présent que $m \neq k$. Si $\sigma(j)$ n'est ni i , ni k , ni m , alors $i, j, k, \sigma(j)$ et m sont cinq nombres différents, et

$$\theta = (i, j, \sigma(j), m, k) \quad (5.81)$$

est un 5-cycle. Si $\sigma(j) = i$, alors

$$\theta = (ikj)(jim) = (imk) \quad (5.82)$$

qui est un 3-cycle. Si $\sigma(j) = k$, alors

$$\theta = (ikj)(jkm) = (ikm) \quad (5.83)$$

qui est encore un 3-cycle.

Bref nous avons montré que θ est soit un 3-cycle, soit un 5-cycle, soit un 2×2 -cycle. Si θ est un 3-cycle, la preuve est terminée.

Si $\theta = (ab)(cd)$, alors on considère $e \in \{1, \dots, n\} \setminus \{a, b, c, d\}$ et nous avons

$$\underbrace{(abe)^{-1}\theta(abe)}_{\in N}\theta^{-1} = (aeb)(ab)(cd)(abe)(an)(cd) = (abe) \in N. \quad (5.84)$$

Si θ est le 5-cycle $(abcde)$, alors l'élément suivant est dans N :

$$(abc)^{-1}\theta(abc)\theta^{-1} = (acb)(abcde)(abc)(aedcb) = (acd). \quad (5.85)$$

Dans tous les cas nous avons trouvé un 3-cycle dans N et nous avons par conséquent $N = A_n$, ce qui fait que A_n ne contient pas de sous-groupes normaux non triviaux. Le groupe alterné A_n est donc simple. $\square$

Nous en déduisons immédiatement que si $n \geq 5$, le groupe dérivé de A_n est A_n parce que A_n ne contient pas d'autres sous-groupes non triviaux.

Lemme 5.37.

Le groupe alterné¹⁴ A_6 n'accepte pas de sous-groupes normaux d'ordre 60.

Démonstration. Soit G normal dans A_6 , et a , un élément d'ordre 5 dans G (qui existe parce que 5 divise 60). Soit aussi un élément b d'ordre 5 dans A_6 . Les groupes $\text{gr}(a)$ et $\text{gr}(b)$ sont deux 5-Sylow dans A_6 . En effet, 5 un nombre premier et est la plus grande puissance de 5 dans la décomposition de 60 ; donc $\text{gr}(a)$ est un 5-Sylow dans G . D'autre part, l'ordre de A_6 (qui est $\frac{1}{2}6!$) ne possède également que 5 à la puissance 1 dans sa décomposition.

En vertu du théorème de Sylow 5.11(3), les 5-Sylow $\text{gr}(a)$ et $\text{gr}(b)$ sont conjugués et il existe $\tau \in A_6$ tel que $b = \tau a \tau^{-1}$. Mais G étant normal dans A_6 , l'élément $\tau a \tau^{-1}$ est encore dans G , de telle sorte que $b \in G$. Du coup G doit contenir tous les éléments d'ordre 5 de A_6 .

14. Définition 5.29.

Les éléments d'ordre 5 de A_6 doivent fixer un des points de $\{1, 2, 3, 4, 5, 6\}$ puis permuter les autres de façon à n'avoir qu'un seul cycle. Un cycle correspond à écrire les nombres 1, 2, 3, 4, 5 dans un certain ordre. Ce faisant, le premier n'a pas d'importance parce qu'on considère la permutation cyclique, par exemple (3, 5, 2, 1, 4) est la même chose que (5, 2, 1, 4, 3). Le nombre de cycles sur $\{1, 2, 3, 4, 5\}$ est donc de $4!$, et par conséquent le nombre d'éléments d'ordre 5 dans A_6 est $6 \cdot 4! = 144$.

Le groupe G doit contenir au moins 144 éléments alors que par hypothèse il en contient 60 ; contradiction. $\square$

Le théorème suivant montre que tout groupe peut être vu, en agissant sur lui-même, comme une partie du groupe symétrique.

Théorème 5.38.

Un groupe G est isomorphe à un sous-groupe de son groupe symétrique $S(G)$.

Démonstration. Nous considérons φ , la translation à gauche :

$$\begin{aligned} \varphi: G &\rightarrow S(G) \\ g &\mapsto t_g \end{aligned} \tag{5.86}$$

où $f_g(h) = gh$. Étant donné que

$$\varphi(gh) = ghx = g(t_h x) = t_g \circ t_h(x), \tag{5.87}$$

l'application φ est un morphisme de groupes. Il est injectif parce que si $gx = hx$ pour tout x , en particulier pour $x = e$ nous trouvons $g = h$.

De la même manière, $\varphi(g)x = \varphi(g)y$ implique $x = y$. Cela montre que l'image est bien dans le groupe symétrique.

L'ensemble $\text{Image}(\varphi)$ est donc un sous-groupe de $S(G)$, et φ est un isomorphisme vers ce groupe. $\square$

Lemme 5.39.

Si $n \geq 3$, alors

- (1) *Le centre de S_n est trivial.*
- (2) *Le groupe S_n est non abélien.*

Démonstration. Soit $s \in Z(S_n)$ et trois éléments distincts a, b et c de $\{1, \dots, n\}$. Nous posons $\tau = (ab)$ et nous avons $s\tau = \tau s$. En notant $a' = s(a)$ et $b' = s(b)$ nous avons

$$a' = s(a) = (\tau s \tau^{-1})(a) = (\tau s)(b) = \tau(b') \tag{5.88a}$$

$$b' = s(b) = (\tau s \tau^{-1})(b) = (\tau s)(a) = \tau(a'). \tag{5.88b}$$

Donc τ permute a' et b' . Mais comme τ ne permute que a et b , en tant qu'ensembles, $\{a, b\} = \{s(a), s(b)\}$. Le même raisonnement sur $\{b, c\}$ donne $\{b, c\} = \{s(b), s(c)\}$. Et vu que a, b et c sont distincts,

$$\{b\} = \{b, c\} \cap \{a, b\} = \{s(b)\}. \tag{5.89}$$

Cela montre que $s(b) = b$, et donc que le centre de S_n est réduit à la permutation identité.

En ce qui concerne le fait que S_n est non abélien, si nous avons $st = ts$ pour tout $s, t \in S_n$ alors $s = tst^{-1}$ pour tout t . Alors s serait dans le centre de S_n . En bref, si S_n était abélien, son centre serait S_n et non $\{\text{Id}\}$. $\square$

Proposition 5.40 ([119, 114]).

Tout groupe simple¹⁵ d'ordre 60 est isomorphe au groupe alterné A_5 .

15. Définition 2.6.

Démonstration. Nous avons la décomposition en nombres premiers $60 = 2^2 \cdot 3 \cdot 5$. Déterminons pour commencer le nombre n_5 de 5-Sylow dans G . Le théorème de Sylow 5.11(4) nous renseigne que n_5 doit diviser 60 et doit être égal à 1 mod 5. Les deux seules possibilités sont $n_5 = 1$ et $n_5 = 6$. Étant donné que tous les p -Sylow sont conjugués, si $n_5 = 1$ alors le 5-Sylow serait un sous-groupe invariant à l'intérieur de G , ce qui est impossible vu que G est simple. Donc $n_5 = 6$.

Par le point (3) du théorème de Sylow, le groupe G agit transitivement sur l'ensemble des 5-Sylow par l'action adjointe :

$$g \cdot S = gSg^{-1}. \quad (5.90)$$

Cela donne donc un morphisme $\theta: G \rightarrow S_6$. Le noyau de θ est un sous-groupe normal. En effet si $k \in \ker \theta$ et si $g \in G$ nous avons

$$(gkg^{-1}) \cdot S = gkg^{-1}Ggk^{-1}g^{-1} \quad (5.91a)$$

$$= gkTk^{-1}g^{-1} \quad (5.91b)$$

$$= gTg^{-1} \quad (5.91c)$$

$$= S \quad (5.91d)$$

où T est le Sylow $T = g^{-1}Sg$. Étant donné que $k \in \ker \theta$ nous avons utilisé $kTk^{-1} = aT$. Au final $gkg^{-1} \cdot S = S$, ce qui prouve que $gkg^{-1} \in \ker \theta$.

Étant donné que $\ker \theta$ est normal dans G , soit est soit réduit à $\{e\}$ soit il vaut G . La seconde possibilité est exclue parce qu'elle reviendrait à dire que G agit trivialement, ce qui n'est pas correct étant donné qu'il agit transitivement. Nous en déduisons que $\ker \theta = \{e\}$, que θ est injective et que G est isomorphe à un sous-groupe de S_6 .

Par ailleurs le groupe dérivé de G est un sous-groupe normal (et non réduit à l'identité parce que G est non commutatif). Donc $D(G) = G$. Étant donné que $G \subset S_6$, nous avons

$$G = D(G) \subset D(S_6) = A_6 \quad (5.92)$$

parce que le groupe dérivé du groupe symétrique est le groupe alterné (lemme 5.33).

L'ensemble $\theta^{-1}(A_6)$ est distingué dans G . En effet si $\sigma \in A_6$ et si $g \in G$ nous avons

$$\theta(g\theta^{-1}(\sigma)g^{-1}) = \theta(g)\sigma\theta(g)^{-1} \in A_6. \quad (5.93)$$

Nous en déduisons que $\theta^{-1}(A_6)$ est soit G entier soit réduit à $\{e\}$. Si $\theta^{-1}(A_6) = \{e\}$, alors pour tout $g \in G$ nous aurions $g^2 = e$ parce que $\theta(g^2) \in A_6$. L'ordre de G étant 60, il n'est pas possible que tous ses éléments soient d'ordre 2. Nous en déduisons que $\theta(G) \subset A_6$.

Nous nommons $H = \theta(G)$ et nous considérons l'ensemble $X = A_6/H$ où les classes sont prises à gauche, c'est-à-dire

$$[\sigma] = \{h\sigma \text{ tel que } h \in H\}. \quad (5.94)$$

Évidemment A_6 agit sur X de façon naturelle. Au niveau de la cardinalité,

$$\text{Card}(X) = \frac{|A_6|}{|H|} = \frac{360}{60} = 6. \quad (5.95)$$

Le groupe A_6 agit sur X qui a 6 éléments. Nous avons donc une application $\varphi: A_6 \rightarrow A_6$. Encore une fois, la simplicité de A_6 montre que $\varphi(A_6) = A_6$.

Nous étudions maintenant $\varphi(H)$ agissant sur X . Un élément $x \in A_6$ fixe la classe de l'unité $[e]$ si et seulement si $x \in H$ et par conséquent $\varphi(H)$ est la fixateur de $[e]$ dans X . À la renumérotation près, nous pouvons identifier $\varphi(H)$ au sous-groupe de A_6 agissant sur $\{1, \dots, 6\}$ et fixant 6. Nous avons alors $\varphi(H) = S_5 \cap A_6 = A_5$. Nous venons de prouver que φ fournit un isomorphisme entre A_5 et H . Étant donné que H était isomorphe à G , nous concluons que G est isomorphe à A_6 . $\square$

5.6.2 Sous-groupes normaux

5.41 ([120]).

Soit le groupe V_4 engendré par les bitranspositions de S_4 . Nous savons de l'exemple 1.155(5) que ce groupe contient exactement 3 éléments non triviaux et l'identité. De plus, comme c'est une classe de conjugaison, V_4 est normal dans S_4 .

Lemme 5.42.

Les sous-groupes $\text{Fix}_{S_n}(a)$ (avec $a \in \{1, \dots, n\}$) sont conjugués entre eux.

Démonstration. Soit $\sigma \in \text{Fix}(a)$ et $s \in S_n$ nous devons prouver que $s\sigma s^{-1}$ est le fixateur d'un élément de $\{1, \dots, n\}$. Nous notons $s(a) = b$. Alors

$$(s\sigma s^{-1})(b) = (s\sigma)(a) = s(a) = b. \quad (5.96)$$

Donc $s \text{Fix}(a) s^{-1} \subset \text{Fix}(b)$.

Dans l'autre sens, si $\sigma \in \text{Fix}(b)$ alors $s^{-1}\sigma s \in \text{Fix}(a)$. Mais $\sigma = s(s^{-1}\sigma s)s^{-1}$, donc $\sigma \in s \text{Fix}(a) s^{-1}$. $\square$

Proposition 5.43 (Sous-groupes normaux de S_n [120]).

Les sous-groupes normaux de S_n ne sont pas légions.

- (1) Pour $n = 4$, les sous-groupes normaux de S_4 sont $\{\text{Id}\}$, V_4 , A_4 et S_4 .
- (2) Pour $n \neq 4$, les sous-groupes normaux de S_n sont $\{\text{Id}\}$, A_n et S_n .

Démonstration. Les cas $n \leq 2$ sont un peu triviaux, donc nous faisons $n \geq 3$. Soit H normal dans S_n et $s \neq \text{Id}$ dans H ; par le lemme 5.39, s n'est pas dans le centre de S_n et il existe $u \in S_n$ tel que $us \neq su$. Vu que u est un produit de transpositions (proposition 1.156), il existe une transposition t telle que $st \neq ts$. Le sous-groupe H est normal et que $s \in H$ nous avons aussi $ts^{-1}t^{-1} \in H$. Mais en même temps, la combinaison sts^{-1} est le conjugué d'une transposition et est donc également une transposition (classe de conjugaison de S_4 dans 1.155). Nous en concluons que $sts^{-1}t^{-1}$ est un produit de deux transpositions appartenant à H .

Nous venons de prouver que H contient au moins un produit de deux transpositions. Et ce produit est différent de Id parce que $sts^{-1}t^{-1} = \text{Id}$ impliquerait $st = ts$.

Soient donc deux transpositions $t_1, t_2 \in H$ telles que $t_1 t_2 \neq \text{Id}$. Les supports de t_1 et t_2 ont soit 1 soit aucun élément communs.

Premier cas Supposons $t_1 = (a, b)$, $t_2 = (b, c)$ avec a, b, c distincts dans $\{1, \dots, n\}$. Dans ce cas $t_1 t_2 = (a, b, c)$ et H contient un cycle de longueur 3. Vu que H est normal et que les cycles de longueur trois sont une classe de conjugaison (exemple 1.155) et que A_n est engendré par ceux-ci (proposition 5.34), $A_n \subset H$. Mais A_n est d'indice deux dans S_n (proposition (2)(2)). Quel nombre plus grand que $n!/2$ divise $n!$? Seulement n lui-même. Donc H est soit A_n soit S_n .

Second cas Le groupe H contient un élément de la forme $(ab)(cd)$ avec a, b, c, d distincts dans $\{1, \dots, n\}$.

Si $n = 3$ Impossible parce que avec $n = 3$ nous n'avons pas quatre éléments distincts.

Si $n = 4$ Le sous-groupe H de S_4 contient un élément de V_4 qui n'est pas l'identité. Par normalité et classes de conjugaison, H contient V_4 . Nous devons maintenant prouver que si H n'est pas V_4 alors H est A_4 ou S_4 . Nous avons les inclusions $V_4 \subset H \subset S_4$ et donc les inégalités

$$4 \leq |H| \leq 24. \quad (5.97)$$

Donc le nombre $|H|$ est un multiple de 4 qui divise 24. Les possibilités sont $|H| = 4, 8, 12, 24$. La possibilité $|H| = 4$ donne $H = V_4$; si $|H| = 24$ alors $H = S_4$; si $|H| = 12$ alors H est d'indice 2 dans S_4 et $H = A_4$ (proposition 5.30(3)). Quid de $|H| = 8$?

D'après le corolaire 2.36 au théorème de Lagrange, l'ordre d'un élément divise l'ordre du groupe. Soit x dans H mais pas dans V_4 . L'ordre de x peut être 1, 2, 4 ou 8. Ordre 1 serait $x = \text{Id}$. Ordre 8, pas possible parce que S_4 n'a pas d'éléments d'ordre 8.

x d'ordre 2 Prenons la décomposition de x en cycles disjoints. Vu qu'on est dans S_4 , ces cycles ne peuvent être que des transpositions. Soit il y en a un (alors H contient une transposition et donc $H = S_4$), soit il y en a deux et alors x est dans V_4 .

x d'ordre 4 L'élément x serait alors un cycle de longueur 4. Et alors H contient tous les cycles de longueur 4. Par exemple il contient le produit $(abcd)(bacd) = (adc)$. Le sous-groupe H contient alors A_4 (parce qu'il contient tous les 3-cycles).

Si $n \geq 5$ Soit un élément e distinct de a, b, c et d . Par notre liste préférée des classes de conjugaisons (exemple 1.155(5)), le 2-cycle $(c, e)(a, b)$ est conjugué à $(a, b)(c, d)$ et appartient donc à H . Mais alors le produit suivant est également dans H :

$$(ce)(ab)(ab)(cd) = (ce)(cd) = (ecd). \quad (5.98)$$

Donc H contient un 3-cycle, et par conséquent tous les 3-cycles. Encore une fois, cela prouve que H est soit A_n soit S_n .

Pourquoi $n = 4$ est spécial ? Dans le premier cas, nous montrons tout de suite que $H = V_4$ n'est pas possible. Dans le deuxième cas, nous montrons que, grâce à un élément différent de a, b, c et d , la possibilité $H = V_4$ est exclue. La possibilité $H = V_4$ n'existe que pour $n = 4$. □

5.6.3 Indice

Théorème 5.44.

Tout sous-groupe d'indice n dans S_n est isomorphe à S_n .

Démonstration. Pour $n = 1$, il n'y a rien. Pour $n = 2$, un sous-groupe d'indice 2 ne peut contenir que 1 élément qui est donc l'identité. Ok pour que $\{\text{Id}\}$ soit égal à S_1 ?

Pour les autres, il y a un peu plus de travail.

Pour $n = 3$ Nous avons $|S_3| = 6$. Donc un sous-groupe d'indice 3 dans S_3 contient exactement 2 éléments. Il contient Id et un autre élément $\sigma \in S_3$ qui doit vérifier $\sigma^2 = \text{Id}$ ou $\sigma^2 = \sigma$. Aucun élément de S_3 ne vérifie $\sigma^2 = \sigma$ (à part l'identité). Donc $\sigma^2 = \text{Id}$, ce qui fait que σ est une transposition. Donc

$$H = \{\text{Id}, (12)\} \quad (5.99)$$

ou l'identité avec (23) ou avec (13) . Dans tous les cas c'est isomorphe à S_2 .

Pour $n = 4$ Nous avons $|S_4 : H| = 4$, donc $|H| = 6$. Mais $6 = 2 \times 3$ et $2 \mid 3 - 1$, donc le théorème 5.25 nous dit que H est soit cyclique¹⁶ (et donc abélien), soit un produit semi-direct. Vu que S_4 n'a pas d'éléments d'ordre 6, aucun sous-groupe d'ordre 6 ne peut être cyclique. Nous sommes donc dans le cas du produit semi-direct

$$H = \mathbb{Z}_3 \rtimes_{\varphi} \mathbb{Z}_2 \quad (5.100)$$

où $\varphi: \mathbb{Z}_2 \rightarrow \text{Aut}(\mathbb{Z}_3)$ et $\varphi(1)$ est d'ordre 2 dans $\text{Aut}(\mathbb{Z}_3)$. Il convient de nous attarder un peu pour être sûr d'avoir bien compris tout ce qui se trouve dans l'identification (5.100). D'abord un point de notations : ici nous considérons les groupes $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ munis de l'addition. Donc 1 n'est pas le neutre. Ensuite nous savons du théorème 5.18 que $\text{Aut}(\mathbb{Z}/3\mathbb{Z}) = (\mathbb{Z}/3\mathbb{Z})^*$, et que via cette identification, $\varphi(1) = 2 \in (\mathbb{Z}/3\mathbb{Z})^*$ au sens où $\varphi(1)x = 2x$. Nous avons alors $\varphi(1)^2x = 4x = x$ dans $\mathbb{Z}/3\mathbb{Z}$. Cela montre bien que $\varphi(1)$ est d'ordre 2.

Par rapport à la proposition 5.31, ici nous écrivons $\mathbb{Z}_2 = (\{0, 1\}, +)$ alors que là nous écrivons $\mathbb{Z}_2 = (\{-1, 1\}, \cdot)$. Ce sont les mêmes groupes, mais il convient de remarquer que le 1 ici est le -1 là.

Nous savons par la proposition 5.31 que $S_n = A_n \rtimes_{\varphi} \mathbb{Z}_2$; en comparant avec (5.100) nous voyons qu'il suffit de prouver que $A_3 = \mathbb{Z}/3\mathbb{Z}$ pour avoir $H = S_3$.

16. Définition 2.15.

Le groupe A_3 possède $|S_3|/2 = 3$ éléments. Il est vite vu que $A_3 = \{\text{Id}, (12)(31), (12)(32)\}$: ce sont trois éléments de signature paire dans S_3 ; donc c'est A_3 . La correspondance $\text{Id} \mapsto 0$, $(12)(13) \mapsto 1$, $(13)(12) \mapsto 2$ donne un isomorphisme avec $(\mathbb{Z}_3, +)$.

Pour $n \geq 5$ Soit un sous-groupe H d'indice n dans S_n et l'action à gauche de S_n sur $E = S_n/H$ (qui n'est à priori pas un groupe) donnée par $g \cdot [s] = [gs]$.

Morphisme $\varphi: S_n \rightarrow S_E$ Le φ défini par l'action est un morphisme parce que

$$\varphi(g_1 g_2)[s] = [g_1 g_2 s] = \varphi(g_1)[g_2 s] = \varphi(g_1)\varphi(g_2)[s]. \quad (5.101)$$

Mais il faut également vérifier que pour chaque $g \in G$, l'application $\varphi(g): E \rightarrow E$ est bien une permutation. Pour l'injectivité, si $\varphi(g)[s_1] = \varphi(g)[s_2]$ alors $[gs_1] = [gs_2]$, donc il existe $h \in H$ tel que $gs_1 = gs_2 h$, ce qui prouve que $s_1 = s_2 h$ et donc que $[s_1] = [s_2]$. Pour la surjectivité, soit $[t] \in S_n/H$ et résolvons $\varphi(g)[s] = [t]$ par rapport à s . L'élément $s = g^{-1}t$ fonctionne.

ker(φ) est normal Soit $z \in \ker(\varphi)$, c'est-à-dire que $\varphi(z) = \text{Id}_E$. Alors pour $\sigma \in S_n$ nous avons $\varphi(\sigma z \sigma^{-1}) = \varphi(\sigma)\varphi(z)\varphi(\sigma^{-1}) = \text{Id}_E$.

$\ker(\varphi) = \bigcap_{g \in S_n} gHg^{-1}$ Supposons que $z \in gHg^{-1}$ pour tout g , et calculons $\varphi(z)[s]$. D'abord par hypothèse il existe $h \in H$ tel que $z = shs^{-1}$, donc

$$\varphi(z)[s] = [zs] = [zhs^{-1}s] = [s], \quad (5.102)$$

ce qui prouve que $\varphi(z) = \text{Id}$.

Dans l'autre sens, soit $z \in \ker(\varphi)$. Donc $\varphi(z)[s] = [s]$. Il existe donc $h \in H$ tel que $zs = sh$, c'est-à-dire tel que $z = shs^{-1}$. La formule demandée est donc prouvée.

Questions d'ordre Nous savons que $|H| = (n-1)!$ alors que $|A_n| = \frac{n!}{2}$. Donc $|H| < |A_n|$ avec une inégalité stricte. En même temps nous avons $|\ker(\varphi)| \leq |H|$ parce que $\ker(\varphi)$ est une intersection dont un des termes est H lui-même. Nous avons alors les inégalités

$$|\ker(\varphi)| \leq |H| = (n-1)! < |A_n|. \quad (5.103)$$

Mais le seul sous-groupes normaux de S_n sont A_n et S_n et $\{\text{Id}\}$ (proposition 5.43). Donc $\ker(\varphi) = \text{Id}$ et φ est une injection entre deux ensembles finis de même cardinalité. Cela fait de φ une bijection et donc un isomorphisme de groupes

$$\varphi: S_n \rightarrow S_E. \quad (5.104)$$

Soit une fonction de numérotation $\psi: E \rightarrow \{1, \dots, n\}$. Avec cela nous définissons un isomorphisme de groupes

$$\begin{aligned} \tilde{\psi}: S_E &\rightarrow S_n \\ \sigma &\mapsto \psi\sigma\psi^{-1}. \end{aligned} \quad (5.105)$$

Fixateur Nous montrons à présent que $(\tilde{\psi} \circ \varphi)(H) = \text{Fix}(\psi[\text{Id}])$ où le stabilisateur est pris dans S_n . Pour la première inclusion, soit $h \in H$. Nous avons $(\tilde{\psi} \circ \varphi)(h) = \psi \circ \varphi(h)\psi^{-1}$, qui nous appliquons à $\psi[\text{Id}]$:

$$(\tilde{\psi} \circ \varphi)(h)\psi[\text{Id}] = \psi \circ \varphi(h)[\text{Id}] = \psi[h] = \psi[\text{Id}]. \quad (5.106)$$

Donc $(\tilde{\psi} \circ \varphi)(H) \subset \text{Fix}(\psi[\text{Id}])$.

Pour l'autre inclusion, soit $\sigma \in S_n$ tel que $\sigma\psi[\text{Id}] = \psi[\text{Id}]$. Vu que $\sigma \in S_n$ nous avons $s \in S_E$ tel que $\sigma = \tilde{\psi}(s)$. Pour ce s nous avons donc

$$(\tilde{\psi}(s) \circ \psi)[\text{Id}] = \psi[\text{Id}], \quad (5.107)$$

d'où nous déduisons $s[\text{Id}] = [\text{Id}]$. Cela prouve que s stabilise $[\text{Id}]$ dans S_E . Donc $s = \varphi(h)$ pour un certain $h \in H$, et au final $\sigma = \tilde{\psi}(\varphi(h))$.

Conclusion L'application $\tilde{\psi} \circ \varphi: H \rightarrow S_n$ est une application dont l'image est le fixateur d'un point. Plus précisément,

$$\tilde{\psi} \circ \varphi: H \rightarrow \text{Fix}(\psi[\text{Id}]) \quad (5.108)$$

est un isomorphisme de groupe. Mais le stabilisateur d'un point dans S_n est S_{n-1} .

□

5.7 Isométriques du cube

Les isométries du cube proviennent de [79].

Nous considérons le cube centré en l'origine de $\mathbb{R}^3$ et G , le groupe des isométries de $\mathbb{R}^3$ préservant ce cube. Nous notons aussi G^+ le sous-groupe de G constitué des éléments de déterminant positif. Nous notons

$$\mathcal{D} = \{D_1, \dots, D_4\} \quad (5.109)$$

l'ensemble des grandes diagonales, c'est-à-dire les segments $[AG]$, $[EC]$, $[FD]$, et $[BH]$. Nous savons que G préserve les longueurs et que ces segments sont les plus longs possibles à l'intérieur du cube. Donc G agit sur $\mathcal{D}$ parce qu'il ne peut transformer une grande diagonale qu'en une autre grande diagonale. Nous avons donc un morphisme de groupes

$$\rho: G \rightarrow S_4. \quad (5.110)$$

Nous montrons ce que morphisme est surjectif en montrant qu'il contient les transpositions. Le groupe G contient la symétrie axiale passant par le milieu M de $[AE]$ et le milieu N de $[CG]$. Il est facile de voir que cette symétrie permute $[AG]$ avec $[EC]$. De plus elle laisse $[FD]$ inchangée. En effet, aussi incroyable que cela paraisse en regardant le dessin, nous avons $FD \perp MN$, parce qu'en termes de vecteurs directeurs,

$$\overrightarrow{ON} = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} \quad \overrightarrow{OF} = \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}. \quad (5.111)$$

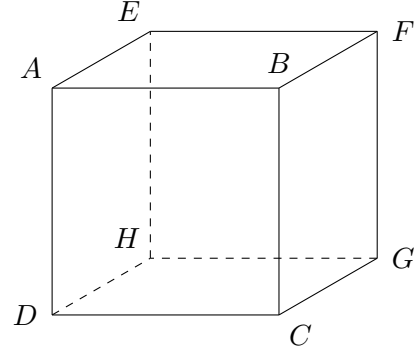
Étudions à présent le noyau $\ker(\rho)$. Si $f \in \ker(\rho)$ n'est pas l'identité, alors $f(D_i) = D_i$ pour tout i , mais au moins pour une des diagonales les sommets sont inversés. Quitte à renommer les sommets du cube nous supposons que la diagonale $[AG]$ est retournée : $f(A) = G$ et $f(G) = A$. Regardons où peut partir B sous l'effet de f . Étant donné que f préserve les diagonales, $f(B) \in \{B, C\}$, mais étant donné que f est une isométrie, $d(f(B), f(G)) = d(B, G)$, et nous concluons que $f(B) = H$. Donc la diagonale $[BH]$ est retournée sous l'effet de f . En raisonnant de même, nous voyons que f retourne toutes les diagonales. Donc les éléments non triviaux de $\ker(\rho)$ retournent toutes les diagonales ; il n'y en a donc qu'un seul et c'est la symétrie centrale :

$$\ker(\rho) = \{\text{Id}, s_0\}. \quad (5.112)$$

Le premier théorème d'isomorphisme 2.29 nous permet d'écrire le quotient de groupes :

$$\frac{G}{\{\text{Id}, s_0\}} \simeq S_4. \quad (5.113)$$

Une classe d'équivalence modulo $\ker(\rho)$ dans G est donc toujours de la forme $\{f, f \circ s_0\}$. Et vu que s_0 est de déterminant -1 , une classe contient toujours exactement un élément de déterminant 1 et un de déterminant -1 .



D'autre part $\ker(\rho)$ est normal dans G parce que en tant que matrice, $s_0 = -\mathbb{1}$, donc les problèmes de commutativité ne se posent pas. L'application

$$\begin{aligned} \varphi: \frac{G}{\{\text{Id}, s_0\}} &\rightarrow G^+ \\ [g] &\mapsto \begin{cases} g & \text{si } \det(g) > 0 \\ g \circ s_0 & \text{sinon} \end{cases} \end{aligned} \quad (5.114)$$

est un isomorphisme de groupes. Et enfin nous pouvons écrire

$$G^+ \simeq S_4. \quad (5.115)$$

Nous allons maintenant utiliser le corolaire 2.66 pour montrer que $G = G^+ \times_{\sigma} \ker(\rho)$. Les conditions sont remplies :

- $\ker(\rho)$ normalise G^+ parce que $\ker(\rho)$ ne contient que $\pm \mathbb{1}$.
- $\ker(\rho) \cap G^+ = \{\text{Id}\}$.
- $\ker(\rho)G^+ = G$ parce que les classes d'équivalence de G modulo $\ker(\rho)$ sont composées de $\{f, f \circ s_0\}$.

Vu que $G^+ \simeq S_4$ et $\ker(\rho) \simeq \mathbb{Z}/2\mathbb{Z}$ nous pouvons écrire de façon plus brillante que

$$G \simeq S_4 \times_{\sigma} \mathbb{Z}/2\mathbb{Z}. \quad (5.116)$$

Mais étant donné que la conjugaison par s_0 est triviale, le produit semi-direct est un produit direct :

$$G \simeq S_4 \times \mathbb{Z}/2\mathbb{Z}. \quad (5.117)$$

Il est maintenant du meilleur gout de pouvoir identifier géométriquement ces éléments. Les éléments de $\mathbb{Z}/2\mathbb{Z} = \{\text{Id}, s_0\}$ ne font pas de mystères. Dans S_4 nous avons les classes de conjugaison des éléments Id , (12) , (123) , (1234) et $(12)(34)$ déterminées durant l'exemple 1.155.

- (1) L'élément (12) consiste à permuter deux diagonales et laisser les autres en place. Nous avons déjà vu que c'était une symétrie axiale passant par les milieux de deux côtés opposés. Cela fait 6 axes d'ordre 2.
- (2) L'élément (123) fixe une des diagonales. C'est donc la symétrie axiale le long de la diagonale fixée. Par exemple la symétrie d'axe (AG) fait bouger le point B de la façon suivante :

$$B \rightarrow D \rightarrow E \rightarrow B. \quad (5.118)$$

C'est une rotation est d'angle $\frac{2\pi}{3}$. Cela sont 8 rotations d'ordre 3.

Notons à ce propos que la différence entre (234) et (243) est que la première fait une rotation d'angle $2\pi/3$ tandis que la seconde fait une rotation d'angle $-2\pi/3$.

- (3) L'élément (1234) ne maintient aucune des diagonales et est d'ordre 4. C'est donc la rotation d'angle $\pi/2$ ou $-\pi/2$ autour de l'axe passant par les milieux de deux faces opposées. Il y en a 6 comme ça (3 paires de faces puis pour chaque il y a $\pi/2$ et $-\pi/2$), et ça tombe bien 6 est justement la taille de la classe de conjugaison de (1234) dans S_4 .
- (4) L'élément $(12)(34)$ est le carré de la précédente¹⁷, c'est-à-dire les rotations d'angle π autour des mêmes axes. Cela fait 3 éléments d'ordre 2.

17. En fait c'est $(13)(24)$, le carré de la précédente, mais c'est la même classe de conjugaison.

Chapitre 6

Corps

6.1 Généralités

6.1.

Nous trouvons parfois le terme **anneau à division**. Cela provient du fait que dans beaucoup de cas on considère uniquement des corps commutatifs ; donc on voudrait une façon de parler d'un anneau dont tous les éléments non nuls sont inversibles. Dans ce cadre on dit :

- Un anneau à division est un anneau dont tous les éléments non nuls sont inversibles,
- Un corps est un anneau à division commutatif.

Pour prendre un exemple de cette différence, le théorème de Wedderburn 19.34 est énoncé ici sous les termes « Tout corps fini est commutatif ». Sous-entendu : la commutativité ne fait pas partie de la définition d'un corps. Par contre dans [79] il est énoncé sous les termes « Tout anneau à division fini est un corps ». Chez lui, un corps est toujours commutatif et un anneau à division est ce que nous appelons ici un corps.

6.1.1 Corps ordonnés

Nous avons vu la définition de corps totalement ordonné en 1.253.

Définition 6.2 ([49]).

Un corps est **formellement réel** si -1 n'est pas une somme de carrés.

Proposition 6.3.

Un corps totalement ordonné est formellement réel.

Démonstration. Soit un corps totalement ordonné $(\mathbb{K}, \leq)$ et $a \in \mathbb{K}$ alors $a^2 \geq 0$. En effet si $a \geq 0$ alors $a^2 = a \times a \geq 0$ directement par la définition 1.253(1b). Si $a \leq 0$ alors $-a \geq 0$ et

$$a^2 = (-a)^2 \geq 0. \quad (6.1)$$

Vu que $-1 < 0$, il ne peut donc pas être écrit comme un carré. A fortiori comme somme de carrés. $\square$

6.1.2 Automorphismes de $\mathbb{R}$ et $\mathbb{C}$

Proposition 6.4 ([121, 1]).

L'identité est l'unique automorphisme du corps $\mathbb{R}$.

Démonstration. Soit un automorphisme $\sigma: \mathbb{R} \rightarrow \mathbb{R}$. Comme pour tout automorphisme,

$$\sigma(a) = \sigma(1a) = \sigma(1)\sigma(a). \quad (6.2)$$

Donc $\sigma(1) = 1$.

Identité sur les rationnels De plus

$$\sigma(n) = \sigma(1 + \dots + 1) = \sigma(1) + \dots + \sigma(1) = n, \quad (6.3)$$

et

$$\sigma\left(\frac{1}{n}\right) + \dots + \sigma\left(\frac{1}{n}\right) = \sigma\left(\frac{1}{n} + \dots + \frac{1}{n}\right) = \sigma(1) = 1. \quad (6.4)$$

Donc $\sigma(1/n) = 1/n$.

Nous en déduisons que pour tout $q \in \mathbb{Q}$, $\sigma(q) = q$. Cela ne suffit pas pour déduire $\sigma(x) = x$ pour tout $x \in \mathbb{R}$ parce que rien n'indique que σ soit continue.

Positive sur les positifs Si $x > 0$ alors $\sigma(x) = \sigma(\sqrt{x})^2 > 0$.

Croissance Si $x > y$ alors $x - y > 0$ et $\sigma(x - y) > 0$. Cela donne $\sigma(x) > \sigma(y)$.

Identité sur les réels Soit un irrationnel $x \in \mathbb{R}$ et une suite (q_i) dans $\mathbb{Q}$ qui converge de façon croissante vers x . Soit $\epsilon > 0$ dans $\mathbb{Q}$. Il existe N tel que si $i > N$ alors $q_i + \epsilon > x$; en appliquant σ à cette inégalité et en se souvenant que σ est l'identité sur $\mathbb{Q}$,

$$q_i + \epsilon > \sigma(x). \quad (6.5)$$

Mais de plus, $q_i < x$ donne $\sigma(q_i) < \sigma(x)$, c'est-à-dire $q_i < \sigma(x)$. En regroupant ces deux inégalités,

$$q_i < \sigma(x) < q_i + \epsilon \quad (6.6)$$

pour tout $\epsilon > 0$ dans $\mathbb{Q}$ et $i > N$. Ce ϵ étant fixé nous pouvons prendre la limite des inégalités (6.6) :

$$x \leq \sigma(x) \leq x + \epsilon. \quad (6.7)$$

Cela étant valable pour tout $\epsilon > 0$ dans $\mathbb{Q}$, nous avons bien $x = \sigma(x)$.

□

Remarque 6.5.

Certains[121] pensent que l'énoncé de cette proposition, ne parlant que de *corps* $\mathbb{R}$ n'autorise pas l'utilisation d'autre structure réelle que celle de corps. Du coup il faut reconstruire la notion d'ordre à partir seulement du langage des corps. Par exemple en disant que $a > b$ si et seulement si il existe k tel que $a = b + k^2$.

On peut s'en sortir en donnant l'énoncé suivant : « Si $\mathbb{K}$ est un corps isomorphe (en tant que corps) à $\mathbb{R}$ alors son unique automorphisme est l'identité ». Cela se démontre immédiatement en disant que si f est un automorphisme de $\mathbb{K}$ et si ϕ est un isomorphisme $\mathbb{K} \rightarrow \mathbb{R}$ alors $\phi \circ f \circ \phi^{-1}$ est un automorphisme de $\mathbb{R}$. Donc il est l'identité et f l'est également.

Attention cependant à prouver que ϕ^{-1} est un morphisme. En effet en posant $\phi^{-1}(x) = a$ et $\phi^{-1}(y) = b$ nous avons

$$\phi(\phi^{-1}(x) + \phi^{-1}(y)) = x + y \quad (6.8)$$

parce que ϕ est un morphisme. D'autre part,

$$\phi(\phi^{-1}(x) + \phi^{-1}(y)) = \phi(a + b). \quad (6.9)$$

Donc

$$\phi^{-1}(x + y) = \phi^{-1}(\phi(a) + \phi(b)) = \phi^{-1}(\phi(a + b)) = a + b = \phi^{-1}(x) + \phi^{-1}(y). \quad (6.10)$$

Proposition 6.6.

Un automorphisme du corps $\mathbb{C}$ qui fixe $\mathbb{R}$ est soit l'identité soit la conjugaison complexe¹.

Démonstration. Soit un automorphisme σ vérifiant la condition de fixer $\mathbb{R}$. Alors la restriction de σ à $\mathbb{R}$ est un automorphisme de $\mathbb{R}$ et y est donc l'identité par la proposition 6.4.

En ce qui concerne les imaginaires purs,

$$-1 = \sigma(-1) = \sigma(ii) = \sigma(i)^2. \quad (6.11)$$

Donc $\sigma(i)$ est un élément de $\mathbb{C}$ vérifiant $\sigma(i)^2 = -1$. C'est-à-dire $\sigma(i) = \pm i$.

Si $\sigma(i) = i$ alors $\sigma = \text{Id}$. Si $\sigma(i) = -i$ alors σ est la conjugaison complexe.

□

1. Par « fixer $\mathbb{R}$ » nous entendons que $\sigma(\mathbb{R}) = \mathbb{R}$, pas spécialement que $\sigma(x) = x$ pour tout $x \in \mathbb{R}$.

6.1.3 Corps premier

Définition 6.7.

Un corps est **premier** s'il est son seul sous corps. Le **sous corps premier** d'un corps est l'intersection de tous ses sous corps.

Lemme 6.8.

Un corps premier est commutatif.

Démonstration. Le centre d'un corps est certainement un sous corps. Par conséquent un corps premier doit être contenu dans son propre centre, c'est-à-dire être commutatif. $\square$

Définition 6.9.

Soit p un nombre premier. Nous notons $\mathbb{F}_p = \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$.

Nous verrons plus loin (section 19.4) comment nous pouvons définir $\mathbb{F}_{p^n}$ lorsque p est premier, ainsi que l'unicité d'un tel corps.

Nous avons par exemple

$$\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\} \quad (6.12)$$

avec la loi $2 = 0$.

Notons que $\mathbb{F}_p$ est un corps² possédant p éléments. L'ensemble $\mathbb{F}_p^*$ est un groupe d'ordre $p - 1$.

Lemme 6.10.

Les corps $\mathbb{Q}$ et $\mathbb{F}_p$ (avec p premier) sont premiers.

Démonstration. Tout sous corps de $\mathbb{Q}$ doit contenir 1, et par conséquent $\mathbb{Z}$. Devant également contenir tous les inverses, il contient $\mathbb{Q}$.

Tout sous corps de $\mathbb{F}_p$ doit contenir 1 et donc $\mathbb{F}_p$ en entier. Par ailleurs nous savons de la proposition 3.63 que $\mathbb{F}_p$ est un corps lorsque p est premier. $\square$

Proposition 6.11.

Soit $\mathbb{K}$ un corps de caractéristique p et $\mathbb{P}$ son sous corps premier. Si $p = 0$ alors $\mathbb{P} = \mathbb{Q}$. Si $p > 0$, alors $\mathbb{P} = \mathbb{F}_p$.

Démonstration. Notons d'abord que la caractéristique d'un corps est toujours soit 0 soit un nombre premier, parce qu'un corps est en particulier un anneau intègre (proposition 1.238).

Étant donné que 1 est dans tout sous corps, nous devons avoir $\mathbb{Z}1 \subseteq \mathbb{P}$. Si $p = 0$, alors $\mathbb{Z}1 \simeq \mathbb{Z}$, et nous avons

$$\mathbb{Z}1_{\mathbb{A}} \subset \mathbb{P} \subset \mathbb{K}. \quad (6.13)$$

Pour chaque $(n, m) \in \mathbb{Z}1_{\mathbb{A}} \times (\mathbb{Z}1_{\mathbb{A}})^*$ l'élément $nm^{-1} \in \mathbb{K}$ est dans $\mathbb{P}$ parce que $\mathbb{P}$ est un corps. Nous en déduisons que le corps des fractions de $\mathbb{Z}$ est contenu dans $\mathbb{P}$ par conséquent $\mathbb{P} = \mathbb{Q}$ (théorème 1.252).

Si par contre la caractéristique de $\mathbb{K}$ est $p \neq 0$, nous avons $\mathbb{Z}1_{\mathbb{A}} \simeq \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ par le lemme 1.233. L'ensemble $\mathbb{F}_p$ étant un corps, c'est le corps premier de $\mathbb{K}$. $\square$

Proposition 6.12.

Soit $\mathbb{K}$ un corps et $\mathbb{P}$ son sous-corps premier. Si $\sigma \in \text{Aut}(\mathbb{K})$ alors $\sigma|_{\mathbb{P}} = \text{Id}$, c'est-à-dire que $\sigma(x) = x$ pour tout $x \in \mathbb{P}$.

6.1.4 Petit théorème de Fermat

Théorème 6.13 (Petit théorème de Fermat).

Soit p un nombre premier.

- (1) Si $x \in \mathbb{Z}/p\mathbb{Z}$ alors $x^p = x$.
- (2) Si $x \in (\mathbb{Z}/p\mathbb{Z})^*$, alors $x^{p-1} = 1$.

2. Quand p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps, proposition 3.63.

(3) Si $x \in (\mathbb{Z}/p\mathbb{Z})^*$ alors $x^{-1} = x^{p-2}$.

(4) Si x est premier avec p , alors $x^{p-1} \in [1]_p$.

Démonstration. Étant donné que $\mathbb{Z}/p\mathbb{Z}$ est un corps commutatif et que p est premier, la proposition 3.41 nous indique que $\sigma(x) = x^p$ est un automorphisme. La proposition 6.12 nous indique alors que

$$a^p = a. \quad (6.14)$$

Si a est inversible alors $a^{p-1} = a^p a^{-1} = 1$.

Pour (4). Le nombre x n'est pas premier avec p uniquement lorsque x est multiple de p . Dans ce cas c'est $[a]_p = 0$ dans $\mathbb{Z}/p\mathbb{Z}$ et donc $a^{p-1} = 0$. $\square$

Exemple 6.14.

Soit $\mathbb{K} = \mathbb{F}_{29}$. Le nombre 29 étant premier, $\mathbb{K}$ est un corps. C'est le corps des entiers modulo 29. Nous avons donc

$$-142 = -113 = -84 = -55 = -26 = 3 = 32 = 61 = 90 = 119. \quad (6.15)$$

Le petit théorème de Fermat nous permet aussi de calculer des exposants et des inverses. En effet, puisque $1 = x^{28}$ pour tout $x \in \mathbb{F}_{29}^*$, nous avons $x^{-1} = x^{27}$, et par suite, pour tout entier a ,

$$x^{-a} = (x^a)^{27} = x^{27a}. \quad (6.16)$$

Le nombre $27a$ peut être grand par rapport à 29. Mais en réutilisant le fait que $1 = x^{28}$, on obtient

$$x^{-a} = x^{[27a]_{28}}. \quad (6.17)$$

Cette expression doit être comprise comme disant que pour tout $k \in [27a]_{28}$ nous avons $x^{-a} = x^k$.

Chose à retenir : dans les exposants nous calculons modulo 28. $\triangle$

6.1.5 Nombres de Sophie Germain

Définition 6.15.

Un nombre premier p est de **Sophie Germain** si $p > 2$ et si le nombre $q = 2p + 1$ est également premier.

Notons qu'il existe des nombres premiers de Sophie Germain. Par exemple $p = 3$ donne $q = 2 \times 3 + 1 = 7$. Vu que 7 est un nombre premier, le nombre 3 est de Sophie Germain. D'après Wikipédia[122], l'existence d'une infinité de nombres premiers de Sophie Germain est encore une question ouverte³.

Lemme 6.16 ([123, 124]).

Soit p , un nombre premier de Sophie Germain. Si $m \in \mathbb{Z}$ n'est pas divisible par q , alors $m^p \in [\pm 1]_q$ où $q = 2p + 1$.

Démonstration. Le petit théorème de Fermat 6.13 nous dit que $m^{q-1} \in [1]_q$. Mais $m^{q-1} = m^{2p} = (m^p)^2$. Donc

$$(m^p)^2 \in [1]_q. \quad (6.18)$$

Vu que q est premier, l'anneau $\mathbb{Z}/q\mathbb{Z}$ est intègre par le corolaire 1.200. Vu que $1 \neq -1$, la proposition 3.146 fonctionne et nous avons $m^p \in [\pm 1]_q$. $\square$

Théorème 6.17 ([123, 124, 125]).

Soit un nombre premier de Sophie Germain (définition 6.15). Il n'existe pas de solutions dans $\mathbb{Z}^3$ au système

$$\begin{cases} x^p + y^p + z^p = 0 \\ [xyz]_p \neq 0. \end{cases} \quad (6.19)$$

3. Si vous lisez ce paragraphe dans un futur où la question est tranchée, n'hésitez pas à m'écrire pour mettre à jour.

Démonstration. Nous supposons que $(x, y, z) \in \mathbb{Z}^3$ est une solution telle que $\text{pgcd}(x, y, z) = 1$.

x, y et z sont premiers deux à deux Supposons que k soit un diviseur commun à x et y . Alors il existe $\alpha, \beta \in \mathbb{Z}$ tels que $x = k\alpha$ et $y = k\beta$. Du coup on aurait $z^p = -k^p(\alpha^p + \beta^p)$. Donc k divise z^p . La proposition 3.18 nous indique qu'alors k divise z . Donc $k = 1$ parce que k diviserait x, y et z .

Ce qui est vrai pour le couple (x, y) est encore vrai pour (x, z) et pour (y, z) .

Le fameux u Nous introduisons à présent une nouvelle variable intermédiaire qui va beaucoup nous aider. En utilisant le lemme 3.40,

$$-x^p = y^p + z^p = (y+z) \sum_{k=0}^{p-1} y^k (-z)^{p-1-k} = (y+z)u \quad (6.20)$$

où nous avons posé $u = \sum_{k=0}^{p-1} y^k (-z)^{p-1-k}$.

$\text{pgcd}(u, y+z) = 1$ Soit α un nombre premier qui divise u et $y+z$.

D'abord α divise x^p et donc x (proposition 3.18). Autrement dit : $[x]_\alpha = 0$.

Ensuite, $0 = [x+z]_\alpha$, de telle sorte que

$$[y]_\alpha = -[z]_\alpha \quad (6.21)$$

Enfin, en prenant la classe de u modulo α , et en substituant (6.21) :

$$0 = [u]_\alpha = \left[\sum_{k=0}^{p-1} y^k (-z)^{p-1-k} \right]_\alpha \quad (6.22a)$$

$$= \sum_{k=0}^{p-1} [y^k]_\alpha [y^{p-1-k}]_\alpha \quad (6.22b)$$

$$= \sum_{k=0}^{p-1} [y]_\alpha^{p-1} \quad (6.22c)$$

$$= p[y]_\alpha^{p-1}. \quad (6.22d)$$

Nous avons donc $p[y]_\alpha^{p-1} = 0$. Mais $\mathbb{Z}/\alpha\mathbb{Z}$ est un anneau intègre⁴. Donc la règle du produit nul s'applique⁵ et nous avons deux possibilités : $[p]_\alpha = 0$ ou $[y]_\alpha^{p-1} = 0$.

D'abord α divise déjà x . Or $\text{pgcd}(x, y) = 1$. Donc α ne peut pas diviser y (à part si $\alpha = 1$ évidemment), et à fortiori pas y^{p-1} non plus. Nous en déduisons que $[p]_\alpha = 0$. Vu que p est premier, nous avons $p = \alpha$.

Mais nous avons déjà vu que α divisait x . Donc $0 = [x]_\alpha = [x]_p$. Mais cela n'est pas possible parce que $[xyz]_p \neq 0$.

Nous avons donc prouvé que $\text{pgcd}(u, y+z) = 1$.

Utilisation d'un lemme Pour rappel, p est impair. Nous avons $(-x)^p = (y+z)u$. Le lemme 3.21 nous dit qu'il existe $a, \alpha \in \mathbb{Z}$ tels que

$$\begin{cases} y+z = a^p \\ u = \alpha^p. \end{cases} \quad (6.23)$$

Ce que nous venons de faire pour $y+x$ peut être fait pour les autres. Donc il existe $a, b, c \in \mathbb{Z}$ tels que

$$y+z = a^p \quad (6.24a)$$

$$x+z = b^p \quad (6.24b)$$

$$x+y = c^p. \quad (6.24c)$$

4. Corollaire 1.200.

5. Proposition 1.174.

q divise un et un seul des x, y ou z Supposons que q ne divise ni x , ni y ni z . Alors le lemme 6.16 dit que $x^p \in [\pm 1]_q$, $y^p \in [\pm 1]_q$ et $z^p \in [\pm 1]_q$. Donc les valeurs possibles pour $[x^p + y^p + z^p]_q$ sont $[\pm 3]_q$ et $[\pm 1]_q$.

Mais nous avons supposé que $x^p + y^p + z^p = 0$ et que $q \geq 5$ de telle sorte que $[\pm 3]_q \neq 0$. Contradiction. Donc q divise au moins un des trois x, y ou z .

Nous avons déjà montré que x, y et z étaient deux à deux premiers entre eux. Donc q ne peut diviser qu'un seul des trois.

q divise x Jusqu'à présent x, y et z avaient des rôles symétriques. Maintenant nous supposons que q divise x .

$[y^p]_q = [\pm 1]_q$ Nous savons que $c^p = x + y$. En passant aux classes modulo q , nous avons

$$[c^p]_q = [x]_q + [y]_q = [y]_q \quad (6.25)$$

parce que nous avons choisis que q divise x . Nous avons maintenant les implications suivantes :
 q ne divise pas y .

$\Rightarrow q$ ne divise pas c^p parce que $[y]_q = [c^p]_q$.

$\Rightarrow q$ ne divise pas c par le lemme 3.19.

$\Rightarrow c^p \in [\pm 1]_q$ par le lemme 6.16.

$\Rightarrow y \in [\pm 1]_q$ toujours parce que $[y]_q = [c^p]_q$.

$[z^p]_q = [\pm 1]_q$ Parce que les rôles de y et z sont symétriques. Donc ce que nous avons fait pour obtenir $[y^p]_q = [\pm 1]_q$ tient pour avoir $[z^p]_q = [\pm 1]_q$.

q divise $y + z$ Nous avons dit que q divisait x . Il divise donc aussi $2x$. Nous avons :

$$2x = (x + y) + (x + z) - (y + z) = c^p + b^p - a^p. \quad (6.26)$$

En passant au modulo q , à gauche nous avons $[2x]_q = 0$. Donc

$$[a^p]_q = [c^p]_q + [b^p]_q \quad (6.27a)$$

$$= [y]_q + [z]_q \quad (6.27b)$$

$$= [\pm 1]_q + [\pm 1]_q \quad (6.27c)$$

$$\in \{[2]_q, [-2]_q, [0]_q\}. \quad (6.27d)$$

En tout état de cause, $[a^p]_q$ n'est pas $[\pm 1]_q$. La contraposée du lemme 6.16 nous dit alors que q divise $a^p = y + z$.

$[y]_q = [-z]_q$ Il s'agit seulement du fait que q divise $y + z$.

$[u]_q = [p]_q$ Par définition, $u = \sum_{k=0}^{p-1} y^k (-z)^{p-1-k}$. On passe au modulo q , en substituant $[-z]_q$ par $[y]_q$:

$$[u]_q = \sum_{k=0}^{p-1} [y]_q^k [y]_q^{p-1-k} = \sum_{k=0}^{p-1} [y]_q^{p-1} = p[y]_q^{p-1} = [p]_q \quad (6.28)$$

La dernière égalité est le fait que $[y]_q = [\pm 1]_q$ et que $p - 1$ est pair.

La contradiction Vous vous souvenez de (6.23) qui disait que $u = \alpha^p$ pour un certain p ? Nous avons les implications suivantes :

$[\alpha^p]_q = [p]_q \neq 0 \Rightarrow q$ ne divise pas α^p .

$\Rightarrow q$ ne divise pas α .

$\Rightarrow \alpha^p \in [\pm 1]_q$.

$\Rightarrow [p]_q \in [\pm 1]_q$.

La dernière ligne est clairement fausse parce que $q > p$ et p n'est certainement pas égal à 1 ou -1 .

Nous avons prouvé le théorème pour les triples (x, y, z) qui n'ont pas de facteurs communs. Si k est un diviseur commun de x, y et z , alors $(x/k, y/k, z/k)$ est encore une solution, et donc n'existe pas. $\square$

6.2 Théorème des deux carrés

Proposition 6.18.

Soit p un nombre premier et P un élément de $\mathbb{F}_p[X]$. L'anneau $\mathbb{F}_p[X]/(P)$ est intègre si et seulement si P est irréductible dans $\mathbb{F}_p[X]$.

Démonstration. Supposons que P soit réductible dans $\mathbb{F}_p[X]$, c'est-à-dire qu'il existe $Q, R \in \mathbb{F}_p[X]$ tels que $P = QR$. Dans ce cas, $\bar{Q}$ est diviseur de zéro dans $\mathbb{F}_p[X]/(P)$ parce que $\bar{Q}\bar{R} = 0$.

Nous supposons maintenant que $\mathbb{F}_p[X]/(P)$ ne soit pas intègre : il existe des polynômes $R, Q \in \mathbb{F}_p[X]$ tels que $\bar{Q}\bar{R} = 0$. Dans ce cas le polynôme QR est le produit de P par un polynôme : $QR = PA$. Tous les facteurs irréductibles de A étant soit dans Q soit dans R , il est possible de modifier un peu Q et R pour obtenir $QR = P$, ce qui signifie que P n'est pas irréductible. $\square$

6.2.1 Un peu de structure dans $\mathbb{Z}[i]$

Lemme 6.19.

L'application

$$\begin{aligned} N: \mathbb{Z}[i] &\rightarrow \mathbb{N} \\ a + bi &\mapsto a^2 + b^2 \end{aligned} \quad (6.29)$$

est un stathme euclidien pour $\mathbb{Z}[i]$.

Démonstration. Soient $t, z \in \mathbb{Z}[i] \setminus \{0\}$ dont le quotient s'écrit

$$\frac{z}{t} = x + iy \quad (6.30)$$

dans $\mathbb{C}$. Nous considérons $q = a + bi$ où a et b sont les entiers les plus proches de x et y . S'il y a *ex aequo*, on prend au hasard⁶. Alors nous avons

$$\left| \frac{z}{t} - q \right| \leq \frac{|1 + i|}{2} = \frac{\sqrt{2}}{2} < 1. \quad (6.31)$$

On pose $r = z - qt$ qui est bien un élément de $\mathbb{Z}[i]$. De plus

$$|r| = |z - qt| = |t| \left| \frac{z}{t} - q \right| < |t|, \quad (6.32)$$

c'est-à-dire que $|r|^2 < |t|^2$ et donc $N(r) < N(t)$. $\square$

Étant donné que $\mathbb{Z}[i]$ est euclidien, il est principal (proposition 3.102).

Lemme 6.20.

Les éléments inversibles de $\mathbb{Z}[i]$ sont $\{\pm 1, \pm i\}$.

Démonstration. Déterminons les éléments inversibles de $\mathbb{Z}[i]$. Si $z \in \mathbb{Z}[i]^*$, alors il existe $z' \in \mathbb{Z}[i]^*$ tel que $zz' = 1$. Dans ce cas nous aurions

$$1 = N(zz') = N(z)N(z'), \quad (6.33)$$

ce qui est uniquement possible avec $N(z) = N(z') = 1$, c'est-à-dire $z = \pm 1$ ou $z = \pm i$. Nous avons donc

$$\mathbb{Z}[i]^* = \{\pm 1, \pm i\}. \quad (6.34)$$

$\square$

Définition 6.21 ([126]).

Un **monoïde** est un triple $(E, *, e)$ où E est un ensemble, e est un élément de E et $*$: $E \times E \rightarrow E$ est une loi de composition telle que pour tout $x, y \in E$,

6. Dans l'exemple 3.101, nous prenions toujours l'inférieur parce que le stathme tenait compte de la positivité.

- (1) $x * (y * z) = (x * y) * z$ (associativité)
 (2) $e * x = x * e = x$ (e est un neutre).

Nous notons $\Sigma = \{a^2 + b^2 \text{ tel que } a, b \in \mathbb{N}\}$.

Lemme 6.22.

L'ensemble $\Sigma = \{a^2 + b^2 \text{ tel que } a, b \in \mathbb{N}\}$ est un sous-monoïde⁷ de $\mathbb{N}$.

Démonstration. Il suffit de prouver que si $m, n \in \Sigma$, alors le produit mn est également dans Σ . Si N est le stathme euclidien sur $\mathbb{Z}[i]$, alors $n \in \Sigma$ si et seulement s'il existe $z \in \mathbb{Z}[i]$ tel que $N(z) = n$. Si $z, z' \in \mathbb{Z}[i]$, alors $zz' \in \mathbb{Z}[i]$ et de plus

$$N(zz') = N(z)N(z') = nm. \quad (6.35)$$

Donc nm est l'image de zz' par N , ce qui prouve que $nm \in \Sigma$. □

Théorème 6.23 (Théorème des deux carrés, version faible).

Un nombre premier est somme de deux carrés si et seulement si $p = 2$ ou $p \equiv 1 \pmod{4}$.

Remarque 6.24.

Il n'est pas dit que les nombres dans $[1]_4$ sont premiers ($9 = 8 + 1$ ne l'est pas par exemple). Le théorème signifie que (à part 2), si un nombre premier est dans $[1]_4$ alors il est somme de deux carrés, et inversement, si un nombre premier est somme de deux carrés, il est dans $[1]_4$.

Démonstration. Soit p un nombre premier dans Σ . Si $a = 2k$, alors $a^2 = 4k^2$ et $a^2 \equiv 0 \pmod{4}$. Si au contraire a est impair, $a = 2k + 1$ et $a^2 = 4k^2 + 1 + 4k \equiv 1 \pmod{4}$. La même chose est valable pour b . Par conséquent, $a^2 + b^2$ est automatiquement $[0]_4$, $[1]_4$ ou $[2]_4$. Évidemment les nombres de la forme $0 \pmod{4}$ ne sont pas premiers ; parmi les $2 \pmod{4}$, seul $p = 2$ est premier (et vaut $1^2 + 1^2$).

Nous avons démontré que les seuls premiers de la forme $a^2 + b^2$ sont $p = 2$ et les $p \equiv 1 \pmod{4}$. Il reste à faire le contraire : démontrer que si un nombre premier p vaut $1 \pmod{4}$, alors il est premier. Nous considérons l'anneau

$$\mathbb{Z}[i] = \{a + bi \text{ tel que } a, b \in \mathbb{Z}\}. \quad (6.36)$$

puis l'application

$$\begin{aligned} N: \mathbb{Z}[i] &\rightarrow \mathbb{N} \\ a + bi &\mapsto a^2 + b^2. \end{aligned} \quad (6.37)$$

Un peu de calcul dans $\mathbb{C}$ montre que pour tout $z, z' \in \mathbb{Z}[i]$, $N(zz') = N(z)N(z')$.

Nous savons que les éléments inversibles de $\mathbb{Z}[i]$ sont ± 1 et $\pm i$ (lemme 6.20).

Le lemme 6.19 montre que $\mathbb{Z}[i]$ est un anneau euclidien parce que N est un stathme. L'anneau $\mathbb{Z}[i]$ étant euclidien, il est principal (proposition 3.102).

Pour la suite, nous allons d'abord montrer que $p \in \Sigma$ si et seulement si p n'est pas irréductible dans $\mathbb{Z}[i]$, puis nous allons voir quels sont les irréductibles de $\mathbb{Z}[i]$.

Soit p , un nombre premier dans Σ . Si $p = a^2 + b^2$, alors nous avons $p = (a + ib)(a - bi)$, mais étant donné que p est premier, nous avons $a \neq 0$ et $b \neq 0$. Du coup p n'est pas inversible dans $\mathbb{Z}[i]$, mais il peut être écrit comme le produit de deux non inversibles. Le nombre p est donc non irréductible dans $\mathbb{Z}[i]$.

Dans l'autre sens, nous supposons que p est un nombre premier non irréductible dans $\mathbb{Z}[i]$. Nous avons alors $p = zz'$ avec ni z ni z' dans $\{\pm 1, \pm i\}$. En appliquant N nous avons

$$p^2 = N(p) = N(z)N(z'). \quad (6.38)$$

7. Définition 6.21.

Vu que p est premier, cela est uniquement possible avec $N(z) = N(z') = p$ (avoir $N(z) = 1$ est impossible parce que cela dirait que z est inversible). Si $z = a + ib$, alors $p = N(z) = a^2 + b^2$, et donc $p \in \Sigma$.

Nous savons déjà que $\mathbb{Z}[i]$ est un anneau principal et n'est pas un corps ; la proposition 3.78 s'applique donc et p sera non irréductible si et seulement si l'idéal (p) sera non premier. Le fait que (p) soit un idéal non premier implique que le quotient $\mathbb{Z}[i]/(p)$ est non intègre (c'est la définition d'un idéal premier). Nous cherchons donc les nombres premiers pour lesquels le quotient $\mathbb{Z}[i]/(p)$ n'est pas intègre.

Nous commençons par écrire le quotient $\mathbb{Z}[i]/(p)$ sous d'autres formes. D'abord en remarquant que si I et J sont deux idéaux, on a $(\mathbb{A}/I)/J \simeq (\mathbb{A}/J)/I$, du coup, en tenant compte du fait que $\mathbb{Z}[i] = \mathbb{Z}[X]/(X^2 + 1)$, nous avons

$$\mathbb{Z}[i]/(p) = (\mathbb{Z}[X]/(p))/(X^2 + 1) = \mathbb{F}_p[X]/(X^2 + 1). \quad (6.39)$$

Nous avons donc équivalence des propositions suivantes :

$$p \in \Sigma \quad (6.40a)$$

$$\mathbb{F}_p[X]/(X^2 + 1) \text{ n'est pas intègre} \quad (6.40b)$$

$$X^2 + 1 \text{ n'est pas irréductible dans } \mathbb{F}_p \quad (6.40c)$$

$$X^2 + 1 \text{ admet une racine dans } \mathbb{F}_p \quad (6.40d)$$

$$-1 \in (\mathbb{F}_p^*)^2 \quad (6.40e)$$

$$\exists y \in \mathbb{F}_p^* \text{ tel que } y^2 = -1. \quad (6.40f)$$

Le point (6.40c) vient de la proposition 6.18. Maintenant nous utilisons le fait que p soit un premier impair (parce que le cas de $p = 2$ est déjà complètement traité), donc $(p-1)/2 \in \mathbb{N}$ et nous avons, pour le y de la dernière ligne,

$$(-1)^{(p-1)/2} = (y^2)^{(p-1)/2} = y^{p-1} = 1 \quad (6.41)$$

parce que dans $\mathbb{F}_p$ nous avons $y^{(p-1)} = 1$ par le petit théorème de Fermat (théorème 6.13). Du coup p doit vérifier

$$1 = (-1)^{(p-1)/2}, \quad (6.42)$$

c'est-à-dire $\frac{p-1}{2} \equiv 0 \pmod{2}$ ou encore $p \equiv 1 \pmod{4}$. $\square$

Théorème 6.25 (Théorème des deux carrés[79]).

Soit $n \geq 2$ un nombre dont nous notons

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)} \quad (6.43)$$

où $\mathcal{P}$ est l'ensemble des nombres premiers. Alors $n \in \Sigma$ si et seulement si pour tout $p \in \mathcal{P} \cap [3]_4$, nous avons $v_p(n) \in [0]_2$ (c'est-à-dire $v_p(n)$ est pair).

Démonstration. **Condition suffisante.** Le produit (6.43) est évidemment un produit fini que nous pouvons alors regrouper en quatre parties : $\mathcal{P} \cap [0]_4$, $\mathcal{P} \cap [1]_4$, $\mathcal{P} \cap [2]_4$ et $\mathcal{P} \cap [3]_4$.

- Il n'y a pas de nombres premiers dans $[0]_4$.
- Les nombres premiers de $[1]_4$ sont dans Σ . Le produit d'éléments de Σ étant dans Σ , nous avons

$$\prod_{p \in \mathcal{P} \cap [1]_4} p^{v_p(n)} \in \Sigma. \quad (6.44)$$

- Le seul nombre premier dans $[2]_4$ est 2. C'est un élément de Σ .

— Le produit

$$\prod_{p \in \mathcal{P} \cap [3]_4} p^{v_p(n)} \quad (6.45)$$

est par hypothèse un produit de carrés ($v_p(n)$ est pair), et est donc un carré.

Au final le produit $\prod_{p \in \mathcal{P}} p^{v_p(n)}$ est un produit d'un carré par un élément de Σ , ce qui est encore un élément de Σ .

Pour cette partie, nous avons utilisé et réutilisé le lemme 6.22.

Condition nécessaire. Soit p , un nombre premier. Nous voulons montrer que

$$\{v_p(n) \text{ tel que } n \in \Sigma\} \subset [2]_2. \quad (6.46)$$

Pour montrer cela nous allons procéder par récurrence sur les ensembles

$$E_k = \{v_p(n) \text{ tel que } n \in \Sigma\} \cap \{0, \dots, k\}. \quad (6.47)$$

Il est évident que les éléments de E_0 sont pairs, vu qu'il n'y a que zéro, qui est pair.

Supposons que $E_k \subset [0]_2$, et montrons que $E_{k+1} \subset [0]_2$. Soit un élément de E_{k+1} , c'est-à-dire $v_p(n) \leq k+1$ avec $n = a^2 + b^2$. Si $v_p(n) = 0$ alors l'affaire est réglée ; sinon c'est que p divise n . Mais dans $\mathbb{Z}[i]$ nous avons

$$n = a^2 + b^2 = (a + bi)(a - bi) \quad (6.48)$$

Vu que $\mathbb{Z}[i]$ est principal, le lemme de Gauss 3.88 nous dit que si p divise n , alors il doit diviser soit $a + bi$, soit $a - bi$ (et du coup en fait les deux). Nous avons alors $p \mid a$ et $p \mid b$ en même temps. Du coup

$$p^2 \mid a^2 + b^2 = n. \quad (6.49)$$

Posons $a = pa'$ et $b = pb'$ avec $a', b' \in \mathbb{N}$. Nous avons

$$\frac{n}{p^2} = \frac{p^2 a'^2 + p^2 b'^2}{p^2} = a'^2 + b'^2 \in \Sigma. \quad (6.50)$$

Mais par construction,

$$v_p\left(\frac{n}{p^2}\right) = v_p(n) - 2 < k. \quad (6.51)$$

Donc $v_p(\frac{n}{p^2})$ est pair et du coup $v_p(n)$ doit également être pair.

□

6.2.2 Résultats chinois

Nous allons maintenant parler du système d'équations

$$\begin{cases} x = a_1 \pmod{p} \end{cases} \quad (6.52a)$$

$$\begin{cases} x = a_2 \pmod{q} \end{cases} \quad (6.52b)$$

avec a_1, a_2 donnés dans $\mathbb{Z}$ et p, q des entiers premiers entre eux. Le lemme chinois nous donne la liste des solutions ainsi qu'une manière de les construire. Le théorème chinois en sera une espèce de corolaire qui établira l'isomorphisme d'anneaux $\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$. Voir [127].

Lemme 6.26 (Lemme chinois [128]).

Soient n_1, n_2 deux entiers premiers entre eux. Soient $a_1, a_2 \in \mathbb{Z}$. Les solutions du système

$$\begin{cases} x = a_1 \pmod{n_1} \end{cases} \quad (6.53a)$$

$$\begin{cases} x = a_2 \pmod{n_2} \end{cases} \quad (6.53b)$$

pour $x \in \mathbb{Z}/n_1n_2\mathbb{Z}$ sont données de la façon suivante. Soient u_1, u_2 deux entiers qui satisfont la relation de Bézout⁸

$$u_1n_1 + u_2n_2 = 1, \quad (6.54)$$

et

$$a = (a_1u_2n_2 + a_2u_1n_1) \pmod{n_1}. \quad (6.55)$$

Alors $x = a \pmod{n_1n_2}$.

Démonstration. Vérifions que le x donné par $x = a \pmod{n_1n_2}$ est bien une solution. D'abord

$$a \pmod{n_2} = a_1u_2n_2 \pmod{n_1} \quad (6.56a)$$

$$= a_1(1 - u_1n_1) \pmod{n_1} \quad (6.56b)$$

$$= a_1 \pmod{n_1} \quad (6.56c)$$

où nous avons utilisé l'identité de Bézout (6.54). La vérification de $a \pmod{n_2} = a_2 \pmod{n_2}$ est la même.

Soit maintenant $x \in \mathbb{Z}/n_1n_2\mathbb{Z}$ une solution du système (6.53) et a donné par la formule (6.55). Alors

$$(x - a) \pmod{n_1} = \left(a_1 - (a_1n_2u_2 + a_2u_1n_1) \right) \pmod{n_1} \quad (6.57a)$$

$$= a_1 - a_1u_2n_2 \pmod{n_1} \quad (6.57b)$$

$$= 0, \quad (6.57c)$$

donc $(x - a) \pmod{n_1} = 0$, ce qui signifie que $x - a$ est divisible par n_1 . De la même façon, $(x - a) \pmod{n_2} = 0$ et $x - a$ est divisible par n_2 . Nous savons maintenant que $x - a$ est divisible par n_1 et n_2 . Étant donné que n_1 et n_2 sont premiers entre eux, nous en déduisons que $x - a$ est divisible par n_1n_2 , ou encore que $x = a \pmod{n_1n_2}$. $\square$

Théorème 6.27 (Théorème chinois).

Soient p, q deux naturels premiers entre eux. Si $p, q \geq 2$ alors l'application

$$\begin{aligned} \phi: \mathbb{Z}/pq\mathbb{Z} &\rightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ [x]_{pq} &\mapsto ([x]_p, [x]_q) \end{aligned} \quad (6.58)$$

est un isomorphisme d'anneaux.

Démonstration. Nous devons prouver que l'application ϕ respecte la somme, le produit et qu'elle est bijective. En ce qui concerne la somme,

$$\phi([x]_{pq} + [y]_{pq}) = \phi((x + y) \pmod{pq}) \quad (6.59a)$$

$$= ([x + y]_p, [x + y]_q) \quad (6.59b)$$

$$= ([x]_p + [y]_p, [x]_q + [y]_q) \quad (6.59c)$$

$$= ([x]_p, [x]_q) + ([y]_p, [y]_q) \quad (6.59d)$$

$$= \phi(x) + \phi(y). \quad (6.59e)$$

En ce qui concerne le produit, c'est le même jeu : nous obtenons

$$\phi([xy]_{pq}) = \phi([x]_{pq})\phi([y]_{pq}) \quad (6.60)$$

en utilisant le fait que $[xy]_p = [x]_p[y]_p$.

Montrons maintenant que ϕ est surjective. Soient $y_1, y_2 \in \mathbb{Z}$ et $x \in \mathbb{Z}$. Demander

$$\phi([x]_{pq}) = ([y_1]_p, [y_2]_q) \quad (6.61)$$

8. voir le théorème 1.181

revient à demander que $[x]_p = [y_1]_p$ et $[x]_q = [y_2]_q$, c'est-à-dire que x résolve le système

$$\begin{cases} x = y_1 \pmod{p} \\ x = y_2 \pmod{q} \end{cases} \quad (6.62a)$$

$$(6.62b)$$

Le lemme chinois 6.26 nous assure qu'une solution existe.

En ce qui concerne l'injectivité, nous supposons que x et y soient deux entiers tels que

$$\phi([x]_{pq}) = \phi([y]_{pq}). \quad (6.63)$$

Nous en déduisons le système

$$\begin{cases} x \pmod{p} = y \pmod{p} \\ x \pmod{q} = y \pmod{q} \end{cases} \quad (6.64a)$$

$$(6.64b)$$

c'est-à-dire qu'il existe des entiers k et l tels que $x = y + kp$ et $x = y + lq$ ou encore tels que

$$kp + lq = 0. \quad (6.65)$$

Étant donné que p et q sont premiers entre eux, la seule possibilité est $k = l = 0$, c'est-à-dire $x = y$. $\square$

Théorème 6.28 (Théorème chinois[1]).

Soit A un anneau commutatif. Soient $n \geq 2$, des éléments $x_1, \dots, x_n$ dans A et des idéaux $I_1, \dots, I_n$ tels que $I_i + I_j = A$ pour tout $i \neq j$.

Alors il existe un $x \in A$ tel que $x - x_i \in I_i$ pour tout $1 \leq i \leq n$.

Démonstration. En plusieurs points.

Définition de J_k Pour $k \in \{1, \dots, n\}$ nous notons J_k le produit $J_k = \prod_{l \neq k} I_l$. Étant donné que chaque I_k est un idéal, nous avons

$$I_k \subset J_l \quad (6.66)$$

dès que $k \neq l$.

$I_i + J_i = A$ En effet, soit $k \neq i$. Nous avons $J_i \subset I_k$ et donc

$$I_i + J_i \subset I_i + I_k = A. \quad (6.67)$$

Des α et des β Soit $i \in \{1, \dots, n\}$. Vu que $I_i + J_i = A$, nous donc prendre $\alpha_i \in I_i$ et $\beta_i \in J_i$ tels que

$$\alpha_i + \beta_i = 1. \quad (6.68)$$

Et enfin Nous posons $x = \sum_{i=1}^n \beta_i x_i$. Pour chaque k nous avons

$$x - x_k = \sum_{i=1}^n \beta_i x_i - x_k \quad (6.69a)$$

$$= \sum_{i \neq k} \beta_i x_i + (\beta_k - 1)x_k \quad (6.69b)$$

$$= \sum_{i \neq k} \beta_i x_i - \alpha_k x_k. \quad (6.69c)$$

Les deux termes sont dans I_k . En effet, d'une part $\beta_i \in J_i \subset I_k$ et I_k est un idéal, donc $\beta_i x_i \in I_k$, et d'autre part $\alpha_k \in I_k$, donc $\alpha_k x_k \in I_k$.

Un idéal étant stable par somme, la somme du tout est dans I_k . $\square$

Remarque 6.29.

Ce théorème chinois est bien une généralisation du lemme chinois 6.26. En effet, l'élément x dont il est question est solution du problème $x = x_i \pmod{I_i}$. L'hypothèse $I_i + I_j = A$ n'est pas nouvelle non plus étant donné que si p et q sont des entiers premiers entre eux nous avons $p\mathbb{Z} + q\mathbb{Z} = \mathbb{Z}$ par le corolaire 1.183.

6.3 Polynômes à coefficients dans un corps

Nous supposons que $\mathbb{K}$ est un corps commutatif, et nous étudions l'anneau $\mathbb{K}[X]$, défini en 1.240.

Proposition 6.30.

L'anneau $\mathbb{K}[X]$ des polynômes sur un corps commutatif $\mathbb{K}$ est factoriel.

Le théorème suivant est un cas particulier pour $\mathbb{K}[X]$ du théorème chinois 3.85.

Théorème 6.31 (Théorème chinois).

Si P et Q sont deux polynômes premiers entre eux, alors nous avons l'isomorphisme

$$\mathbb{K}[X]/(P, Q) \simeq \mathbb{K}[X]/(P) \times \mathbb{K}[X]/(Q). \quad (6.70)$$

6.3.1 Irréductibilité

Définition 6.32 ([129]).

Un polynôme à coefficients dans un anneau commutatif est irréductible si il

- (1) n'est pas inversible,
- (2) n'est pas le produit de deux non inversibles.

Un polynôme est irréductible dans $\mathbb{K}[X]$ au sens de la définition 3.64 si et seulement s'il est irréductible au sens de la définition 6.32 parce que seules les constantes (non nulles) sont inversibles dans $\mathbb{K}[X]$.

Exemple 6.33.

Si un polynôme $P \in \mathbb{Z}[X]$ n'a que des racines complexes, ça ne l'empêche pas d'être réductible sur $\mathbb{Z}$. La réductibilité ne signifie pas qu'on peut mettre des racines en évidence. Par exemple le polynôme $P = X^4 + 3X^2 + 2$ est réductible sur $\mathbb{Z}$ en

$$P = (X^2 + 1)(X^2 + 2), \quad (6.71)$$

mais n'a pas de racines dans $\mathbb{Z}$. Par contre, il est vrai que si on veut réduire plus, il faut sortir de $\mathbb{Z}$.

△

Définition 6.34.

Nous disons que $P \in \mathbb{K}[X]$ est **scindé** sur $\mathbb{K}$ s'il est produit dans $\mathbb{K}[X]$ de polynômes de degré 1.

Définition 6.35 (Polynôme scindé).

Soit $P \in \mathbb{K}[X]$ un polynôme irréductible, et $\mathbb{L}$ un corps, extension du corps $\mathbb{K}$. On dit que P est **scindé** dans $\mathbb{L}$ si P se décompose en un produit de polynômes de degré 1 dans $\mathbb{L}[X]$.

Note : les constantes ne sont donc pas des polynômes scindés.

Proposition 6.36 (Critère d'Eisenstein).

Soit le polynôme $P = \sum_{k=0}^n a_k X^k$ dans $\mathbb{Z}[X]$. Nous supposons avoir un nombre premier p tel que

- (1) p divise tous les $a_0, \dots, a_{n-1}$,
- (2) p ne divise pas a_n ,
- (3) p^2 ne divise pas a_0 .

Alors P est irréductible dans $\mathbb{Q}[X]$.

Si de plus P est primitif au sens du pgcd (définition 3.133) alors P est irréductible dans $\mathbb{Z}[X]$.

Démonstration. Nous considérons $\bar{P}$ le polynôme réduit modulo p , c'est-à-dire $\bar{P} \in \mathbb{F}_p[X]$. Étant donné que par hypothèse tous les coefficients sont multiples de p sauf a_n , nous avons $\bar{P} = cX^n$.

Supposons par l'absurde que $P = QR$ avec $Q, R \in \mathbb{Q}[X]$. Alors le lemme de Gauss (3.88) impose $P, Q \in \mathbb{Z}[X]$.

Nous avons aussi, au niveau des réductions modulo p que $\bar{Q}\bar{R} = \bar{P}$. Or $\bar{P}$ est un monôme, donc $\bar{Q}$ et $\bar{R}$ doivent également l'être. Donc $\bar{Q} = dX^k$ et $\bar{R} = eX^{n-k}$ et en particulier $\bar{Q}(0) = \bar{R}(0) = 0$, c'est-à-dire que $Q(0)$ et $R(0)$ sont divisibles par p . Cela impliquerait que $a_0 = Q(0)R(0)$ soit divisible par p^2 , ce qui est exclu par les hypothèses. Donc P est irréductible.

Supposons de surcroît que P est primitif au sens du pgcd. Il est donc irréductible et primitif sur $\mathbb{Q}[X]$ et le corolaire 3.147 nous dit alors que P est irréductible sur $\mathbb{Z}[X]$. $\square$

Exemple 6.37.

Soit le polynôme $P = 3X^4 + 15X^2 + 10$. Pour faire fonctionner le critère d'Eisenstein il nous faut un nombre premier p divisant 15 et 10, mais pas 3 et dont le carré ne divise pas 10. C'est vite vu que $p = 5$ fait l'affaire. Le polynôme P est donc irréductible sur $\mathbb{Q}[X]$. $\triangle$

6.3.2 Idéaux

Soit $P \in \mathbb{K}[X]$ un polynôme. Nous notons (P) l'idéal engendré par P :

$$(P) = \{PR \text{ tel que } R \in \mathbb{K}[X]\}. \quad (6.72)$$

Lemme 6.38.

Nous avons

- (1) $(P) \subset (Q)$ si et seulement si Q divise P ,
- (2) $(P) = (Q)$ si et seulement si P et Q sont multiples (non nuls) l'un de l'autre.

Démonstration. Si $(P) \subset (Q)$, en particulier $P \in (Q)$ et il existe $R \in \mathbb{K}[X]$ tel que $P = QR$, ce qui signifie que Q divise P .

Si les idéaux de P et de Q sont identiques, l'un divise l'autre et l'autre divise l'un. Ils sont donc multiples l'un de l'autre. $\square$

Théorème 6.39.

Soit $\mathbb{K}$ un corps commutatif.

- (1) L'anneau $\mathbb{K}[X]$ est euclidien et principal.
- (2) Si I est un idéal dans $\mathbb{K}[X]$ et si $P \in I$ est de degré minimal, alors $(P) = I$.
- (3) De plus si $I \neq \{0\}$, il existe un unique polynôme unitaire μ tel que $I = (\mu)$.

Démonstration. Le point (1) a déjà été démontré dans le lemme 3.127 via le fait que $\mathbb{K}[X]$ est euclidien. Nous allons cependant donner ici une preuve directe que tous les idéaux de $\mathbb{K}[X]$ sont principaux. Si $I = \{0\}$, le résultat est évident. Nous supposons donc I non nul. Soit P de degré minimum parmi les éléments de I . Évidemment $(P) \subset I$. Nous allons démontrer qu'en réalité $(P) = I$.

Soit $P' \in I$. Par le théorème 3.124 de la division euclidienne⁹, il existe Q et R dans $\mathbb{K}[X]$ tels que $P' = PQ + R$ avec $\deg(R) < \deg(P)$. Étant donné que $R = P' - PQ$ nous avons $R \in I$ et par conséquent $R = 0$ parce que P a été choisi de degré minimum dans I . Nous avons donc $P' = PQ$ et $I \subset (P)$.

L'existence d'un polynôme unitaire qui génère I est obtenu en choisissant $\mu = P/a_n$ où a_n est le coefficient du terme de plus haut degré. L'unicité d'un tel polynôme est obtenu par le fait que si μ et μ' génèrent le même idéal, alors ils sont multiples l'un de l'autre, or puisqu'ils sont unitaires, ils sont égaux. $\square$

Nous voyons que n'importe quel polynôme de degré minimum dans un idéal génère l'idéal. Une importante conséquence du théorème 6.39 que nous verrons plus bas est que tout polynôme annulateur d'un endomorphisme est divisé par le polynôme minimal (proposition 9.97).

9. Ici $\mathbb{K}$ est un corps et donc l'hypothèse d'inversibilité est automatiquement vérifiée.

Corolaire 6.40.

Si $\mathbb{K}$ est un corps et si P est un polynôme irréductible, alors l'ensemble $\mathbb{L} = \mathbb{K}[X]/(P)$ est un corps. De plus $\mathbb{L}$ est un espace vectoriel de dimension $\deg(P)$.

Démonstration. En effet $\mathbb{K}[X]$ est un anneau principal par le théorème 6.39, par conséquent la proposition 3.80(2) déduit que $\mathbb{K}[X]/(P)$ est un corps.

Une base de $\mathbb{L}$ est donnée par les projections de $1, X, X^2, \dots, X^{n-1}$. En effet ces éléments forment une famille libre parce que si $\sum_{k=0}^{n-1} a_k \bar{X}^k = 0$ alors un représentant de cette classe doit être de la forme SP dans $\mathbb{K}[X]$, c'est-à-dire

$$\sum_{k=0}^{n-1} a_k X^k = SP, \quad (6.73)$$

ce qui n'est possible que si $S = 0$ et $a_k = 0$. D'autre part c'est un système générateur. En effet si $P = X^n + Q$ avec $\deg(Q) = n - 1$ alors

$$\bar{X}^{n+l} = \bar{X}^n \bar{X}^l = (\bar{P} - \bar{Q}) \bar{X}^l = \bar{Q} \bar{X}^l. \quad (6.74)$$

Nous avons donc exprimé $\bar{X}^{n+l}$ comme une somme de termes de degré $n + l - 1$. Par récurrence nous pouvons exprimer tout $\bar{X}^{n+l}$ comme combinaison d'éléments de degré plus petit que n . $\square$

6.41.

Ce corolaire prendra une nouvelle jeunesse lorsque nous parlerons de polynômes d'endomorphismes, en particulier la proposition 9.107 va donner des précisions.

Lemme 6.42 ([130]).

Soit un isomorphisme de corps $\tau: \mathbb{K} \rightarrow \mathbb{K}'$. Alors

(1) L 'application étendue

$$\begin{aligned} \tau: \mathbb{K}[X] &\rightarrow \mathbb{K}'[X] \\ \sum_i a_i X^i &\mapsto \sum_i \tau(a_i) X^i \end{aligned} \quad (6.75)$$

est un isomorphisme d'anneaux ;

(2) pour tout $P \in \mathbb{K}[X]$, le passage au quotient

$$\begin{aligned} \phi_\tau: \mathbb{K}[X]/(P) &\rightarrow \mathbb{K}'[X]/(\tau(P)) \\ \bar{Q} &\mapsto \overline{\tau(Q)} \end{aligned} \quad (6.76)$$

est un isomorphisme d'anneaux (et d'abord est bien définie).

Démonstration. Nous n'allons pas faire explicitement toutes les vérifications, mais tout de même les principales. Montrons que τ respecte le produit entre $\mathbb{K}[X]$ et $\mathbb{K}'[X]$. Nous rappelons que ce produit est défini par la formule (1.361). En notant P_i les coefficients de P et Q_i ceux de Q et en remarquant que la définition de τ est essentiellement que $\tau(P)_i = \tau(P_i)$, nous avons :

$$\tau(PQ) = \tau\left(\sum_k \left(\sum_{l=0}^k P_l Q_{k-l}\right) X^k\right) \quad (6.77a)$$

$$= \sum_k X^k \sum_{l=0}^k \tau(P_l Q_{k-l}) \quad (6.77b)$$

$$= \sum_k X^k \sum_{l=0}^k \tau(P_l) \tau(Q_{k-l}) \quad (6.77c)$$

$$= \sum_k X^k \sum_{l=0}^k \tau(P)_l \tau(Q)_{k-l} \quad (6.77d)$$

$$= \sum_i (\tau(P)_i X^i) \sum_j (\tau(Q)_j X^j) \quad (6.77e)$$

$$= \tau(P) \tau(Q). \quad (6.77f)$$

Passons à l'isomorphisme d'anneaux donné par ϕ_τ .

Bien définie Si $\bar{Q}_1 = \bar{Q}_2$ alors $Q_2 = Q_1 + RP$ pour un certain $R \in \mathbb{K}[X]$. Dans ce cas,

$$\phi_\tau(Q_2) = \overline{\tau(Q_2)} = \overline{\tau(Q_1) + \tau(RP)} \quad (6.78a)$$

$$= \overline{\tau(Q_1) + \tau(R)\tau(P)} \quad (6.78b)$$

$$= \overline{\tau(Q_1)}. \quad (6.78c)$$

Ok pour bien définie.

Injection Si $\phi_\tau(\bar{Q}_1) = \phi_\tau(\bar{Q}_2)$ alors $\overline{\tau(Q_1)} = \overline{\tau(Q_2)}$, ce qui signifie que

$$\tau(Q_1) = \tau(Q_2) + R\tau(P) \quad (6.79)$$

pour un certain $R \in \mathbb{K}'[X]$. Vu que $\tau: \mathbb{K}[X] \rightarrow \mathbb{K}'[X]$ est un isomorphisme, nous pouvons y appliquer τ^{-1} pour trouver :

$$Q_1 = Q_2 + \tau^{-1}(R)P, \quad (6.80)$$

ce qui signifie que $\bar{Q}_1 = \bar{Q}_2$.

Surjection Un élément de $\mathbb{K}'[X]/(\tau(P))$ est de la forme $\bar{Q}$ avec $Q \in \mathbb{K}'[X]$. Cela est l'image par ϕ_τ de l'élément $\overline{\tau^{-1}(Q)} \in \mathbb{K}[X]/(P)$.

Morphisme Nous vous laissons vérifier que l'application ϕ_τ est un morphisme d'anneaux. □

6.3.3 Bézout

Théorème 6.43 (Bézout).

Les polynômes $P_1, \dots, P_n$ dans $\mathbb{K}[X]$ sont étrangers entre eux si et seulement s'il existe des polynômes $Q_1, \dots, Q_n \in \mathbb{K}[X]$ tels que

$$P_1Q_1 + \dots + P_nQ_n = 1. \quad (6.81)$$

Deux polynômes P et Q ne sont donc pas premiers entre eux s'il existe des polynômes x et y tels que l'identité de Bézout soit vérifiée :

$$xP + yQ = 0; \quad (6.82)$$

cette dernière pourra être écrite en termes de la matrice de Sylvester, voir sous-section 9.1.7.

Lemme 6.44.

Soient $(P_i)_{i=1, \dots, n} \in \mathbb{K}[X]$ des polynômes étrangers deux à deux. Alors les polynômes

$$Q_i = \prod_{j \neq i} P_j \quad (6.83)$$

sont étrangers entre eux¹⁰.

Lemme 6.45 ([131]).

Soit $\mathbb{K}$ un corps commutatif et $\mathbb{A} \subset \mathbb{K}$ un sous anneau de $\mathbb{K}$. Alors $\mathbb{A}[X]$, vu comme idéal de $\mathbb{K}[X]$, est un idéal premier.

En d'autres termes, si $\phi \in \mathbb{K}[X]$, et s'il existe $Q \in \mathbb{K}[X]$ unitaire tel que $\phi Q \in \mathbb{A}[X]$, alors $\phi \in \mathbb{A}[X]$.

10. Et non seulement deux à deux.

6.3.4 Lemme et théorème de Gauss

Théorème 6.46 (Théorème de Gauss).

Soient $P, Q, R \in \mathbb{K}[X]$ tels que P soit premier avec Q et divise QR . Alors P divise R .

Démonstration. Étant donné que P est premier avec Q , le théorème de Bézout¹¹ nous donne $U, V \in \mathbb{K}[X]$ tels que $PU + QV = 1$. De plus il existe un polynôme S tel que $PS = QR$. En multipliant l'identité de Bézout par R , nous obtenons

$$R = PUR + QVR = PUR + VPS = P(UR + VS), \quad (6.84)$$

ce qui signifie que P divise R . $\square$

Le lemme suivant est une généralisation du lemme de Gauss dans $\mathbb{Z}$ (lemme 3.88).

Lemme 6.47 (Lemme de Gauss[90]).

Soient les polynômes unitaires $P, Q \in \mathbb{Q}[X]$. Si $PQ \in \mathbb{Z}[X]$, alors P et Q sont tous deux dans $\mathbb{Z}[X]$.

Démonstration. Soit $a > 0$ le plus petit entier tel que $aP \in \mathbb{Z}[X]$ (c'est le PPCM des dénominateurs) et de la même façon $b > 0$ le plus petit entier tel que $bQ \in \mathbb{Z}[X]$. On pose $P_1 = aP$ et $Q_1 = bQ$.

Si $ab = 1$, alors $a = b = 1$ et nous avons tout de suite $P, Q \in \mathbb{Z}[X]$. Nous supposons donc $ab > 1$ et nous considérons p , un diviseur premier de ab . Ensuite nous considérons la projection

$$\pi_p: \mathbb{Z}[X] \rightarrow (\mathbb{Z}/p\mathbb{Z})[X]. \quad (6.85)$$

Par définition $abPQ = P_1Q_1 \in \mathbb{Z}[X]$; en prenant la projection,

$$\pi_p(P_1)\pi_p(Q_1) = \pi_p(P_1Q_1) = \pi_p(ab)\pi_p(PQ) = 0 \quad (6.86)$$

parce que $\pi_p(ab) = 0$. Étant donné que $(\mathbb{Z}/p\mathbb{Z})[X]$ est intègre (théorème 3.121), nous avons soit $\pi_p(P_1) = 0$ soit $\pi_p(Q_1) = 0$. Supposons pour fixer les idées que $\pi_p(P_1) = 0$. Alors $P_1 = pP_2$ pour un certain $P_2 \in \mathbb{Z}[X]$. Par ailleurs P est unitaire et $P_1 = aP$, donc le coefficient de plus haut degré de P_1 est a , et nous concluons que p divise a .

Mettons $a = pa'$. Dans ce cas, $pa'P = P_1 = pP_2$, et donc $a'P = P_2 \in \mathbb{Z}[X]$. Cela contredit la minimalité de a . $\square$

6.3.5 Polynômes sur un corps et pgcd

Nous savons qu'un corps est un anneau intègre (lemme 1.194). De plus l'ensemble des polynômes sur un anneau intègre est lui-même un anneau intègre (théorème 3.121). Donc la notion de pgcd à utiliser dans le cas de $\mathbb{K}[X]$ est celle de la définition 1.169.

Lemme 6.48 (Unicité du pgcd à inversibles près).

Soit un corps commutatif $\mathbb{K}$ et $S \subset \mathbb{K}[X]$. Si δ_1 et δ_2 sont des pgcd¹² de S , alors $\delta_1 = k\delta_2$ avec $k \in \mathbb{K}$.

Démonstration. Nous savons que δ_1 est un pgcd de S , mais que δ_2 divise S . Donc $\delta_2 \mid \delta_1$. De la même manière, $\delta_1 \mid \delta_2$. Il existe donc $A, B \in \mathbb{K}[X]$ tels que $\delta_1 = A\delta_2$ et $\delta_2 = B\delta_1$. En substituant,

$$\delta_1 = AB\delta_1. \quad (6.87)$$

Mais $\mathbb{K}[X]$ possède la propriété de simplification par la proposition 1.174(3). Donc $AB = 1$. Cela signifie entre autres que A et B sont des inversibles de $\mathbb{K}[X]$.

Or les seuls inversibles dans $\mathbb{K}[X]$ sont les éléments de $\mathbb{K}$; si vous en doutez, pensez que le degré de AB est supérieur ou égal à celui de A . $\square$

11. théorème 6.43.

12. Définition 1.169.

6.49.

En général, lorsque nous dirons « le » pgcd d'un ensemble, nous parlerons du pgcd unitaire, qui existe et est bien défini par le lemme 6.48.

Lemme 6.50 ([132]).

Soit un corps commutatif $\mathbb{K}$, deux polynômes quelconques $A, B \in \mathbb{K}[X]$ et un polynôme unitaire G .

Nous avons $G = \text{pgcd}(A, B)$ si et seulement si les deux conditions suivantes sont satisfaites :

- (1) Il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = G$,
- (2) G divise A et B .

Démonstration. Une implication dans chaque sens.

$\Rightarrow$ Si G est le pgcd de A et B , il est clair que $G|A$ et $G|B$. Il reste donc à montrer l'existence des polynômes U et V vérifiant $AU + BV = G$. Vu que G divise A et B , il existe des polynômes A_1, B_1 tels que $A = GA_1$ et $B = GB_1$.

Nous montrons que les polynômes A_1 et B_1 sont premiers entre eux. S'ils ont un diviseur commun D , alors GD est un diviseur commun à A et B . Or, G est le pgcd de A et B donc $GD|G$; D ne peut être qu'un polynôme constant (c'est-à-dire un élément de $\mathbb{K}$). Mais comme G est unitaire, le coefficient du terme de plus haut degré de GD doit être 1. Donc $D = 1$. L'élément 1 est l'unique diviseur commun de A_1 et B_1 ; donc A_1 et B_1 sont donc bien premiers entre eux.

D'après le théorème de Bézout 6.43, il existe donc U et V tels que $A_1U + B_1V = 1$. En multipliant par G , nous obtenons l'égalité voulue : $AU + BV = G$.

$\Leftarrow$ Si G vérifie les deux conditions, montrons que G est le pgcd de A et B . Nous savons déjà (par hypothèse) que G divise A et B , il reste à montrer que tous les diviseurs communs à A et B divisent aussi G . Soit donc D un diviseur commun à A et B : il existe A_1 et B_1 tels que $A = DA_1$ et $B = DB_1$. Nous savons que $G = AU + BV$ donc $G = D(A_1U + B_1V)$, et $D|G$. Par définition, G est bien le pgcd de A et B .

□

Notons qu'en supprimant la condition d'unitarité de G , le résultat tient presque : il suffit de remplacer partout « le pgcd » par « un pgcd ».

Lemme 6.51 ([132]).

Soient deux polynômes A, B premiers entre eux. Si le polynôme P est divisible par A et par B alors P est divisible par AB .

Démonstration. Vu que $A | P$, il existe $Q_1 \in \mathbb{K}[X]$ tel que $P = AQ_1$. Mais B divise $P = AQ_1$ alors que B est premier avec A ; donc d'après le théorème de Gauss 6.46 : $B|Q_1$.

Il existe donc $Q_2 \in \mathbb{K}[X]$ tel que $Q_1 = BQ_2$. On a donc $P = ABQ_2$: P est bien divisible par AB . □

Lemme 6.52 ([132]).

Quelques propriétés du PGCD¹³ dans les polynômes. Soient des polynômes $P, Q, R \in \mathbb{K}[X]$.

- (1) Nous avons l'égalité¹⁴

$$\text{pgcd}(P, PQ + R) = \text{pgcd}(P, R). \quad (6.88)$$

- (2) Si Q et R sont premiers entre eux,

$$\text{pgcd}(P, QR) = \text{pgcd}(P, Q) \text{pgcd}(P, R) \quad (6.89)$$

13. Définition 1.169.

14. Notez l'analogie avec le lemme 3.6.

(3) Si P et Q sont premiers entre eux,

$$\text{pgcd}(P, QR) = \text{pgcd}(P, R) \quad (6.90)$$

Démonstration. Dans la suite si A et B sont des polynômes, nous dirons « les diviseurs de $\{A, B\}$ » pour parler des diviseurs communs de A et B .

(1) Nous montrons que $\{P, PQ + R\}$ a les mêmes diviseurs que $\{P, R\}$.

D'une part, si $A \mid \{P, PQ + R\}$, alors il existe des polynômes B_1 et B_2 tels que $P = AB_1$ et $PQ + R = AB_2$. Donc

$$R = AB_2 - PQ = AB_2 - AB_1Q = A(B_2 - B_1Q), \quad (6.91)$$

et nous concluons que A divise R .

D'autre part, si $A \mid \{P, R\}$ alors il existe des polynômes B_1 et B_2 tels que $P = AB_1$ et $R = AB_2$. Donc

$$PQ + R = AB_1Q + AB_2 = A(B_1Q + B_2), \quad (6.92)$$

et A divise $PQ + R$.

Conclusion : les paires $\{P, PQ + R\}$ et $\{P, R\}$ ont même ensemble de diviseurs, et donc même pgcd.

(2) Nous avons trois polynômes P, Q, R et nous savons que Q et R sont premiers entre eux. Nous notons : $G_1 = \text{pgcd}(P, Q)$ et $G_2 = \text{pgcd}(P, R)$. Il faut montrer que G_1G_2 est le pgcd de P et QR ; pour cela nous allons utiliser le lemme 6.50.

$\exists U, V$ tels que $G_1G_2 = PU + QRV$ Vu que $G_1 = \text{pgcd}(P, Q)$, il existe U_1 et V_1 tels que $G_1 = PU_1 + QV_1$ (lemme 6.50). On a de même : $G_2 = PU_2 + RV_2$. En prenant le produit :

$$G_1G_2 = (PU_1 + QV_1)(PU_2 + RV_2) = P(PU_1U_2 + RU_1V_2 + QV_1V_2) + QR(V_1V_2). \quad (6.93)$$

Donc c'est bon pour ce point.

G_1 et G_2 sont premiers entre eux Si D est un diviseur commun à G_1 et G_2 , alors D divise Q et R qui sont premiers entre eux ; D ne peut être qu'un polynôme constant. Tous les diviseurs communs de G_1 et G_2 sont dans $\mathbb{K}$. Mais le pgcd est par définition un diviseur commun unitaire, donc $\text{pgcd}(G_1, G_2) = 1$. Cela signifie que G_1 et G_2 sont premiers entre eux (définition 1.180).

$G_1G_2 \mid QR$ En effet : $G_1 \mid Q$ et $G_2 \mid R$ donc $G_1G_2 \mid QR$.

$G_1G_2 \mid P$ Le polynôme P est divisible par G_1 et par G_2 , et de plus G_1 et G_2 sont premiers entre eux. Donc le lemme 6.51 conclut que P est divisible par G_1G_2 .

(3) Supposons d'abord que $A \in \mathbb{K}[X]$ divise P et QR . Le théorème de Bézout 6.43 assure l'existence de polynômes U et V tels que $PU + QV = 1$. Ensuite l'hypothèse de division nous donne des polynômes B_1 et B_2 tels que $P = AB_1$ et $QR = AB_2$. Nous avons :

$$1 = PU + QV = AB_1U + QV. \quad (6.94)$$

Cela prouve que A est premier avec Q grâce encore à Bézout, mais dans l'autre sens. Donc A est premier avec Q et $A \mid QR$. Donc $A \mid R$ par le théorème de Gauss 6.46.

Dans l'autre sens, si $A \mid R$ alors on a évidemment : $A \mid QR$.

Les diviseurs de $\{P, QR\}$ sont exactement les diviseurs de $\{P, R\}$. En conséquence, nous concluons que les paires $\{P, QR\}$ et $\{P, R\}$ ont le même pgcd.

□

6.4 Extension de corps

Lemme 6.53.

Soit $\mathbb{L}$ un corps¹⁵ fini et $\mathbb{K}$ un sous corps de $\mathbb{L}$. Alors il existe $s \in \mathbb{N}$ tel que

$$\text{Card}(\mathbb{L}) = \text{Card}(\mathbb{K})^s. \quad (6.95)$$

Démonstration. Le corps $\mathbb{L}$ est un $\mathbb{K}$ -espace vectoriel de dimension finie. Si s est la dimension alors nous avons la formule (6.95) parce que chaque élément de $\mathbb{L}$ est un s -uplet d'éléments de $\mathbb{K}$. $\square$

Définition 6.54 ([133]).

Soit $\mathbb{K}$ un corps commutatif. Une **extension** de $\mathbb{K}$ est un couple $(\mathbb{L}, j)$ où $\mathbb{L}$ est un corps et $j: \mathbb{K} \rightarrow \mathbb{L}$ est un morphisme de corps.

Nous identifions le plus souvent $\mathbb{K}$ avec $i(\mathbb{K}) \subset \mathbb{L}$, mais il faut savoir que le corps $\mathbb{L}$ étendant $\mathbb{K}$ n'est pas toujours un sur-corps de $\mathbb{K}$. En particulier, l'ensemble $\mathbb{L}$ peut ne pas être un extension de l'ensemble $\mathbb{K}$.

Lemme-Définition 6.55.

Si $(\mathbb{L}, i)$ est une extension de $\mathbb{K}$, alors $\mathbb{L}$ devient un espace vectoriel sur $\mathbb{K}$ si nous posons

$$\lambda \cdot x = i(\lambda)x \quad (6.96)$$

pour tout $\lambda \in \mathbb{K}$ et $x \in \mathbb{L}$. La multiplication du membre de droite est celle du corps $\mathbb{L}$.

Définition 6.56.

Le **degré** de $\mathbb{L}$ est la dimension de cet espace vectoriel. Il est noté $[\mathbb{L} : \mathbb{K}]$; notons qu'il peut être infini.

Exemple 6.57.

L'ensemble $\mathbb{C}$ est une extension de $\mathbb{R}$ et son degré est $[\mathbb{C} : \mathbb{R}] = 2$. $\triangle$

Proposition 6.58 (Composition des degrés[134]).

Si $\mathbb{L}_2$ est une extension de $\mathbb{L}_1$ qui est elle-même une extension de $\mathbb{K}$, alors $\mathbb{L}_2$ est une extension de $\mathbb{K}$ et on a :

$$[\mathbb{L}_2 : \mathbb{K}] = [\mathbb{L}_2 : \mathbb{L}_1][\mathbb{L}_1 : \mathbb{K}]. \quad (6.97)$$

Dans ce cas, si $\{v_i\}_{i \in I}$ est une $\mathbb{K}$ -base de $\mathbb{L}_1$ et si $\{w_\alpha\}_{\alpha \in A}$ est une $\mathbb{L}_1$ -base de $\mathbb{L}_2$ alors $\{v_i w_\alpha\}_{\substack{i \in I \\ \alpha \in A}}$ est une $\mathbb{K}$ -base de $\mathbb{L}_2$.

Notons que la formule (6.97) n'est pas très instructive dans le cas des extensions non finies. La seconde partie, sur les bases, est en réalité nettement plus intéressante.

Démonstration. Soit $a \in \mathbb{L}_2$. Vu que les w_α forment une $\mathbb{L}_2$ -base nous avons une décomposition

$$a = \sum_{\alpha} a_{\alpha} w_{\alpha} \quad (6.98)$$

pour des éléments $a_{\alpha} \in \mathbb{L}_1$. Mais les v_i forment une $\mathbb{K}$ -base de $\mathbb{L}_1$, donc chacun des a_{α} peut être décomposé comme $a_{\alpha} = \sum_i a_{\alpha i} v_i w_{\alpha}$. Donc :

$$a = \sum_{\alpha i} a_{\alpha i} v_i w_{\alpha}, \quad (6.99)$$

qui donne une décomposition de a en éléments de $\{v_i w_{\alpha}\}$ à coefficients dans $\mathbb{K}$. La partie proposée est donc génératrice.

Pour prouver qu'elle est également libre, nous supposons avoir des éléments $a_{\alpha i} \in \mathbb{K}$ tels que

$$\sum_{\alpha i} a_{\alpha i} v_i w_{\alpha} = 0. \quad (6.100)$$

15. Définition 1.190.

En récrivant sous la forme

$$\sum_{\alpha} \left(\sum_i a_{\alpha i} v_i \right) w_{\alpha} = 0, \quad (6.101)$$

nous reconnaissons une combinaison linéaire nulle des w_{α} à coefficients dans $\mathbb{L}_1$. Les coefficients sont donc nuls : $\sum_i a_{\alpha i} v_i = 0$. Cela est une combinaison linéaire nulle des v_i à coefficients dans $\mathbb{K}$. Vu que les v_i forment une base, les coefficients sont nuls : $a_{\alpha i} = 0$. $\square$

6.4.1 Extension et polynôme minimal

Lemme-Définition 6.59 (Polynôme minimal).

Soit $\mathbb{L}$ une extension de $\mathbb{K}$ et $a \in \mathbb{L}$. Nous considérons la partie

$$I_a = \{P \in \mathbb{K}[X] \text{ tel que } P(a) = 0\} \quad (6.102)$$

que nous supposons non réduite à $\{0\}$ ¹⁶

- (1) La partie I_a est un idéal dans $\mathbb{K}[X]$,
- (2) la partie I_a est un idéal principal dans $\mathbb{K}[X]$,
- (3) l'idéal I_a possède un unique générateur unitaire.

Cet unique générateur unitaire est le **polynôme minimal** de a sur $\mathbb{K}$.

Démonstration. En plusieurs parties.

Pour (1) Soit $P \in I_a : P(a) = 0$. Si $Q \in \mathbb{K}[X]$ alors la proposition 1.243 nous indique que

$$(PQ)(a) = P(a)Q(a) = 0. \quad (6.103)$$

Donc $PQ \in I_a$. Comme de plus I_a est clairement vectoriel, I_a est un idéal.

Notez que nous avons utilisé la règle du produit nul justifiée par le fait que $\mathbb{K}$ soit un corps ¹⁷ et donc soumis au point (3) de la proposition 1.174.

Pour (2) Nous savons par le théorème 6.39 que $\mathbb{K}[X]$ est un anneau principal. En particulier, tous ses idéaux sont principaux, c'est dans la définition 3.72 d'un anneau principal.

Pour (3) Le théorème 6.39(3) nous informe alors que I_a possède un unique générateur unitaire. $\square$

Si nous avons un corps et un élément dans une extension du corps, il n'est pas autorisé de dire « soit le polynôme minimal de cet élément dans le premier corps » parce qu'il n'existe peut-être pas de polynôme annulateur.

6.60.

Dans le cas des opérateurs sur un espace de dimension finie (par exemple les matrices), il existe toujours un polynôme minimal, comme nous le verrons dans le lemme 9.92.

Exemple 6.61.

Le polynôme minimal dépend du corps sur lequel on le considère. Par exemple le nombre imaginaire pur i accepte $X - i$ comme polynôme minimal sur $\mathbb{C}$ et $X^2 + 1$ sur $\mathbb{Q}[X]$. $\triangle$

Proposition 6.62 ([1]).

Soit $\mathbb{L}$ une extension de $\mathbb{K}$ et $a \in \mathbb{L}$ dont le polynôme minimal sur $\mathbb{K}$ est $\mu_a \in \mathbb{K}[X]$. Alors

- (1) le polynôme μ_a est irréductible ¹⁸ sur $\mathbb{K}$;

16. La non trivialité de I_a est une vraie hypothèse. En effet si nous prenons $\mathbb{K} = \mathbb{Q}$ et l'extension $\mathbb{L} = \mathbb{R}$, alors il suffit de prendre un réel a non algébrique sur $\mathbb{Q}$ pour que I_a soit réduit au seul polynôme identiquement nul.

17. Si vous connaissez un contre-exemple à cette proposition dans le cas où $\mathbb{K}$ serait remplacé par un anneau, écrivez-moi.

18. Définition 6.32.

(2) Le polynôme μ_a est premier¹⁹ avec tout polynôme de $\mathbb{K}[X]$ non annulateur de a .

Démonstration. Une chose à la fois.

- (1) D'abord le polynôme μ_a n'est pas inversible parce que seuls les éléments de $\mathbb{K}$ (ceux de degré zéro) peuvent être inversibles²⁰. Mais ces polynômes sont constants et ne peuvent donc pas être des polynômes annulateurs de quoi que ce soit.

Ensuite, supposons la décomposition $\mu_a = PQ$ avec $P, Q \in \mathbb{K}[X]$. En évaluant cette égalité en a nous avons

$$0 = P(a)Q(a). \quad (6.104)$$

Vu que nous sommes sur un corps, nous avons la règle du produit nul²¹ et nous déduisons que soit $P(a)$ soit $Q(a)$ est nul, ou les deux. Pour fixer les idées, nous supposons $P(a) = 0$.

Dans ce cas, P fait partie de l'idéal annulateur de a , lequel idéal est engendré par μ_a . Donc il existe $S \in \mathbb{K}[X]$ tel que $P = S\mu_a$. En réécrivant $\mu_a = PQ$ avec cela nous avons :

$$\mu_a = S\mu_a Q \quad (6.105)$$

ou encore : $SQ = 1$, ce qui signifie que S et Q sont dans $\mathbb{K}$ et inversibles.

Nous concluons que μ_a ne peut pas être écrit sous forme de produit de deux non inversibles.

- (2) Soit Q un polynôme non annulateur de a . Soit aussi un diviseur commun P de Q et μ_a dans $\mathbb{K}[X]$. Nous devons prouver que P est un inversible, c'est-à-dire un élément de $\mathbb{K}$ (le fait que P ne soit pas le polynôme nul est évident). Nous avons $\mu_a = PR_1$ et $Q = PR_2$ pour certains polynômes $R_1, R_2 \in \mathbb{K}[X]$. Vu que μ_a est irréductible par (1), il n'est pas produit de deux non inversibles. En d'autres termes, soit P soit R_1 est inversible. Si P n'est pas inversible, alors R_1 est inversible ; disons $R_1 = k \in \mathbb{K}$. Alors

$$0 = \mu_a(a) = P(a)k, \quad (6.106)$$

donc $P(a) = 0$. Mais alors

$$Q(a) = P(a)R_2(a) = 0, \quad (6.107)$$

ce qui est contraire à l'hypothèse selon laquelle Q n'était pas annulateur de a .

Nous retenons donc que P est inversible, ce qu'il fallait montrer.

□

Définition 6.63.

Deux éléments α et β dans $\mathbb{L}$ sont dit **conjugués** s'ils ont même polynôme minimal. Par exemple i et $-i$ sont conjugués dans $\mathbb{C}$ vu comme extension de $\mathbb{Q}$.

6.4.2 Extensions algébriques et éléments transcendants

6.4.2.1 Éléments algébriques et transcendants

Définition 6.64.

L'ensemble $A[X]$ devient un $\mathbb{K}$ -espace vectoriel avec la définition

$$(\lambda P)_k = \lambda P_k. \quad (6.108)$$

Voici une définition d'un élément algébrique sur un corps. Une caractérisation plus « pratique » sera donnée dans le lemme 6.67.

19. Définition 3.128.

20. Et d'ailleurs, le sont, mais ce n'est pas important ici.

21. Parce que un corps est un anneau intègre par le lemme 1.194 et qu'un anneau intègre est justement un anneau sur lequel nous avons la règle du produit nul, voir la définition 1.174.

Lemme-Définition 6.65 (Élément algébrique et transcendant[135]).

Soit une extension $\mathbb{L}$ de $\mathbb{K}$ et $\alpha \in \mathbb{L}$. Nous considérons l'application

$$\begin{aligned}\varphi: \mathbb{K}[X] &\rightarrow \mathbb{L} \\ P &\mapsto P(\alpha).\end{aligned}\tag{6.109}$$

Alors

(1) L'application φ est un morphisme d'anneaux²².

(2) L'application φ est un morphisme de $\mathbb{K}$ -espace vectoriel.

Si φ est injective, nous disons que α est **transcendant**. Sinon, nous disons qu'il est **algébrique**.

Démonstration. Le fait que φ soit un morphisme d'anneaux est le lemme 1.243 déjà prouvé.

Pour le morphisme de $\mathbb{K}$ -espace vectoriel, il faut seulement ajouter le calcul

$$\varphi(\lambda P) = (\lambda P)(\alpha) = \lambda P(\alpha) = \lambda \varphi(P).\tag{6.110}$$

Notons la justification suivante qui n'est pas tout à fait triviale :

$$(\lambda P)(\alpha) = \sum_k (\lambda P)_k \alpha^k = \sum_k \lambda P_k \alpha^k = \lambda P(\alpha)\tag{6.111}$$

qui utilise la définition 6.64. □

Exemple 6.66.

L'injectivité de φ n'est pas automatique. Prenons par exemple $\mathbb{L} = \mathbb{Q}[\sqrt{2}]$ dans $\mathbb{R}$. Les polynômes dans $\mathbb{Q}[X]$ ont des degrés arbitrairement élevés en X , tandis que les éléments de $\mathbb{L}$ n'ont pas de degré très élevés en $\sqrt{2}$ parce que $\sqrt{2}\sqrt{2} = 2$. L'ensemble $\mathbb{Q}[\sqrt{2}]$ ne contient donc que des éléments de la forme $a + b\sqrt{2}$ avec $a, b \in \mathbb{Q}$.

Si par contre $x_0 \in \mathbb{R}$ n'est racine d'aucun polynôme (cela existe parce que $\mathbb{R}$ n'est pas dénombrable), alors $\mathbb{Q}[x_0]$ contient tous les $\sum_{k=0}^N a_k x_0^k$ avec N arbitrairement grand. Et tous ces nombres sont différents. △

Le lemme suivant donne une caractérisation d'élément algébrique moins abstraite que la définition 6.65.

Lemme 6.67.

Soit $\mathbb{K}$, un corps et $\mathbb{L}$, une extension de $\mathbb{K}$. Un élément $\alpha \in \mathbb{L}$ est algébrique sur $\mathbb{K}$ si et seulement si existe un polynôme non nul $P \in \mathbb{K}[X]$ tel que $P(\alpha) = 0$.

Démonstration. Nous considérons l'application φ de la définition 6.65. Si φ n'est pas injective, c'est qu'il existe un polynôme P dans $\mathbb{K}[X]$ tel que $\varphi(P) = 0$. Dans ce cas, $P(\alpha) = 0$.

À l'inverse si il existe P non nul dans $\mathbb{K}[X]$ tel que $P(\alpha) = 0$, alors $\varphi(P) = 0$ et φ n'est pas injective. □

Définition 6.68.

Un corps $\mathbb{K}$ est **algébriquement clos** si tout polynôme non constant à coefficients dans $\mathbb{K}$ contient au moins une racine dans $\mathbb{K}$.

Définition 6.69 (Extension algébrique, clôture algébrique).

Soient un corps $\mathbb{K}$ et une extension $\alpha: \mathbb{K} \rightarrow \mathbb{L}$.

(1) L'extension $\mathbb{L}$ est une extension **algébrique** de $\mathbb{K}$ si tous ses éléments sont algébriques²³ sur $\mathbb{K}$, c'est à dire sont racines de polynômes à coefficients dans $\alpha(\mathbb{K})$, voir le lemme 6.67.

(2) L'extension $\mathbb{L}$ est **algébriquement close** si tout $\mathbb{L}$ est algébriquement clos (définition 6.68).

22. Définition 1.31.

23. Définition 6.65.

(3) L'extension $\mathbb{L}$ est une **clôture algébrique** du corps $\mathbb{K}$ si elle est une extension algébrique qui est algébriquement close.

6.70.

Donc une extension est algébrique si elle contient seulement des racines de polynômes ; elle est close si elle contient au moins une racine de chaque polynôme. Elle est une clôture algébrique si elle est les deux en même temps.

Exemple 6.71.

Le corps $\mathbb{R}$ n'est pas une extension algébrique de $\mathbb{Q}$. En effet il existe seulement une infinité *dénombrable* de polynômes dans $\mathbb{Q}[X]$ et donc une infinité dénombrable de racines de tels polynômes. Toute extension algébrique de $\mathbb{Q}$ est donc dénombrable. Voir aussi la proposition 6.123. $\triangle$

Lemme 6.72.

Un corps est algébriquement clos si et seulement si tous ses polynômes sont scindés²⁴.

Démonstration. Si tout polynôme est scindé, tout polynôme possède des racines ; c'est l'autre sens qui est plus consistant.

Soit un corps algébriquement clos $\mathbb{K}$. Nous allons par récurrence sur le degré des polynômes. Si P est un polynôme de degré 1, alors il est scindé.

Nous supposons que tous les polynômes de degré $n - 1$ sont scindés. Soit un polynôme P de degré n . Le corps étant algébriquement clos, le polynôme P a une racine que nous notons $a_n \in \mathbb{K}$. La proposition 3.140 nous explique qu'il existe un polynôme Q de degré $n - 1$ tel que $P = (X - a_n)Q$.

Par hypothèse de récurrence, le polynôme Q est scindé : il existe $\{a_i\}_{i=1, \dots, n-1}$ dans $\mathbb{K}$ tels que $Q = \prod_{i=1}^{n-1} (X - a_i)$. Au final,

$$P = (X - a_n)Q = \prod_{k=1}^n (X - a_k) \quad (6.112)$$

et P est scindé. $\square$

Lemme 6.73.

Soient un corps $\mathbb{K}$ et un polynôme $P \in \mathbb{K}[X]$. Nous supposons que P est scindé :

$$P = \prod_{k=1}^n (X - a_k). \quad (6.113)$$

Si α est une racine de P , alors α est l'un des a_k .

Démonstration. Dire que α est une racine de P revient à dire que

$$\prod_{k=1}^n (\alpha - a_k) = 0 \quad (6.114)$$

Un corps est toujours un anneau intègre (lemme 1.194), c'est à dire que la règle du produit nul est utilisable. Dans notre cas, le produit nul (6.114) nous indique que $\alpha - a_i = 0$ pour (au moins) un des i . Donc effectivement α est l'un des a_i . $\square$

Lemme 6.74.

Soient un corps algébriquement clos $\mathbb{K}$ ainsi qu'une extension algébrique $\alpha: \mathbb{K} \rightarrow \mathbb{L}$. Alors $\alpha(\mathbb{K}) = \mathbb{L}$.

Démonstration. Nous allons montrer que tous les éléments de $\mathbb{L}$ sont dans l'image de α . Soit donc $l \in \mathbb{L}$. Vu que l'extension $\alpha: \mathbb{K} \rightarrow \mathbb{L}$ est une extension algébrique, il existe un polynôme $P \in \alpha(\mathbb{K})[X]$ tel que $P(l) = 0$.

24. Définition 6.34

Étant donné que α est injective, il est possible de considérer le polynôme $Q = \alpha^{-1}(P)$, c'est à dire que, si $P = \sum_k a_k X^k$, nous posons $Q = \sum_k \alpha^{-1}(a_k) X^k$.

Le corps $\mathbb{K}$ étant algébriquement clos, le polynôme Q est scindé (proposition 6.72) :

$$Q = \prod_{k=1}^n (X - b_k) \quad (6.115)$$

avec $b_k \in \mathbb{K}$. Nous avons alors aussi la factorisation

$$P = \prod_{k=1}^n (X - \alpha(b_k)) \quad (6.116)$$

dans $\mathbb{L}[X]$. Nous avons vu que l était une racine de P . Donc l est un des $\alpha(b_k)$ (lemme 6.73). Cela prouve que $l \in \alpha(\mathbb{K})$. $\square$

6.4.3 Extension algébrique et polynôme minimal

Proposition 6.75 ([68]).

Soit une extension algébrique²⁵ $\mathbb{L}$ du corps $\mathbb{K}$.

- (1) Pour tout $a \in \mathbb{L}$, il existe un polynôme $P \in \mathbb{K}[X]$ tel que $P(a) = 0$.
- (2) Le polynôme minimal de a dans $\mathbb{K}[X]$ est l'unique polynôme unitaire irréductible annulant a .

Démonstration. Le premier point est seulement la définition 6.69 d'une extension algébrique.

L'idéal annulateur $I_a = \{P \in \mathbb{K}[X] \text{ tel que } P(a) = 0\}$ n'est pas réduit à $\{0\}$ parce que $\mathbb{L}$ est une extension algébrique. L'existence du polynôme minimal est le lemme 6.59 et le fait qu'il soit irréductible est la proposition 6.62(1).

Ce qui nous intéresse ici est l'unicité. Soit $\mu_1 \in \mathbb{K}[X]$, un polynôme annulateur de a irréductible et unitaire. Vu que $\mu_1 \in I_a$ et que par définition, $I_a = (\mu)$, il existe $P \in \mathbb{K}[X]$ tel que $\mu_1 = P\mu$. Vu que μ n'est pas inversible et que μ_1 est irréductible, P doit être inversible : $\mu_1 = k\mu$ pour un certain $k \in \mathbb{K}$.

Vu que μ et μ_1 sont unitaires, $k = 1$. Donc $\mu_1 = \mu$. $\square$

Lemme 6.76.

Soient un corps $\mathbb{K}$, une extension $\mathbb{L}$ de $\mathbb{K}$ et $\alpha \in \mathbb{L}$, un élément algébrique²⁶ sur $\mathbb{K}$. Si μ est le polynôme minimal de α sur $\mathbb{K}$ alors

$$\begin{aligned} \varphi: \mathbb{K}[\alpha] &\rightarrow \mathbb{K}[X]/(\mu) \\ Q(\alpha) &\mapsto \bar{Q} \end{aligned} \quad (6.117)$$

avec $Q \in \mathbb{K}[X]$ est un isomorphisme de corps et de $\mathbb{K}$ -espaces vectoriels.

Démonstration. D'abord, α est algébrique, donc l'idéal annulateur I_α n'est pas réduit à $\{0\}$, et l'existence d'un polynôme minimal est assurée par le lemme 6.59.

Ensuite, le fait que $\mathbb{K}[X]/(\mu)$ soit un corps est le corolaire 6.40. Nous montrons à présent que φ est un isomorphisme (d'anneaux) ; cela suffit pour en déduire que $\mathbb{K}[\alpha]$ est également un corps.

Ces préliminaires étant dits, nous commençons.

Bien définie Nous devons prouver que φ est bien définie, c'est-à-dire que tout élément de $\mathbb{K}[\alpha]$ peut être écrit sous la forme $Q(\alpha)$ pour un $Q \in \mathbb{K}[X]$, et que si $Q_1(\alpha) = Q_2(\alpha)$ alors $\bar{Q}_1 = \bar{Q}_2$. Le fait que tous les éléments de $\mathbb{K}[\alpha]$ peuvent être écrits sous la forme $Q(\alpha)$ est la proposition 3.120. Supposons que $Q_1(\alpha) = Q_2(\alpha)$. Alors nous définissons $R \in \mathbb{K}[X]$ par $Q_1 = Q_2 + R$, et en évaluant cette égalité en α nous avons

$$Q_1(\alpha) = Q_2(\alpha) + R(\alpha), \quad (6.118)$$

25. Définition 6.69.

26. Définition 6.65.

autrement dit $R(\alpha) = 0$. Donc R est dans l'idéal annulateur de α et est donc dans (μ) , c'est-à-dire que dans le quotient $\mathbb{K}[X]/(\mu)$ nous avons $\bar{R} = 0$ et donc $\bar{Q}_1 = \bar{Q}_2$.

Surjective Tout élément de $\mathbb{K}[X]/(\mu)$ est de la forme $\bar{Q}$ pour un $Q \in \mathbb{K}[X]$. Or ces éléments sont ceux de l'ensemble d'arrivée de φ .

Injective Si $\bar{Q}_1 = \bar{Q}_2$, alors $Q_1 = Q_2 + R$ avec R dans l'idéal engendré par μ , c'est-à-dire entre autres $R(\alpha) = 0$. Donc $Q_1(\alpha) = Q_2(\alpha)$.

Nous devons encore montrer que nous avons là un morphisme de $\mathbb{K}$ -espaces vectoriels.

(1) Si $k \in \mathbb{K}$ alors $\varphi(kQ(\alpha)) = \overline{kQ}$. Mais par définition de la structure d'espace vectoriel sur $\mathbb{K}[X]/(\mu)$, $\overline{kQ} = k\bar{Q}$ (vérifier que cette définition de la multiplication par un scalaire sur $\mathbb{K}[X]/(\mu)$ est correcte).

(2) Nous avons aussi $\varphi(Q_1(\alpha) + Q_2(\alpha)) = \varphi((Q_1 + Q_2)(\alpha)) = \overline{Q_1 + Q_2} = \bar{Q}_1 + \bar{Q}_2$.

□

6.4.4 Extensions et polynômes

Nous savons déjà depuis la définition 1.240 ce qu'est $A[X]$ pour tout anneau A et donc a fortiori pour un corps.

Définition 6.77.

Soit un corps commutatif²⁷. Nous notons $\mathbb{K}(X)$ le corps des fractions²⁸ de $\mathbb{K}[X]$.

Lemme-Définition 6.78.

Si $R \in \mathbb{K}(X)$, avec $R = P/Q$ et si $\mathbb{L}$ est une extension²⁹ de $\mathbb{K}$ contenant l'élément α , alors nous définissons

$$R(\alpha) = P(\alpha)Q(\alpha)^{-1}. \quad (6.119)$$

Cela est une bonne définition au sens où elle ne dépend pas du choix du représentant (P, Q) pris dans la classe P/Q .

Démonstration. Supposons $R = P_1/Q_1 = P_2/Q_2$. Par définition des classes (définition 1.248) nous avons

$$P_1Q_2 = Q_1P_2. \quad (6.120)$$

Vu que l'évaluation est un morphisme $\mathbb{K}[X] \rightarrow \mathbb{K}$ ³⁰ nous pouvons évaluer l'équation (6.120) en α :

$$P_1(\alpha)Q_2(\alpha) = Q_1(\alpha)P_2(\alpha). \quad (6.121)$$

Cette dernière est une égalité dans le corps $\mathbb{K}$. Nous pouvons donc la multiplier par $Q_2(\alpha)^{-1}P_2(\alpha)^{-1}$ (et utiliser toutes les hypothèses de commutativité des anneaux et corps) pour obtenir

$$P_1(\alpha)Q_1(\alpha)^{-1} = P_2(\alpha)Q_2(\alpha)^{-1}, \quad (6.122)$$

c'est-à-dire

$$(P_1/Q_1)(\alpha) = (P_2/Q_2)(\alpha). \quad (6.123)$$

□

Proposition-Définition 6.79 ([1]).

Soient un corps $\mathbb{K}$, une extension $(\mathbb{L}, j_{\mathbb{L}})$ de $\mathbb{K}$ et un élément $\alpha \in \mathbb{L}$. Nous définissons $\mathbb{K}(\alpha)_{\mathbb{L}}$ comme étant l'intersection de tous les sous-corps de $\mathbb{L}$ contenant $j_{\mathbb{L}}(\mathbb{K})$ et α .

Alors

27. Sauf mention du contraire, tous les corps du Frido sont commutatifs.

28. Définition 1.248.

29. Définition 6.54.

30. Lemme 1.243. Certes ce lemme ne parle que d'anneaux, mais à y bien penser, dans le passage de (6.120) à (6.121), nous ne considérons que les structures d'anneaux sur $\mathbb{K}[X]$ et $\mathbb{K}$.

- (1) $\mathbb{K}(\alpha)_{\mathbb{L}}$ est un sous-corps de $\mathbb{L}$,
 (2) $\mathbb{K}(\alpha)_{\mathbb{L}}$ est une extension³¹ de $\mathbb{K}$.

Démonstration. Nous commençons par prouver que $\mathbb{K}(\alpha)_{\mathbb{L}}$ est bien un corps. Si $a, b \in \mathbb{K}(\alpha)_{\mathbb{L}}$ alors il suffit de calculer ab , $a + b$ et a^{-1} dans n'importe quel sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et α ; nous avons une garantie que a , b , ab , $a + b$ et a^{-1} sont dans tous les tels sous-corps.

Pour prouver que $\mathbb{K}(\alpha)_{\mathbb{L}}$ est bien une extension, nous devons trouver un homomorphisme de corps $j: \mathbb{K} \rightarrow \mathbb{K}(\alpha)_{\mathbb{L}}$. Il se fait que prendre $j = j_{\mathbb{L}}$ fonctionne parce que par définition, $\mathbb{K}(\alpha)_{\mathbb{L}}$ est une partie de $\mathbb{L}$ contenant l'image de $j_{\mathbb{L}}$. $\square$

Lemme 6.80.

Soit n tel que $\sqrt{n}$ ne soit pas un rationnel. Si $\alpha \in \{a + b\sqrt{n}\}_{a,b \in \mathbb{Q}}$, alors il existe un unique choix $(x, y) \in \mathbb{Q}^2$ tel que

$$\alpha = x + y\sqrt{n}. \quad (6.124)$$

Démonstration. L'existence est dans la définition de α . Il s'agit de voir l'unicité. Supposons $x + y\sqrt{n} = a + b\sqrt{n}$ avec $x, y, a, b \in \mathbb{Q}$. Si $b \neq y$ nous pouvons écrire

$$\sqrt{n} = \frac{x - a}{b - y}. \quad (6.125)$$

Vu que $\sqrt{n}$ n'est pas un rationnel, une telle écriture est impossible. Donc $b = y$. Nous avons alors $x + y\sqrt{n} = a + y\sqrt{n}$ et du coup aussi $x = a$. $\square$

Exemple 6.81.

Nous avons

$$\mathbb{Q}(\sqrt{2})_{\mathbb{R}} = \{a + b\sqrt{2}\}_{a,b \in \mathbb{Q}} \quad (6.126)$$

où à droite nous calculons les sommes et les produits dans $\mathbb{R}$. Le tout est un sous-ensemble de $\mathbb{R}$ qui se révèle être un corps contenant $\mathbb{Q}$ et $\sqrt{2}$.

En particulier, dans $\mathbb{Q}(\sqrt{2})_{\mathbb{R}}$ nous avons $\sqrt{2}\sqrt{2} = 2$. $\triangle$

Lemme 6.82.

Les corps $\mathbb{Q}(\sqrt{2})_{\mathbb{R}}$ et $\mathbb{Q}(\sqrt{3})_{\mathbb{R}}$ ne sont pas isomorphes.

Démonstration. Supposons l'existence d'un morphisme de corps³²

$$\psi: \mathbb{Q}(\sqrt{2})_{\mathbb{R}} \rightarrow \mathbb{Q}(\sqrt{3})_{\mathbb{R}}. \quad (6.127)$$

Nous notons « 1 » à la fois le neutre de la multiplication dans $\mathbb{Q}(\sqrt{2})_{\mathbb{R}}$ et $\mathbb{Q}(\sqrt{3})_{\mathbb{R}}$ (qui s'évèrent être les mêmes en tant qu'élément de $\mathbb{R}$, mais ça n'a pas d'importance ici).

Soit $\alpha \in \mathbb{Q}(\sqrt{2})_{\mathbb{R}}$ tel que $\alpha^2 - 1 = 0$. Alors nous avons aussi

$$\psi(\alpha)^2 - 1 = \psi(\alpha^2) - \psi(1) = \psi(\alpha^2 - 1) = \psi(0) = 0. \quad (6.128)$$

Donc $\psi(\alpha)$ est un élément de $\mathbb{Q}(\sqrt{3})_{\mathbb{R}}$ qui est une racine de $X^2 - 1$.

Or un tel élément n'existe pas dans $\mathbb{Q}(\sqrt{3})_{\mathbb{R}}$ parce que nous savons que dans $\mathbb{R}$ entier, il n'y a que deux racines : $\pm\sqrt{2}$, et aucune des deux n'est dans $\mathbb{Q}(\sqrt{3})_{\mathbb{R}}$. $\square$

Exemple 6.83.

Est-ce que $\mathbb{K}(\alpha)_{\mathbb{L}}$ dépend réellement de $\mathbb{L}$? Si $\mathbb{L}_2$ est une extension de $\mathbb{L}$ alors nous avons évidemment³³ $\mathbb{K}(\alpha)_{\mathbb{L}_2} = \mathbb{K}(\alpha)_{\mathbb{L}}$.

Nous commençons par construire un corps $\mathbb{K}$ un peu idiot qui, comme ensemble, est comme $\mathbb{Q}(\sqrt{2})_{\mathbb{R}}$, c'est-à-dire la partie

$$\{a + b\sqrt{2}\}_{a,b \in \mathbb{Q}}, \quad (6.129)$$

31. Définition 6.54.

32. Définition 1.31. Oui, c'est un bête morphisme d'anneaux. Il n'y a pas plus de structure dans un corps que dans un anneau.

33. Vérifiez-le tout de même.

de $\mathbb{R}$.

Mais cette fois nous définissons la multiplication suivante :

$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + 3bd + (ad + bc)\sqrt{2}. \quad (6.130)$$

Cela est un corps parce que tout élément non nul est inversible. En effet, l'équation

$$(a + b\sqrt{2})(x + y\sqrt{2}) = 1 \quad (6.131)$$

donne

$$\begin{pmatrix} a & 3b \\ b & a \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \quad (6.132)$$

Ce système a une unique solution si et seulement si $\det \begin{pmatrix} a & 3b \\ b & a \end{pmatrix} = 0$. Cela survient si et seulement si

$$a^2 - 3b^2 = 0. \quad (6.133)$$

Les solutions de cela dans $\mathbb{R}$ sont $a = \pm\sqrt{3}|b|$. Dès que a ou b est non nul, cela ne peut pas satisfaire $a, b \in \mathbb{Q}$. Donc le déterminant est toujours non nul et il existe $x, y \in \mathbb{Q}$ tels que (6.131) soit satisfaite.

Tout cela nous a donné un corps $\mathbb{K}$ dont $\mathbb{Q}$ est un sous-corps et qui contient l'élément $\sqrt{2}$ de $\mathbb{R}$. Il n'est cependant pas un sous-corps de $\mathbb{R}$.

Ce corps est isomorphe à $\mathbb{Q}(\sqrt{3})_{\mathbb{R}}$. En effet, nous montrons que

$$\begin{aligned} \psi: \mathbb{K} &\rightarrow \mathbb{Q}(\sqrt{3})_{\mathbb{R}} \\ a + b\sqrt{2} &\mapsto q + b\sqrt{3} \end{aligned} \quad (6.134)$$

est un isomorphisme de corps. Pour le produit, nous avons

$$\psi((a + b\sqrt{2})(c + d\sqrt{2})) = \psi(qc + 3bd + (ad + bc)\sqrt{2}) \quad (6.135a)$$

$$= ac + 3bd + (ad + bc)\sqrt{3} \quad (6.135b)$$

$$= (a + b\sqrt{3})(c + d\sqrt{3}) \quad (6.135c)$$

$$= \psi(a + b\sqrt{2})\psi(c + d\sqrt{2}). \quad (6.135d)$$

Remarques :

- L'application ψ est bien définie grâce au lemme 6.80 couplé au théorème 3.35 appliqué à $n = 2$ et $n = 3$.
- Dans le membre de gauche de (6.135a), $b\sqrt{2}$ est un produit dans $\mathbb{R}$ (d'où l'importance du lemme 6.80 qui permet de re-séparer les éléments de $\mathbb{R}$ partie rationnelle et partie multiple de $\sqrt{2}$), et le produit entre $(a + b\sqrt{2})$ et $(c + d\sqrt{2})$ est un produit dans $\mathbb{K}$.
- Dans (6.135b) et (6.135c), tous les produits sont dans $\mathbb{R}$.

En comparant avec le lemme 6.82, nous avons alors

$$\mathbb{Q}(\sqrt{2})_{\mathbb{K}} = \mathbb{Q}(\sqrt{3})_{\mathbb{R}} \neq \mathbb{Q}(\sqrt{2})_{\mathbb{R}} \quad (6.136)$$

△

6.84.

Nous allons encore enfoncer le clou sur le fait que $\mathbb{K}(\alpha)_{\mathbb{L}}$ dépend de $\mathbb{L}$.

Le fait est que si on y pense, l'objet $\sqrt{2}$ n'a aucun rapport avec $\mathbb{Q}$. En effet les objets de $\mathbb{Q}$ sont des classes d'équivalence de couples d'éléments de $\mathbb{Z}$, alors que l'élément $\sqrt{2}$ est une classe d'équivalence de suites de Cauchy dans $\mathbb{Q}$.

Lorsque nous écrivons $\mathbb{Q}(\sqrt{2})$, nous associons des objets de nature complètement différentes, et il n'y a aucune raison à priori de définir la multiplication entre eux d'une façon plutôt qu'une autre.

Plus généralement, dans ZF (que nous faisons du semblant de suivre tout en sachant que nous ne savons pas ce que c'est réellement³⁴), tout est ensemble. Peut-on dire ce que serait $\mathbb{Q}(I)$ si I est un ensemble quelconque ? Attention : en écrivant $\mathbb{Q}(I)$, nous entendons un corps dont I est un élément, pas un corps qui contiendrait comme éléments tous les éléments de I .

Si I est juste un ensemble, quelle définition donner de I^2 ? Il y a plein de choix et rien ne se dégage clairement comme étant pertinent. Si par contre, en guise de I nous considérons l'ensemble $\sqrt{2}$ (oui, c'est un ensemble : un ensemble de suites de Cauchy dans $\mathbb{Q}$), alors tout de suite nous nous disons que la bonne façon de faire est $\sqrt{2^2} = 2$. Ce réflexe est juste conditionné par le fait que nous connaissons déjà par ailleurs le corps $\mathbb{R}$. Rien de plus.

Donc oui, $\mathbb{K}(\alpha)_{\mathbb{L}}$ dépend de $\mathbb{L}$, mais dans les cas particuliers où $\mathbb{K}$ est un sous-corps de $\mathbb{C}$, il y a un implicite comme quoi $\mathbb{L} = \mathbb{C}$. Cela étant dit, il n'y a plus d'ambiguïtés en écrivant $\mathbb{Q}(\sqrt{2})$.

Dans l'énoncé suivant, la notation $R(\alpha)_{\mathbb{L}}$ signifie que l'évaluation de R sur α se fait en calculant dans le sur-corps $\mathbb{L}$ de $\mathbb{K}$. Cette proposition semble indiquer que $\mathbb{K}(\alpha)$ est donné en termes de $\mathbb{K}(X)$, lequel est défini de façon très intrinsèque sans faire appel à un corps ambiant de $\mathbb{K}$.

Proposition 6.85 ([1]).

Soit une extension $\mathbb{L}$ du corps $\mathbb{K}$ et $\alpha \in \mathbb{L}$. Alors nous avons les isomorphismes de corps suivants :

- (1) $\mathbb{K}(\alpha)_{\mathbb{L}} = \text{Frac}(\mathbb{K}[\alpha]_{\mathbb{L}})$,
- (2) $\mathbb{K}(\alpha)_{\mathbb{L}} = \{R(\alpha)_{\mathbb{L}} \text{ tel que } R \in \mathbb{K}(X)\}$.

Démonstration. Le corps $\mathbb{K}(\alpha)$ est un sous-corps de $\mathbb{L}$ contenant $\mathbb{K}[\alpha]$ comme sous-anneau. La proposition 1.249 nous dit alors que l'application suivante est un morphisme injectif de corps :

$$\begin{aligned} \epsilon: \text{Frac}(\mathbb{K}[\alpha]) &\rightarrow \mathbb{K}(\alpha) \\ P/Q &\mapsto PQ^{-1}. \end{aligned} \quad (6.137)$$

Pour rappel, la notation P/Q est bien une notation pour la classe d'équivalence du couple (P, Q) pour la relation définie en 1.248.

Par ailleurs, la partie $\epsilon(\text{Frac}(\mathbb{K}[\alpha]))$ est incluse à $\mathbb{L}$ et est un corps contenant $\mathbb{K}$ et α . Donc le corps $\mathbb{L}$ fait partie des corps sur lesquels on prend l'intersection pour définir $\mathbb{K}(\alpha)$. Cela prouve que

$$\mathbb{K}(\alpha) \subset \epsilon(\text{Frac}(\mathbb{K}[\alpha])). \quad (6.138)$$

L'application ϵ est donc surjective sur $\mathbb{K}(\alpha)$. Vu qu'elle était déjà injective, elle est bijective.

Pour la seconde partie, veuillez lire la définition 1.251 de l'évaluation d'une fraction rationnelle sur un élément de l'anneau. Si $R = P/Q \in \mathbb{K}(X)$ et si $\alpha \in \mathbb{L}$, nous avons

$$R(\alpha) = P(\alpha)Q(\alpha)^{-1}. \quad (6.139)$$

Tout sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et α doit contenir en particulier $\{P(\alpha) \text{ tel que } P \in \mathbb{K}[X]\}$, les inverses $\{P(\alpha)^{-1} \text{ tel que } P \in \mathbb{K}[X], P(\alpha) \neq 0\}$ et les produits d'iceux. Donc tout sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et α contient $\{R(\alpha) \text{ tel que } R \in \mathbb{K}(X)\}$.

Nous avons donc

$$\{R(\alpha) \text{ tel que } R \in \mathbb{K}(X)\} \subset \mathbb{K}(\alpha). \quad (6.140)$$

Mais vu que $\mathbb{K}(\alpha)$ est lui-même un sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et α , il est contenu dans $\{R(\alpha) \text{ tel que } R \in \mathbb{K}(X)\}$. D'où l'égalité. $\square$

Pourquoi cela ne contredit pas l'exemple 6.83 ? Lorsque nous écrivons

$$\mathbb{K}(\alpha) = \{R(\alpha) \text{ tel que } R \in \mathbb{K}(X)\}, \quad (6.141)$$

certaines $\mathbb{K}(X)$ est défini sans faire appel à un corps contenant $\mathbb{K}$. Mais l'évaluation $R(\alpha)$, oui. Pour calculer $R(\alpha)$, il faut écrire $R = P/Q$ et calculer $P(\alpha)Q(\alpha)^{-1}$. Tous les calculs de cette dernière

34. En lisant quelques pages de Wikipédia, vous pourrez briller en société, mais ne tentez pas le coup à l'agrégation.

expression doivent se faire dans un sur-corps de $\mathbb{K}$. Il suffit que le sur-corps en question soit un monceau de mauvaise foi comme celui de l'exemple 6.83, et en réalité $\mathbb{K}(\alpha)$ peut ne pas être ce que l'on croit.

Le corolaire suivant montre que les choses s'arrangent.

Corolaire 6.86.

Soient un corps $\mathbb{K}$, une extension $\mathbb{L}_1$ de $\mathbb{K}$, un élément $\alpha \in \mathbb{L}_1$ et une extension $\mathbb{L}_2$ de $\mathbb{L}_1$. Alors

$$\mathbb{K}(\alpha)_{\mathbb{L}_1} = \mathbb{K}(\alpha)_{\mathbb{L}_2}. \quad (6.142)$$

Démonstration. La proposition 6.85 nous dit que

$$\mathbb{K}(\alpha)_{\mathbb{L}_1} = \{R(\alpha)_{\mathbb{L}_1} \text{ tel que } R \in \mathbb{K}(X)\} \quad (6.143a)$$

$$\mathbb{K}(\alpha)_{\mathbb{L}_2} = \{R(\alpha)_{\mathbb{L}_2} \text{ tel que } R \in \mathbb{K}(X)\}. \quad (6.143b)$$

Mais lorsque $R \in \mathbb{K}(X)$, le calcul de $R(\alpha)$ est exactement le même dans $\mathbb{L}_1$ et dans $\mathbb{L}_2$ parce que $\mathbb{L}_2$ est un sur-corps de $\mathbb{L}_1$ et que les calculs effectifs de $R(\alpha) = P(\alpha)Q(\alpha)^{-1}$ ne font intervenir que des quantités de $\mathbb{K}$ et des puissances de α . $\square$

Ce que ce corolaire nous dit est que si le contexte fixe une extension de $\mathbb{K}$, nous pouvons faire tous les calculs dans cette extension, même si il y a des piles d'extensions à côté.

Typiquement, à chaque fois que nous considérons des sous-corps de $\mathbb{C}$, les extensions se feront dans $\mathbb{C}$: pour tout $\alpha \in \mathbb{C}$, les corps $\mathbb{Q}(\alpha)$, $\mathbb{R}(\alpha)$ se calculent dans $\mathbb{C}$.

Proposition 6.87.

Soit un corps $\mathbb{K}$, une extension $\mathbb{L}$ et un élément $\alpha \in \mathbb{L}$. Nous considérons l'application

$$\begin{aligned} \varphi: \mathbb{K}[X] &\rightarrow \mathbb{L} \\ P &\mapsto P(\alpha). \end{aligned} \quad (6.144)$$

- (1) Si α est transcendant, alors $\mathbb{K}[\alpha] = \mathbb{K}[X]$ (isomorphisme d'anneaux).
- (2) Si α est transcendant, alors $\mathbb{K}(\alpha)_{\mathbb{L}} = \mathbb{K}(X)$ (isomorphisme de corps),
- (3) Si α est algébrique, alors $\ker(\varphi)$ est un idéal possédant un unique générateur unitaire, lequel est le polynôme minimal³⁵ de α sur $\mathbb{K}$.

Démonstration. Point par point.

- (1) Nous savons que $\mathbb{K}[\alpha] = \{Q(\alpha) \text{ tel que } Q \in \mathbb{K}[X]\}$ (c'est la proposition 3.120). Donc φ est surjective sur $\mathbb{K}[\alpha]$, et est donc bijective. Elle est un isomorphisme³⁶ parce que le lemme 6.65 dit déjà que c'est un morphisme.
- (2) Nous supposons encore que α est transcendant et nous considérons l'application

$$\begin{aligned} \psi: \mathbb{K}(X) &\rightarrow \mathbb{K}(\alpha) \\ P &\mapsto R(\alpha). \end{aligned} \quad (6.145)$$

Note : cette application n'est pas φ . En effet φ n'est définie que sur $\mathbb{K}[X]$; le corps des fractions $\mathbb{K}(X)$ est nettement plus grand (classes d'équivalence de couples).

Le fait que cette application soit surjective est la proposition 6.85(2). Pour l'injectivité nous supposons que $\psi(R) = 0$, c'est-à-dire que $R(\alpha) = 0$. Nous considérons un représentant (P, Q) de R ; c'est-à-dire $R = P/Q$. L'égalité $R(\alpha) = 0$ signifie $P(\alpha)Q(\alpha)^{-1} = 0$ (égalité dans $\mathbb{L}$). Vu que $\mathbb{L}$ est un corps, c'est un anneau intègre et nous avons la règle du produit nul; soit $P(\alpha) = 0$, soit $Q(\alpha)^{-1} = 0$. La seconde possibilité est impossible parce que zéro n'est pas inversible. Donc $P(\alpha) = 0$. Donc $\varphi(P) = 0$ et φ étant injective, $P = 0$.

Lorsque $P = 0$, la classe P/Q est nulle dans $\mathbb{K}(X) = \text{Frac}(\mathbb{K}[X])$.

35. Définition 6.59.

36. Les amateurs d'écriture inclusive ne seront, je l'espère, pas choqué par « elle est un isomorphisme »; c'est une tournure que je propose ici sur le modèle de l'immonde « elle est un ministre » ou, à peine moins grave, « il est une sommité ».

(3) C'est le lemme-définition 6.59.

□

Proposition 6.88.

Soit un corps $\mathbb{K}$ et une extension $\mathbb{L}$. Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{L}$, une racine de P . Alors le polynôme minimal d'une racine divise³⁷ tout polynôme annulateur.

Autrement dit, l'idéal engendré par le polynôme minimal est l'idéal des polynômes annulateurs.

Démonstration. Nous considérons l'idéal

$$I = \{Q \in \mathbb{K}[X] \text{ tel que } Q(a) = 0\}. \quad (6.146)$$

Le fait que cela soit un idéal est simplement dû à la définition du produit : $(PQ)(a) = P(a)Q(a)$. Par le théorème 6.39, le polynôme minimal μ_a de a est dans I et qui plus est le génère : $I = (\mu_a)$. Par conséquent tout polynôme annulateur de a est divisé par μ_a . □

6.4.4.1 Extension algébrique, degré

Proposition 6.89.

Toute extension finie est algébrique.

Démonstration. Soient un corps $\mathbb{K}$, une extension $\mathbb{L}$ de degré³⁸ n de $\mathbb{K}$ et $a \in \mathbb{L}$. Nous devons montrer qu'il existe un polynôme annulateur de a à coefficients dans $\mathbb{K}$.

Soit la partie $S = \{1, a, a^2, \dots, a^n\}$ de $\mathbb{L}$. Si cette partie contient des éléments non distincts, alors c'est plié. En effet, si $a^k = a^l$, alors le polynôme X^{k-l} est un polynôme annulateur de a .

Nous supposons donc que S contienne exactement $n + 1$ éléments distincts. Le lemme 4.9 nous assure que S est une partie liée : il existe des éléments $k_i \in \mathbb{K}$ tels que $\sum_{i=0}^n k_i a^i = 0$.

Donc le polynôme $\sum_i a_i X^i$ est un polynôme annulateur de a . □

Proposition 6.90 (Propriétés d'extensions algébriques[1]).

Soit $\mathbb{K}$ un corps commutatif³⁹ et a un élément algébrique⁴⁰ sur $\mathbb{K}$, de polynôme minimal μ_a de degré n . Alors

(1) En considérant l'application d'évaluation

$$\begin{aligned} \varphi_a: \mathbb{K}[X] &\rightarrow \mathbb{L} \\ Q &\mapsto Q(a), \end{aligned} \quad (6.147)$$

nous avons $\mathbb{K}[a] = \text{Image}(\varphi_a)$.

(2) Une base de $\mathbb{K}[a]$ comme espace vectoriel sur $\mathbb{K}$ est donnée par $\{1, a, a^2, \dots, a^{n-1}\}$.

(3) Le degré de l'extension $\mathbb{K}[a]$ est égal au degré du polynôme minimal :

$$[\mathbb{K}[a] : \mathbb{K}] = n. \quad (6.148)$$

(4) L'anneau $\mathbb{K}[a]$ est l'ensemble des polynômes en a de degré $n - 1$ à coefficient dans $\mathbb{K}$.

(5) $\mathbb{K}(a) = \mathbb{K}[a]$.

(6) Il existe un isomorphisme d'anneaux $\varphi: \mathbb{K}[a] \rightarrow \mathbb{K}[X]/(\mu_a)$ tel que $\varphi(k) = \bar{k}$ pour tout $k \in \mathbb{K}$. $\mathbb{K}[a] \simeq \mathbb{K}[X]/(\mu_a)$ (isomorphisme d'anneau).

L'intérêt de (6) est qu'il permet de caractériser $\mathbb{K}[a]$ sans avoir recours à un sur-corps de $\mathbb{K}$. Le point (3) indique que le degré d'une extension algébrique est égal au degré du polynôme minimal.

37. Définition 3.125.

38. Définition 6.56.

39. Juste en passant nous rappelons que tous les corps considérés ici sont commutatifs

40. Définition 6.65.

Démonstration. (1) Nous avons $\mathbb{K}[a] \subset \text{Image}(\varphi_a)$ parce que $\text{Image}(\varphi_a)$ est lui-même un sous-anneau de $\mathbb{L}$ contenant $\mathbb{K}$ et a . Pour rappel, $\mathbb{K}[a]$ est l'intersection de tous les tels sous-anneaux.

L'inclusion inverse est le fait que si $Q \in \mathbb{K}[X]$ alors $Q(a) \in \mathbb{K}[a]$ parce que $\mathbb{K}[a]$ est un anneau et contient donc tous les a^n .

- (2) La partie $\{1, a, a^2, \dots, a^{n-1}\}$ est libre parce qu'une combinaison linéaire de ces éléments est un polynôme de degré $n-1$ en a . Un tel polynôme ne peut pas être nul parce que nous avons mis comme hypothèse que le polynôme minimal de a est n .

Rappelons qu'en vertu de la définition 6.59, le polynôme minimal μ_a est unitaire ; donc le polynôme $\mu_a(X) - X^n$ est un polynôme de degré $n-1$. Par conséquent en posant $S(X) = X^n - \mu_a(X)$, le polynôme S est de degré $n-1$ et vérifie $a^n = S(a)$.

En vertu du point (1), un élément de $\mathbb{K}[a]$ s'écrit $Q(a)$ pour un certain $Q \in \mathbb{K}[X]$. Supposons que Q soit de degré $p > n-1$; alors nous le décomposons en une partie contenant les termes de degré jusqu'à $n-1$ et une partie contenant les autres :

$$Q(X) = Q_1(X) + X^n Q_2(X) \quad (6.149)$$

où Q_1 est de degré $n-1$ et Q_2 de degré $p-n$. Nous évaluons cette égalité en a :

$$Q(a) = Q_1(a) + S(a)Q_2(a). \quad (6.150)$$

Donc $Q(a)$ est l'image de a par le polynôme $Q_1 + SQ_2$ qui est de degré $p-1$. Par récurrence, $Q(a)$ est l'image de a par un polynôme de degré $n-1$.

Notons que l'idée est très simple : il s'agit de remplacer récursivement tous les a^n par $S(a)$.

- (3) Conséquence immédiate de (2).
 (4) Conséquence immédiate de (2).
 (5) Un élément général non nul de $\mathbb{K}[a]$ est de la forme $Q(a)$ avec $Q \in \mathbb{K}[X]$; il s'agit de lui trouver un inverse. Pour cela nous remarquons que les polynômes $\mu_a(X)$ et $Q(x)$ sont premiers entre eux, sinon μ_a ne serait pas un polynôme minimal (voir la proposition 6.62). Donc le théorème de Bézout 6.43 affirme l'existence d'éléments $U, V \in \mathbb{K}[X]$ tels que

$$U\mu_a + VQ = 1 \quad (6.151)$$

dans $\mathbb{K}[X]$. Nous évaluons cette égalité en a en tenant compte de $\mu_a(a) = 0$ dans $\mathbb{K}[a]$:

$$U(a)\mu_a(a) + V(a)Q(a) = 1 \quad (6.152)$$

dans $\mathbb{K}[a]$. Par conséquent $V(a)Q(a) = 1$, ce qui signifie que $V(a)$ est l'inverse de $Q(a)$.

- (6) Nous considérons l'application

$$\begin{aligned} \psi: \mathbb{K}[X]/(\mu_a) &\rightarrow \mathbb{K}[a] \\ \bar{R} &\mapsto R(a) \end{aligned} \quad (6.153)$$

et nous montrons qu'elle convient. Pour cela, nous nous souvenons que la proposition 6.88 nous enseigne que (μ_a) , l'idéal engendré par μ_a , est égal à l'idéal des polynômes annulateurs de a dans $\mathbb{K}[X]$. Le polynôme μ_a divise tous les éléments de cet idéal ; voir aussi la définition 3.42 de l'idéal (μ_a) . Cela étant mis au point, nous passons à la preuve.

ψ est bien définie Si $\bar{R} = \bar{S}$ alors $R = S + Q$ avec $Q \in (\mu_a)$, et par conséquent $R(a) = S(a) + Q(a)$ avec $Q(a) = 0$.

Surjective Nous savons que $\mathbb{K}[a] = \text{Image}(\varphi_a)$. Si $x \in \mathbb{K}[a]$ alors il existe $Q \in \mathbb{K}[X]$ tel que $x = Q(a)$. Dans ce cas nous avons aussi $x = \psi(\bar{Q})$.

Injective Si $\psi(\bar{R}) = 0$ alors $R(a) = 0$, mais comme mentionné plus haut, μ_a engendre l'idéal des polynômes annulateurs de a . Donc $R \in (\mu_a)$ et nous avons $\bar{R} = 0$ dans $\mathbb{K}[X]/(\mu_a)$.

□

Exemple 6.91.

Un fait connu est que $\frac{1}{\sqrt{2}} = \frac{\sqrt{2}}{2}$. Donc l'inverse de $\sqrt{2}$ s'exprime bien comme un polynôme en $\sqrt{2}$ à coefficients dans $\mathbb{Q}$, ce qui confirme le point (5) de la proposition 6.90. Du point de vue de Bézout, $\mu_{\sqrt{2}}(X) = X^2 - 2$, et nous cherchons des polynômes U et V tels que

$$U(X^2 - 2) + VX = 1. \quad (6.154)$$

cette égalité est réalisée par $U = -\frac{1}{2}$ et $V = \frac{1}{2}X$. Et effectivement $V(\sqrt{2})$ est bien l'inverse de $\sqrt{2}$:

$$V(\sqrt{2}) = \frac{1}{2}\sqrt{2}. \quad (6.155)$$

△

Proposition 6.92 ([135]).

Soient un corps $\mathbb{K}$, une extension $\mathbb{L}$ de $\mathbb{K}$ et un élément α de $\mathbb{L}$. Il y a équivalence entre les trois points suivants :

- (1) α est algébrique sur $\mathbb{K}$,
- (2) $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$,
- (3) $\mathbb{K}[\alpha]$ est un $\mathbb{K}$ -espace vectoriel de dimension finie.

Si ces affirmations sont vraies, alors $[\mathbb{K}(\alpha) : \mathbb{K}]$ est le degré du polynôme minimal de α sur $\mathbb{K}$.

Démonstration. Démonstration décomposée en plusieurs implications.

(1) implique (2) Soit α algébrique sur $\mathbb{K}$. Nous considérons le polynôme minimal de α sur $\mathbb{K}$ (définition 6.59). Nous savons par le lemme 6.76 (qui fonctionne parce que α est algébrique) que $\mathbb{K}[\alpha] = \mathbb{K}[X]/(\mu)$ en tant qu'anneaux.

Mais $\mathbb{K}[X]$ est un anneau principal et μ en est un élément irréductible. Donc la proposition 3.78 dit que (μ) est un idéal maximum ; la proposition 3.80 avance encore un peu en disant que $\mathbb{K}[X]/(\mu)$ est un corps.

Donc $\mathbb{K}[X]/(\mu)$ est un corps isomorphe à $\mathbb{K}[\alpha]$ en tant qu'anneaux. En conséquence de quoi $\mathbb{K}[\alpha]$ est un corps.

Le corps $\mathbb{K}[\alpha]$ est un sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et α ; par définition nous avons donc $\mathbb{K}(\alpha) \subset \mathbb{K}[\alpha]$. Mais d'autre part, $\mathbb{K}[\alpha]$ est contenu dans tout sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et α , donc il est inclus dans l'intersection de tout ces corps, donc $\mathbb{K}[\alpha] \subset \mathbb{K}(\alpha)$.

Les deux inclusions sont prouvées.

(2) implique (1) Nous montrons que non-(1) implique non-(2). Nous disons donc que α est transcendant sur $\mathbb{K}$; cela implique par la proposition 6.87(1) que $\mathbb{K}[\alpha] = \mathbb{K}[X]$ en tant qu'anneaux. Donc $\mathbb{K}[\alpha]$ n'est pas un corps parce que $\mathbb{K}[X]$ ne l'est pas.

N'étant pas un corps, $\mathbb{K}[\alpha]$ ne peut pas être égal à $\mathbb{K}(\alpha)$ qui, lui, est un corps.

(1) implique (3) L'élément α est maintenant algébrique et nous considérons son polynôme minimal μ . Nous savons par le lemme 6.76 que $\mathbb{K}[\alpha] = \mathbb{K}[X]/(\mu)$ en tant qu'espaces vectoriels. Or $\mathbb{K}[X]/(\mu)$ est de dimension finie $\deg(\mu)$. Donc $\mathbb{K}[\alpha]$ est également de dimension finie.

(3) implique (1) Nous démontrons la contraposée. En supposant que α est transcendant nous avons $\mathbb{K}[\alpha] = \mathbb{K}[X]$ par la proposition 6.87. Or $\mathbb{K}[X]$ n'est pas de dimension finie sur $\mathbb{K}$, donc $\mathbb{K}[\alpha]$ non plus.

□

Lemme 6.93 ([136]).

Soit $\mathbb{L}$ un corps commutatif et $(\mathbb{K}_i)_{i \in I}$ une famille de sous-corps de $\mathbb{L}$. Alors $\bigcup_{i \in I} \mathbb{K}_i$ est un sous-corps de $\mathbb{L}$.

Définition 6.94.

Soit une extension⁴¹ de corps $j: \mathbb{K} \rightarrow \mathbb{L}$. Soit $A \subset \mathbb{L}$.

- (1) Nous notons $\mathbb{K}(A)_{\mathbb{L}}$ le plus petit sous corps de $\mathbb{L}$ contenant $j(\mathbb{K})$ et A . C'est l'intersection de tous les sous-corps de $\mathbb{L}$ contenant A et $j(\mathbb{K})$.
- (2) Nous notons $\mathbb{K}[A]_{\mathbb{L}}$ le plus petit sous anneau de $\mathbb{L}$ contenant $j(\mathbb{K})$ et A . C'est l'intersection de tous les sous-anneaux de $\mathbb{L}$ contenant A et $j(\mathbb{K})$.

Le plus souvent, l'indice $\mathbb{L}$ dans $\mathbb{K}(A)_{\mathbb{L}}$ et $\mathbb{K}[A]_{\mathbb{L}}$ est omis parce que le contexte est clair⁴², et nous avons même très souvent $\mathbb{K} \subset \mathbb{L}$ en tant que ensembles. Dans ce cas, l'application j est l'identité et elle sera omise.

Nous disons que l'extension $\mathbb{L}$ de $\mathbb{K}$ est **monogène** ou **simple** s'il existe $\theta \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}(\theta)$. Un tel élément θ est dit **élément primitif** de $\mathbb{L}$. Il n'est pas nécessairement unique.

Remarque 6.95.

Les ensembles $\mathbb{K}(A)$ et $\mathbb{K}[A]$ sont aussi appelés respectivement corps **engendré** et anneau engendré par A . Cependant il faut bien remarquer que ce sont les parties de $\mathbb{L}$ engendrées par A . Il n'est pas question à priori de parler de corps engendré par A sans dire dans quel corps plus grand nous nous plaçons.

Exemple 6.96.

Nous savons que $\mathbb{R}$ est une extension de $\mathbb{Q}$. Si $a \in \mathbb{R}$ alors $\mathbb{Q}(a)$ est le plus petit corps contenant $\mathbb{Q}$ et a . $\triangle$

Exemple 6.97.

Nous avons déjà vu à l'occasion de la définition 1.240 que $A[X]$ est l'anneau de tous les polynômes de degré fini en X . Cela rentre dans le cadre de la définition 6.94 parce un anneau contenant X doit contenir tous les X^n .

Notons que même si $\mathbb{K}$ est un corps, $\mathbb{K}[X]$ reste un anneau parce qu'un éventuel inverse de X n'est pas dedans⁴³. Par contre, $\mathbb{K}(X)$ est un corps parce qu'il contient également les fractions rationnelles. $\triangle$

Exemple 6.98.

Si nous prenons $\mathbb{F}_5$ et que nous l'étendons par i , nous obtenons le corps $\mathbb{K} = \mathbb{F}_5(i)$. Nous savons que tous les éléments $a \in \mathbb{F}_5$ sont racines de $X^5 - X$. Mais étant donné que $i^5 = i$, nous avons aussi $x^5 = x$ pour tout $x \in \mathbb{F}_5(i)$. Pour le prouver, utiliser le morphisme de Frobenius. Le polynôme $X^5 - X$ est donc le polynôme nul dans $\mathbb{K}$.

Ceci est un cas très particulier parce que nous avons étendu $\mathbb{F}_p$ par un élément α tel que $\alpha^p = \alpha$. En général sur $\mathbb{F}_p(\alpha)$, le polynôme $X^p - X$ n'est pas identiquement nul, et possède donc au maximum p racines. Pour $x \in \mathbb{F}_p(\alpha)$, nous avons $x^p = x$ si et seulement si $x \in \mathbb{F}_p$. $\triangle$

Lemme 6.99.

Soit $P \in \mathbb{K}[X]$ un polynôme unitaire irréductible de degré n . Il existe une extension $\mathbb{L}$ de $\mathbb{K}$ et $a \in \mathbb{L}$ telle que $\mathbb{L} = \mathbb{K}(a)$ et P est le polynôme minimal de a dans $\mathbb{L}$.

Démonstration. Nous prenons $\mathbb{L} = \mathbb{K}[X]/(P)$ où (P) est l'idéal dans $\mathbb{K}[X]$ généré par P . Cela est un corps par le corolaire 6.40. Nous identifions $\mathbb{K}$ avec $\phi(\mathbb{K})$ où

$$\phi: \mathbb{K}[X] \rightarrow \mathbb{L} \tag{6.156}$$

est la projection canonique. Nous considérons également $a = \phi(X)$.

Nous avons alors $P(a) = 0$ dans $\mathbb{L}$. En effet $P(a) = P(\phi(X))$ est à voir comme l'application du polynôme P au polynôme X , le résultat étant encore un élément de $\mathbb{L}$. En l'occurrence le résultat est P qui vaut 0 dans $\mathbb{L}$.

41. Définition 6.54.

42. Et je me demande si il est possible de trouver un cas tordu où $\mathbb{K}(A)_{\mathbb{L}} \neq \mathbb{K}(A)_{\mathbb{M}}$. Par exemple lorsque A est dans $\mathbb{L}$ et $\mathbb{M}$, mais que $\mathbb{L}$ n'est pas inclus à $\mathbb{M}$, ni $\mathbb{M}$ dans $\mathbb{L}$.

43. Lorsqu'on multiplie, les degrés montent toujours.

Le polynôme P étant unitaire et irréductible, il est minimum dans $\mathbb{L}$.

Nous devons encore montrer que $\mathbb{L} = \mathbb{K}(a)$. Le fait que $\mathbb{K}(a) \subset \mathbb{L}$ est une tautologie parce qu'on calcule $\mathbb{K}(a)$ dans $\mathbb{L}$. Pour l'inclusion inverse soit $Q(X) = \sum_i Q_i X^i$ dans $\mathbb{K}[X]$. Dans $\mathbb{L}$ nous avons évidemment $Q = \sum_i Q_i a^i$. $\square$

Proposition 6.100 ([68]).

Soit $\mathbb{K}$, un corps et $P \in \mathbb{K}[X]$ un polynôme. Soient a et b , deux racines de P dans (éventuellement) une extension $\mathbb{L}$ de $\mathbb{K}$. Si μ_a et μ_b sont les polynômes minimaux de a et b (dans $\mathbb{K}[X]$) et si $\mu_a \neq \mu_b$, alors $\mu_a \mu_b$ divise P dans $\mathbb{K}[X]$.

Démonstration. Nous considérons les idéaux

$$I_a = \{Q \in \mathbb{K}[X] \text{ tel que } Q(a) = 0\}; \quad (6.157a)$$

$$I_b = \{Q \in \mathbb{K}[X] \text{ tel que } Q(b) = 0\}. \quad (6.157b)$$

Même si $Q(a)$ est calculé dans $\mathbb{L}$, ce sont des idéaux de $\mathbb{K}[X]$. Le polynôme μ_a est par définition le générateur unitaire de I_a , et vu que a est une racine de P , nous avons $P \in I_a$ et il existe un polynôme $Q \in \mathbb{K}[X]$ tel que

$$P = \mu_a Q. \quad (6.158)$$

Montrons que $\mu_a(b) \neq 0$. Pour cela, nous supposons que $\mu_a(b) = 0$, c'est-à-dire que $\mu_a \in I_b$. Il existe alors $R \in \mathbb{K}[X]$ tel que $\mu_a = \mu_b R$. Mais par la proposition 6.62, le polynôme μ_a est irréductible, donc soit μ_b soit R est inversible. Vu que les inversibles sont les éléments de $\mathbb{K}$ (polynômes de degré zéro), μ_b n'est pas inversible (sinon il serait constant et ne pourrait pas être annulateur de b). Donc R est inversible. Disons $R = k$.

Donc $\mu_a = k\mu_b$. Mais vu que μ_a et μ_b sont unitaires, nous avons obligatoirement $k = 1$. Cela donnerait $\mu_a = \mu_b$, ce qui est contraire aux hypothèses. Nous en déduisons que $\mu_a(b) \neq 0$.

Étant donné que $\mu_a(b) \neq 0$, l'évaluation de (6.158) en b montre que $Q(b) = 0$, de telle sorte que $Q \in I_b$ et il existe un polynôme S tel que $Q = \mu_b S$, c'est-à-dire tel que $P = \mu_a \mu_b S$, ce qui signifie que $\mu_a \mu_b$ divise P . $\square$

Exemple 6.101.

Soit $P = (X^2 + 1)(X^2 + 2)$ dans $\mathbb{R}[X]$. Dans $\mathbb{C}$ nous avons les racines $a = i$ et $b = \sqrt{2}i$ dont les polynômes minimaux sont $\mu_a = X^2 + 1$ et $\mu_b = X^2 + 2$. Nous avons effectivement $\mu_a \mu_b$ divise P dans $\mathbb{R}[X]$.

Si par contre nous considérons les racines $a = i$ et $b = -i$, nous aurions $\mu_a = \mu_b = X^2 + 1$, tandis que le polynôme μ_a^2 ne divise pas P . $\triangle$

6.4.5 Racines de polynômes

Corolaire 6.102 (Factorisation d'une racine).

Soit $P \in \mathbb{K}[X]$, un polynôme de degré n et $\alpha \in \mathbb{K}$ tel que $P(\alpha) = 0$. Alors il existe un polynôme Q de degré $n - 1$ tel que $P(x) = (X - \alpha)Q$.

Démonstration. Il s'agit d'un cas particulier de la proposition 6.88 : si $\alpha \in \mathbb{K}$ alors son polynôme minimal dans $\mathbb{K}$ est $X - \alpha$; donc $X - \alpha$ divise P . Il existe un polynôme Q tel que $P = (X - \alpha)Q$. Le degré est alors immédiat. $\square$

Avant de lire l'énoncé suivant, allez relire la définition 3.118 pour savoir ce qu'est un polynôme nul.

Théorème 6.103 (Polynôme qui a tellement de racines qu'il s'annule).

Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$ un polynôme de degré n possédant $n + 1$ racines distinctes $\alpha_1, \dots, \alpha_{n+1}$, alors $P = 0$.

Démonstration. Si P est de degré 1, il s'écrit $P = aX + b$; s'il a comme racines α et β , nous avons le système

$$\begin{cases} a\alpha + b = 0 & (6.159a) \\ a\beta + b = 0. & (6.159b) \end{cases}$$

La différence entre les deux donne $a(\alpha - \beta) = 0$. Vu que $\alpha \neq \beta$, la règle du produit nul (lemme 1.194) nous donne $a = 0$. Maintenant que $a = 0$, l'annulation de b est alors immédiate.

Nous faisons maintenant la récurrence en supposant le théorème vrai pour le degré n et en considérant un polynôme P de degré $n + 1$ possédant $n + 2$ racines distinctes. Vu que $P(\alpha_1) = 0$, le corolaire 6.102 nous donne un polynôme Q de degré n tel que

$$P = (X - \alpha_1)Q. \quad (6.160)$$

Étant donné que pour tout $i \neq 1$ nous avons $\alpha_i \neq \alpha_1$,

$$0 = P(\alpha_i) = \underbrace{(\alpha_i - \alpha_1)}_{\neq 0} Q(\alpha_i), \quad (6.161)$$

et la règle du produit nul donne $Q(\alpha_i) = 0$. Par conséquent le polynôme Q est de degré n et possède $n + 1$ racines distinctes; tous ses coefficients sont alors nuls par hypothèse de récurrence. Tous les coefficients du produit (6.160) sont alors également nuls. $\square$

Exemple 6.104.

Un polynôme à plusieurs variables peut s'annuler en une infinité de points sans être nul. Par exemple le polynôme $X^2 + Y^2 - 1 \in \mathbb{R}[X, Y]$ s'annule sur tout un cercle de $\mathbb{R}^2$ mais n'est pas nul, loin s'en faut.

Nous verrons dans la proposition 6.172 une condition pour qu'un polynôme à plusieurs variables s'annule du fait qu'il ait « trop » de racines. $\triangle$

Remarque 6.105.

L'intérêt du théorème 6.103 est que si l'on prouve qu'un polynôme s'annule sur un corps infini, alors il s'annulera sur n'importe quel autre corps. Nous aurons un exemple d'utilisation de cela dans le théorème de Cayley-Hamilton 13.24.

6.4.6 Corps de rupture

Définition 6.106.

Soit $P \in \mathbb{K}[X]$ un polynôme irréductible. Une extension $\mathbb{L}$ de $\mathbb{K}$ est un **corps de rupture** pour P s'il existe $a \in \mathbb{L}$ tel que $P(a) = 0$ et $\mathbb{L} = \mathbb{K}(a)$.

6.107.

Nous insistons sur le fait que nous ne définissons le concept de corps de rupture pour un polynôme irréductible à coefficients dans un corps. Les deux points sont importants : irréductible et à coefficient dans un corps.

Nous discuterons brièvement le pourquoi de cela dans la section 6.4.11.

Exemple 6.108.

Soit $\mathbb{K} = \mathbb{Q}$ et $P = X^2 - 2$. On pose $a = \sqrt{2}$ et $\mathbb{L} = \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$. De cette façon P est scindé dans $\mathbb{L}$:

$$P = (X - \sqrt{2})(X + \sqrt{2}). \quad (6.162)$$

Le corps $\mathbb{Q}(\sqrt{2})$ est donc un corps de rupture pour P . $\triangle$

Exemple 6.109.

Dans l'exemple 6.108, nous avons un corps de rupture dans lequel le polynôme P était scindé. Il n'en est pas toujours ainsi. Prenons

$$P = X^3 - 2 \quad (6.163)$$

et $a = \sqrt[3]{2}$. Nous avons, certes, $P(a) = 0$ dans $\mathbb{Q}(\sqrt[3]{2})$, mais P n'est pas scindé parce qu'il y a deux racines complexes. $\triangle$

Exemple 6.110.

Nous considérons le corps $\mathbb{Z}/p\mathbb{Z}$ où p est un nombre premier. Si $s \in \mathbb{Z}/p\mathbb{Z}$ n'est pas un carré, alors le polynôme $P = X^2 + s$ est irréductible et un corps de rupture de P sur $\mathbb{Z}/p\mathbb{Z}$ est donné par $(\mathbb{Z}/p\mathbb{Z})[X]/(X^2 + s)$, c'est-à-dire l'ensemble des polynômes de degré 1 en $\sqrt{s}$. Le cardinal en est p^2 . $\triangle$

Vu que nous allons abondamment parler du quotient $\mathbb{K}[X]/(P)$, nous nous permettons un petit lemme.

Lemme 6.111.

Soit un corps $\mathbb{K}$ et $P \in \mathbb{K}[X]$ non constant. Alors $\mathbb{K}[X]/(P)$ est un corps si et seulement si P est irréductible.

Démonstration. Nous utilisons le trio d'enfer dont il est question dans le thème 49. D'abord $\mathbb{K}[X]$ est un anneau principal par le lemme 3.127. Donc $\mathbb{K}[X]/(P)$ sera un corps si et seulement si (P) est un idéal maximum (proposition 3.50), et cela sera le cas si et seulement si (P) est engendré par un polynôme irréductible (proposition 3.78).

Il ne nous reste qu'à montrer que (P) est engendré par un irréductible si et seulement si P est irréductible. Il y a un sens dans lequel c'est évident.

Soit un irréductible μ tel que $(P) = (\mu)$. En particulier $\mu \in (P)$, c'est-à-dire qu'il existe Q tel que $\mu = PQ$. Vu que μ est irréductible, soit P soit Q est inversible. Si P est inversible, c'est-à-dire constant, ce que nous avons exclu par hypothèse. Si par contre Q est inversible, alors $P = k\mu$ pour un certain $k \in \mathbb{K}$, ce qui montre que P est irréductible autant que μ . $\square$

Proposition 6.112 (Existence d'un corps de rupture).

Soit un corps $\mathbb{K}$ et un polynôme irréductible non constant P . Alors

- (1) Le corps $\mathbb{L} = \mathbb{K}[X]/(P)$ est un corps de rupture pour P .
- (2) L'élément $\bar{X}$ de $\mathbb{L}$ est une racine de P .
- (3) $\mathbb{L} = \mathbb{K}(\bar{X})_{\mathbb{L}}$

Démonstration. Commençons par nous convaincre que $\mathbb{K}[X]/(P)$ est une extension de $\mathbb{K}$ (définition 6.54). Le fait que ce soit un corps est le lemme 6.111. Le morphisme $j: \mathbb{K} \rightarrow \mathbb{K}[X]/(P)$ est simplement $k \mapsto \bar{k}$ où à droite, $\bar{k}$ voit k dans $\mathbb{K}[X]$ comme étant le polynôme constant. Notez qu'il est automatiquement injectif (lemme 1.196).

Il faut maintenant voir que $\mathbb{K}[X]/(P) = \mathbb{K}(\alpha)$ pour un certain $\alpha \in \mathbb{K}[X]/(P)$. Grâce à notre compréhension des notations acquise dans 1.14.2.2, nous savons que $X \in \mathbb{K}[X]$ et qu'il est donc parfaitement légitime de poser $\alpha = \bar{X}$ dans $\mathbb{K}[X]/(P)$. Il s'agit simplement de l'ensemble $\bar{X} = \{X + QP \text{ tel que } Q \in \mathbb{K}[X]\}$ où X est une notation pour la suite $(0, 1, 0, 0, \dots)$.

Bref, nous notons $\alpha = \bar{X}$ et nous démontrons que $P(\alpha) = 0$ et que $\mathbb{K}[X]/(P) = \mathbb{K}(\alpha)$ (isomorphisme de corps).

$P(\bar{X}) = 0$ C'est le moment de nous souvenir comment la notation des X fonctionne, et en particulier la pirouette autour de (1.370). D'abord la définition du produit sur $\mathbb{K}[X]/(P)$ est $\bar{P}\bar{Q} = \overline{PQ}$; en particulier si $P = \sum_k a_k X^k$, alors $P(\bar{X}) = \sum_k a_k \bar{X}^k = \sum_k a_k \bar{X}^k$, et

$$P(\bar{X}) = \overline{P(X)} = \bar{P} = 0. \quad (6.164)$$

L'égalité Nous montrons à présent que $\mathbb{K}(\bar{X})_{\mathbb{L}} = \mathbb{L}$. C'est-à-dire que $\mathbb{L}$ est bien engendrée par $\mathbb{K}$ et un seul élément. D'abord, $\mathbb{L} = \mathbb{K}[X]/(P)$ contient bien évidemment $\mathbb{K}$ et $\bar{X}$. Ensuite nous devons prouver que tout sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et $\bar{X}$ est en réalité $\mathbb{L}$ entier.

Soit $Q \in \mathbb{K}[X]$, et montrons que $\bar{Q}$ est dans tout sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et $\bar{X}$.

Par le lemme 3.116 nous avons $\bar{Q} = Q(\bar{X})$. Et si un corps contient $\mathbb{K}$ et $\bar{X}$, il doit contenir tous les polynômes en $\bar{X}$ à coefficients dans $\mathbb{K}$. Donc un tel corps doit contenir $Q(\bar{X})$ et donc $\bar{Q}$.

□

Exemple 6.113.

Soit le polynôme $P = X^2 + 1 \in \mathbb{Z}[X]$. Dans le quotient $\mathbb{Z}[X]/(P)$ nous avons $\bar{X}^2 + 1 = 0$ et donc $\bar{X}^2 = -1$. C'est-à-dire que $\mathbb{Z}[X]/(P)$ contient un élément dont le carré est -1 . Avouez que c'est bien ce à quoi nous nous attendions.

Notons que $-\bar{X}$ est également une racine de P dans $\mathbb{Z}[X]/(P)$.

En calculant dans les polynômes à coefficients dans $\mathbb{Z}(\bar{X})$ nous avons :

$$(X + \bar{X})(X - \bar{X}) = X^2 - \bar{X}^2 = X^2 + 1, \quad (6.165)$$

c'est-à-dire que P est bien factorisé, et que nous avons retrouvé la multiplication $x^2 + 1 = (x + i)(x - i)$. $\triangle$

6.114.

Il n'y a évidemment pas unicité d'un corps de rupture pour un polynôme donné. Une raison est qu'un polynôme peut accepter plusieurs racines complètement indépendantes. Le corps étendu par l'une ou l'autre racine donne deux corps de rupture différents. Par exemple dans $\mathbb{Q}[X]$, le polynôme

$$P = X^4 - X^2 - 2 \quad (6.166)$$

a pour racines (dans $\mathbb{C}$) les nombres $\sqrt{2}$ et i . Donc on a deux corps de rupture complètement différents : $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(i)$.

6.115.

La proposition suivante donne une unicité du corps de rupture dans le cas d'un polynôme irréductible. Et nous comprenons pourquoi : un polynôme irréductible n'a fondamentalement qu'une seule racine « indépendante ». Par exemple $X^2 - 2$ a pour racines $\pm\sqrt{2}$. Autre exemple, le polynôme $X^2 + 6X + 13$ a pour racines, dans $\mathbb{C}$, les nombres complexes conjugués $z = -3 + 2i$ et $\bar{z} = -3 - 2i$.

Proposition 6.116 ([130]).

Soient un corps $\mathbb{K}$ et un polynôme irréductible $P \in \mathbb{K}[X]$. Alors toute extension $\mathbb{L}$ contenant une racine α de P admet un unique morphisme de corps

$$\psi: \mathbb{K}[X]/(P) \rightarrow \mathbb{L} \quad (6.167)$$

tel que $\psi(\bar{X}) = \alpha$.

Dans un tel cas,

- (1) l'image de ψ est $\mathbb{K}(\alpha)_{\mathbb{L}}$,
- (2) si $\mathbb{L} = \mathbb{K}(\alpha)_{\mathbb{L}}$ alors ψ est un isomorphisme.

Démonstration. L'idéal annulateur de α parmi les polynôme de $\mathbb{K}[X]$ n'est pas réduit à $\{0\}$ parce qu'il contient P . Le lemme 6.59 s'applique donc et nous avons le polynôme minimal μ de α dans $\mathbb{K}[X]$. Il divise P qui est irréductible, donc

$$P = \lambda\mu \quad (6.168)$$

pour un certain $\lambda \in \mathbb{K}$.

Nous posons

$$\begin{aligned} \psi: \mathbb{K}[X]/(P) &\rightarrow \mathbb{L} \\ \bar{Q} &\mapsto Q(\alpha). \end{aligned} \quad (6.169)$$

Bien définie Si $\bar{Q}_1 = \bar{Q}_2$ alors il existe un $R \in \mathbb{K}[X]$ tel que $Q_1 = Q_2 + RP$. Mais alors $\psi(\bar{Q}_1) = Q_1(\alpha) = Q_2(\alpha) + R(\alpha)P(\alpha) = Q_2(\alpha)$.

Injective Si $\psi(\bar{Q}_1) = \psi(\bar{Q}_2)$ alors $Q_1 - Q_2 = R$ pour un certain $R \in \mathbb{K}[X]$ vérifiant $R(\alpha) = 0$.

Nous avons alors un polynôme S tel que $R = S\mu = \lambda^{-1}SP$. Donc $\bar{R} = 0$ et donc $\bar{Q}_1 = \bar{Q}_2$.

Morphisme Laissé comme exercice ; la paresse de l'auteur de ces lignes attend vos contributions.

La condition Le morphisme ψ respecte de plus la condition

$$\psi(\bar{X}) = X(\alpha) = \alpha. \quad (6.170)$$

En ce qui concerne l'unicité, fixer $\psi(\bar{X})$ est suffisant pour fixer un morphisme. En effet si $\psi(\bar{X}) = \alpha$, alors

$$\psi(\bar{Q}) = \psi\left(\sum_k a_k \bar{X}^k\right) = \sum_k a_k \psi(\bar{X})^k = \sum_k a_k \alpha^k. \quad (6.171)$$

Pour le second point de l'énoncé, il faut remarquer que α est algébrique et non transcendant. Donc en utilisant les propositions 3.120 et 6.90(5) nous trouvons

$$\text{Image}(\psi) = \{Q(\alpha) \text{ tel que } Q \in \mathbb{K}[X]\} = \mathbb{K}[\alpha] = \mathbb{K}(\alpha). \quad (6.172)$$

Et finalement pour le dernier point, un morphisme de corps est toujours injectif. Si il est également surjectif, il sera bijectif. $\square$

6.4.7 Pile d'extensions

Lemme 6.117 ([1]).

Soient un corps $\mathbb{K}$, des extensions $\mathbb{L}_1, \dots, \mathbb{L}_n$ et des éléments $\alpha_i \in \mathbb{L}_i$ tels que

$$\mathbb{L}_1 = \mathbb{K}(\alpha_1)_{\mathbb{L}_1} \quad (6.173)$$

et

$$\mathbb{L}_k = \mathbb{L}_{k-1}(\alpha_k)_{\mathbb{L}_k}. \quad (6.174)$$

Alors

$$\mathbb{L}_n = \mathbb{K}(\alpha_1, \dots, \alpha_n)_{\mathbb{L}_n}. \quad (6.175)$$

Démonstration. Nous démontrons par récurrence sur n . Le cas $n = 1$ est simplement l'hypothèse (6.173).

Supposons donc que le lemme soit correct pour n , et étudions le cas $n + 1$. Nous avons, par définition et par hypothèse de récurrence :

$$\mathbb{L}_{n+1} = \mathbb{L}_n(\alpha_{n+1})_{\mathbb{L}_{n+1}} = \left(\mathbb{K}(\alpha_1, \dots, \alpha_n)_{\mathbb{L}_n}\right)(\alpha_{n+1})_{\mathbb{L}_{n+1}}. \quad (6.176)$$

Notre tâche sera donc de montrer que

$$\left(\mathbb{K}(\alpha_1, \dots, \alpha_n)_{\mathbb{L}_n}\right)(\alpha_{n+1}) = \mathbb{K}(\alpha_1, \dots, \alpha_{n+1}) \quad (6.177)$$

où nous n'écrivons plus les indices $\mathbb{L}_{n+1}$ partout.

Le membre de gauche est un sous-corps de $\mathbb{L}_{n+1}$ contenant à la fois $\mathbb{K}$ et tous les α_i , si bien que

$$\mathbb{K}(\alpha_1, \dots, \alpha_{n+1}) \subset \left(\mathbb{K}(\alpha_1, \dots, \alpha_n)_{\mathbb{L}_n}\right)(\alpha_{n+1})_{\mathbb{L}_{n+1}}. \quad (6.178)$$

Il faut donc prouver l'inclusion inverse ; c'est-à-dire montrer que tout élément x du corps $\left(\mathbb{K}(\alpha_1, \dots, \alpha_n)_{\mathbb{L}_n}\right)(\alpha_{n+1})$ est forcément dans tout sous-corps de $\mathbb{L}_{n+1}$ contenant $\mathbb{K}$ et les α_i . Un tel élément x est, par la proposition 6.85(2), de la forme $r(\alpha_{n+1})$ avec $r \in \mathbb{K}(\alpha_1, \dots, \alpha_n)(X)$, c'est-à-dire

$$P(\alpha_{n+1})Q(\alpha_{n+1})^{-1} \quad (6.179)$$

avec $P, Q \in \mathbb{K}(\alpha_1, \dots, \alpha_n)[X]$.

Prouvons d'abord que si $P \in \mathbb{K}(\alpha_1, \dots, \alpha_n)[X]$, alors $P(\alpha_{n+1})$ est dans tout sous-corps de $\mathbb{L}_{n+1}$ contenant $\mathbb{K}$ et les α_i . Nous pouvons écrire $P = \sum_i a_i X^i$ avec $a_i \in \mathbb{K}(\alpha_1, \dots, \alpha_n)$, et donc

$$P(\alpha_{n+1}) = \sum_i a_i \alpha_{n+1}^i. \quad (6.180)$$

Tout corps contenant $\mathbb{K}$ et les $\alpha_1, \dots, \alpha_n$ contient les a_i . Par produit, tout corps contenant $\mathbb{K}$, $\alpha_1, \dots, \alpha_{n+1}$ contient les termes $a_i \alpha_{n+1}^i$, et donc $P(\alpha_{n+1})$ par somme.

De la même façon, si un corps contient $\mathbb{K}$ et les α_i ($i = 1, \dots, n+1$), alors il contient $Q(\alpha_{n+1})$. Comme c'est un corps, il contient aussi son inverse $Q(\alpha_{n+1})^{-1}$, et il contient aussi le produit

$$r(\alpha_{n+1}) = P(\alpha_{n+1})Q(\alpha_{n+1})^{-1}. \quad (6.181)$$

On vient ainsi de montrer que tout élément $x \in (\mathbb{K}(\alpha_1, \dots, \alpha_n)_{\mathbb{L}_n})(\alpha_{n+1})$ était dans tout sous-corps de $\mathbb{L}_{n+1}$ qui contient $\mathbb{K}$ et les α_i ($i = 1, \dots, n+1$); en d'autres termes :

$$(\mathbb{K}(\alpha_1, \dots, \alpha_n)_{\mathbb{L}_n})(\alpha_{n+1})_{\mathbb{L}_{n+1}} \subset \mathbb{K}(\alpha_1, \dots, \alpha_{n+1}). \quad (6.182)$$

Les inclusions (6.178) et (6.182) prouvent l'égalité d'ensembles (6.177) que nous voulions montrer. $\square$

6.4.8 Clôture algébrique

Le concept de clôture algébrique a été défini dans 6.69. Voici un lemme qui dit qu'une clôture algébrique est en quelque sorte une extension algébrique maximale.

Lemme 6.118 ([1]).

Soient un corps $\mathbb{K}$ et une extension algébrique $\mathbb{F}$ de $\mathbb{K}$. Nous supposons que pour toute extension algébrique de $\mathbb{L}$ nous avons $\mathbb{L} = \mathbb{F}$

Alors $\mathbb{F}$ est algébriquement clos⁴⁴.

Démonstration. Soit un polynôme $P \in \mathbb{K}[X]$. Nous voudrions prouver que P a des racines dans $\mathbb{F}$. Pour cela, nous voyons P comme un polynôme sur $\mathbb{F}[X]$ et, grâce à la proposition 6.112 nous considérons un corps de rupture $\mathbb{L}$ pour P . Vu que $\mathbb{L}$ est une extension de $\mathbb{F}$, nous avons $\mathbb{L} = \mathbb{F}$. Donc $\mathbb{F}$ contient des racines de P . $\square$

6.119.

Nous avons défini le concept d'extension algébrique en 6.69. Nous allons en construire un petit exemple très piéton.

D'abord la proposition 1.333 nous donne l'existence et l'unicité d'un réel $\sqrt{2}$ strictement positif dont le carré est 2. Ce réel est irrationnel par la proposition 1.278. Cela étant posé, nous y allons.

Proposition 6.120 ([137]).

Soit $\mathbb{L} = \{a + b\sqrt{2}\}_{a,b \in \mathbb{Q}}$.

- (1) C'est un sous-corps de $\mathbb{R}$.
- (2) Tout sous-corps de $\mathbb{R}$ contenant $\mathbb{Q}$ et $\sqrt{2}$ contient $\mathbb{L}$.

Démonstration. Nous devons d'abord prouver que $\mathbb{L}$ est un corps en vérifiant d'une part que c'est un anneau (définition 1.30) et d'autre part le fait que tous les éléments non nuls sont inversibles.

— La partie $\mathbb{L}$ de $\mathbb{R}$ est stable pour l'addition : dès que $a, b, a', b' \in \mathbb{Q}$,

$$(a + b\sqrt{2}) + (a' + b'\sqrt{2}) = (a + a') + (b + b')\sqrt{2} \in \mathbb{L}. \quad (6.183)$$

— Les neutres 0 et 1 sont dans $\mathbb{L}$.

— Si $\alpha \in \mathbb{L}$, alors $-\alpha \in \mathbb{L}$:

$$-(a + b\sqrt{2}) = -a - b\sqrt{2}. \quad (6.184)$$

— La partie $\mathbb{L}$ est stable pour le produit parce que

$$(a + b\sqrt{2})(a' + b'\sqrt{2}) = (aa' + 2bb') + (ab' + ba')\sqrt{2}. \quad (6.185)$$

44. Définition 6.69(2).

- L'inverse d'un élément de $\mathbb{L}$ est dans $\mathbb{L}$. C'est le seul point pas tout à fait évident. D'abord, l'ensemble $\mathbb{R}$ est un corps par le théorème 1.286. Donc pour tout $a, b \in \mathbb{R}$, le nombre

$$\frac{1}{a + b\sqrt{2}} \quad (6.186)$$

existe dans $\mathbb{R}$.

D'abord $a - b\sqrt{2}$ n'est pas nul, parce que si il l'était, nous aurions $\sqrt{2} = -a/b \in \mathbb{Q}$ alors que $\sqrt{2}$ n'est pas rationnel par la proposition 1.278. Nous pouvons donc faire le coup de multiplier le numérateur et le dénominateur par le binôme conjugué :

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}. \quad (6.187)$$

Cela est un rationnel. Donc les éléments non nuls de $\mathbb{L}$ ont un inverse qui appartient également à $\mathbb{L}$.

Nous passons à la preuve du point (2). Si $\mathbb{L}'$ est un corps qui contient $\mathbb{Q}$ et $\sqrt{2}$, il doit contenir $b\sqrt{2}$ pour tout $b \in \mathbb{Q}$ et donc aussi tous les $a + b\sqrt{2}$ avec $a, b \in \mathbb{Q}$. En conséquence de quoi $\mathbb{L}'$ doit contenir au moins tout $\mathbb{L}$. $\square$

Proposition 6.121.

Soit $\mathbb{L} = \{a + b\sqrt{2}\}_{a,b \in \mathbb{Q}}$.

- (1) C'est un espace vectoriel de dimension 2 sur $\mathbb{Q}$.
- (2) Si $\alpha \in \mathbb{L}$, alors il existe un polynôme $P \in \mathbb{L}[X]$ de degré 2 ou moins tel que $P(\alpha) = 0$.
- (3) Le corps $\mathbb{L}$ est une extension algébrique de $\mathbb{Q}$.

Démonstration. En plusieurs parties.

- (1) Pour la dimension, notez que $\{1, \sqrt{2}\}$ est une partie libre et génératrice de $\mathbb{L}$.
- (2) Soit $\alpha \in \mathbb{L}$. La partie $\{1, \alpha, \alpha^2\}$ est de cardinal 1, 2 ou 3. Si c'est 1 ou 2, c'est que $1 = \alpha$ ou $1 = \alpha^2$ ou $\alpha = \alpha^2$. Si par exemple $1 = \alpha$ alors avec $P = X - 1$ nous avons $P(\alpha) = 0$. Si au contraire $\{1, \alpha, \alpha^2\}$ est de cardinal 3, alors c'est une partie liée par la proposition 4.6. Il existe donc des rationnels a, b, c tels que $a + b\alpha + c\alpha^2 = 0$, c'est-à-dire $P(\alpha) = 0$ avec $P = cX^2 + bX + a$.
- (3) Nous venons de voir que tous les éléments de $\mathbb{L}$ sont des racines de polynômes de $\mathbb{Q}[X]$. $\square$

Lemme 6.122.

Si $\mathbb{K}$ est un corps infini, alors $\mathbb{K}[X]$ est équipotent⁴⁵ à $\mathbb{K}$.

Démonstration. Notons provisoirement $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré n . Nous avons une surjection

$$\begin{aligned} \varphi: \mathbb{K}^{n+1} &\rightarrow \mathbb{K}_n[X] \\ (k_0, \dots, k_n) &\mapsto \sum_{i=0}^n k_i X^i. \end{aligned} \quad (6.188)$$

Par récurrence sur le théorème⁴⁶ 1.137, nous avons $\mathbb{K}^{n+1} \approx \mathbb{K}$. La surjection (6.188) dit alors que

$$\mathbb{K}_n[X] \leq \mathbb{K}^{n+1} \approx \mathbb{K}. \quad (6.189)$$

Mais vu qu'il y a une surjection $\mathbb{K} \rightarrow \mathbb{K}_n[X]$, nous avons aussi $\mathbb{K}_n[X] \geq \mathbb{K}$. Le théorème 1.121 dit alors que $\mathbb{K}_n[X] \approx \mathbb{K}$.

45. Définition 1.93.

46. J'ai quand même du mal à croire qu'il faut vraiment le lemme de Zorn pour prouver que $\mathbb{K}[X]$ est équipotent à $\mathbb{K}$. Si vous connaissez un moyen plus direct, écrivez-moi.

Le lemme 1.138 nous permet alors de conclure que

$$\mathbb{K}[X] = \bigcup_{n=0}^{\infty} \mathbb{K}_n[X] \approx \mathbb{K}. \quad (6.190)$$

□

Proposition 6.123 ([1]).

Soit un corps $\mathbb{K}$. Une extension algébrique de $\mathbb{K}$ est

- (1) au plus dénombrable si $\mathbb{K}$ est fini,
- (2) équipotente à $\mathbb{K}$ si $\mathbb{K}$ est infini.

Démonstration. En deux parties.

Si $\mathbb{K}$ est fini Un polynôme non nul possède toujours au maximum un nombre fini de racines (éventuellement zéro) par la proposition 6.103. Par ailleurs, chaque degré de polynôme ayant seulement un nombre fini de possibilités, l'ensemble $\mathbb{K}[X]$ est au plus dénombrable (proposition 1.114).

Pour $P \in \mathbb{K}[X]$ nous avons une surjection de $\mathbb{N}$ vers l'ensemble des racines de P . Nous la notons $\varphi_P: \mathbb{N} \rightarrow \mathbb{L}$, en posant par exemple $\varphi_P(n) = 1$ si P n'a pas de racines. Enfin nous posons

$$\begin{aligned} \varphi: \mathbb{K}[X] \times \mathbb{N} &\rightarrow \mathbb{L} \\ (P, n) &\mapsto \varphi_P(n). \end{aligned} \quad (6.191)$$

C'est la fonction qui à un polynôme P et un nombre n fait correspondre la n^{e} racine de P .

Vu que $\mathbb{L}$ est une extension algébrique, φ est surjective.

En termes de cardinalité, que $\mathbb{K}[X]$ soit fini ou dénombrable, dans les deux cas, $\mathbb{K}[X] \times \mathbb{N}$ est dénombrable (proposition 1.111). Il existe donc une surjection d'un ensemble dénombrable vers $\mathbb{L}$. Le lemme 1.113 conclut que $\mathbb{L}$ est fini ou dénombrable.

Si $\mathbb{K}$ est infini Nous procédons de la même manière, mais nous devons faire appel à des résultats plus technologiques pour maîtriser la cardinalité. Nous considérons à nouveau l'application

$$\begin{aligned} \varphi: \mathbb{K}[X] \times \mathbb{N} &\rightarrow \mathbb{L} \\ (P, n) &\mapsto \varphi_P(n). \end{aligned} \quad (6.192)$$

Cette application est encore surjective : $\mathbb{L} \leq \mathbb{K}[X] \times \mathbb{N}$. Le lemme 6.122 nous assure que $\mathbb{K}[X] \approx \mathbb{K}$ parce que $\mathbb{K}$ est infini. Ensuite la proposition 1.131 nous dit que $\mathbb{K}[X] \times \mathbb{N} \approx \mathbb{K}[X]$. Donc

$$\mathbb{K} \approx \mathbb{K}[X] \approx \mathbb{K}[X] \times \mathbb{N} \geq \mathbb{F}. \quad (6.193)$$

Mais $\mathbb{F}$ est une extension de $\mathbb{K}$. Donc il existe une injection $\mathbb{K} \rightarrow \mathbb{F}$, c'est à dire $\mathbb{K} \leq \mathbb{F}$.

Vu que $\mathbb{K} \leq \mathbb{F} \leq \mathbb{K}$, le théorème 1.121 implique que $\mathbb{K} \approx \mathbb{F}$.

□

Lemme 6.124 ([1]).

Soient des corps $\mathbb{K}$ et $\mathbb{L}$ ainsi qu'un homomorphisme de corps $\rho: \mathbb{K} \rightarrow \mathbb{L}$. Si $P \in \mathbb{K}[X]$ a une racine dans $\mathbb{K}$, alors le polynôme $\rho(P)$ a une racine dans $\mathbb{L}$.

Démonstration. Nous notons $P = \sum_k P_k X^k$. Si $a \in \mathbb{K}$ est une racine de P , alors $\sum_k P_k a^k = 0$. Nous appliquons ρ à cette égalité : $\sum_k \rho(P_k) \rho(a)^k = 0$, c'est à dire $\rho(P)(\rho(a)) = 0$. Donc $\rho(a) \in \mathbb{L}$ est une racine de $\rho(P)$. □

Lemme 6.125 ([138]).

Nous considérons un triple $(\mathbb{K}, \mathbb{L}, \mathbb{F})$ où

- (1) $\mathbb{K}$, $\mathbb{L}$ et $\mathbb{F}$ sont des corps
- (2) il existe $a \in \mathbb{L}$ algébrique sur $\mathbb{K}$ tel que $\mathbb{L} = \mathbb{K}(a)$ et un morphisme de corps $\alpha: \mathbb{K} \rightarrow \mathbb{L}$.

(3) $\mathbb{F}$ est une extension algébriquement close de $\mathbb{K}$: il existe un morphisme $\beta: \mathbb{K} \rightarrow \mathbb{F}$.

Alors il existe un morphisme de corps $\sigma: \mathbb{L} \rightarrow \mathbb{F}$ tel que $\sigma|_{\alpha(\mathbb{L})} = \beta$.

Note : en pratique, les corps $\mathbb{L}$ et $\mathbb{F}$ sont le plus souvent des sur-corps de $\mathbb{K}$, de telle sorte que les applications α et β sont l'identité. En particulier, la conclusion de ce lemme s'écrit le plus souvent $\sigma|_{\mathbb{K}} = \text{Id}$. Il faut juste savoir que le Frido est un névrosé des notations précises.

Démonstration. Vu que $\mathbb{L}$ est monogène, si $\mu_a \in \mathbb{K}[X]$ est le polynôme minimal de $a \in \mathbb{L}$, alors les points (5) et (6) de la proposition 6.90 disent que $\mathbb{L} \simeq \mathbb{K}[X]/(\mu_a)$.

Les coefficients de μ_a sont dans $\mathbb{K}$, donc nous pouvons voir $\mu_a \in \mathbb{F}[X]$. Plus précisément, si $\mu_a = \sum_k a_k X^k$, nous définissons

$$\mu'_a = \sum_k \beta(a_k) X^k \in \mathbb{F}[X]. \quad (6.194)$$

Comme $\mathbb{F}$ est algébriquement clos, le polynôme μ'_a possède une racine (au moins) $b \in \mathbb{F} : \mu'_a(b) = 0$.

Nous posons

$$\begin{aligned} \sigma': \mathbb{K}[X]/(\mu_a) &\rightarrow \mathbb{F} \\ \overline{\sum_k s_k X^k} &\mapsto \sum_k \beta(s_k) b^k. \end{aligned} \quad (6.195)$$

Montrons que cela est bien défini. Si $P = \sum_k s_k X^k$ et $\mu_a = \sum_k a_k X^k$ ($a_k, s_k \in \mathbb{K}$), alors

$$\sigma'(\overline{P + \mu_a}) = \sigma'(\overline{\sum_k (a_k + s_k) X^k}) = \sum_k \beta(a_k) b^k + \sum_k s_k b^k = \mu'_a(b) + \sigma'(\overline{P}) = \sigma'(\overline{P}). \quad (6.196)$$

L'application σ' est un morphisme de corps.

Si $\varphi: \mathbb{L} \rightarrow \mathbb{K}[X]/(\mu_a)$ est l'isomorphisme dont nous parlons plus haut, il vérifie $\varphi(\alpha(k)) = \bar{k}$ (la classe du polynôme de degré zéro). En posant $\sigma = \sigma' \circ \varphi$ nous avons, pour tout $k \in \mathbb{K}$,

$$(\sigma' \varphi \alpha)(k) = \sigma'(\bar{k}) = \beta(k), \quad (6.197)$$

c'est ce qu'il fallait. □

Lemme 6.126 ([138]).

Soit un corps $\mathbb{K}$ muni de deux extensions $\alpha: \mathbb{K} \rightarrow \mathbb{L}$ et $\beta: \mathbb{K} \rightarrow \mathbb{F}$ où $\mathbb{L}$ est algébrique sur $\mathbb{K}$ et $\mathbb{F}$ est algébriquement clos.

Alors il existe un morphisme de corps $\sigma: \mathbb{L} \rightarrow \mathbb{F}$ tel que $\sigma \circ \alpha = \beta$.

Démonstration. Nous allons utiliser le lemme de Zorn 1.17 sur l'ensemble

$$\mathcal{A} = \left\{ (\mathbb{M}, \varphi) \text{ tel que } \begin{cases} \mathbb{M} \text{ est un sous-corps de } \mathbb{L} \\ \alpha(\mathbb{K}) \subset \mathbb{M} \\ \varphi: \mathbb{M} \rightarrow \mathbb{F} \text{ est une extension de corps} \\ \varphi \circ \alpha = \beta \end{cases} \right\}. \quad (6.198)$$

Nous ordonnons (partiellement) cet ensemble en disant que $(\mathbb{M}_1, \varphi_1) < (\mathbb{M}_2, \varphi_2)$ si $\mathbb{M}_1 \subset \mathbb{M}_2$ et $\varphi_2|_{\mathbb{M}_1} = \varphi_1$. Il se fait que $\mathcal{A}$ est un ensemble inductif et que nous pouvons donc lui appliquer le lemme de Zorn.

Soit un élément maximum $(\mathbb{M}, \varphi)$. Nous allons montrer que $\mathbb{M} = \mathbb{L}$.

Soit $l \in \mathbb{L}$. Vu que $\mathbb{L}$ est une extension algébrique de $\mathbb{K}$, il existe un polynôme P à coefficients dans $\alpha(\mathbb{K})$ tel que $P(l) = 0$. Mais vu que $\alpha(\mathbb{K}) \subset \mathbb{M}$, ce polynôme est également à coefficients dans $\mathbb{M}$. Donc l est un élément algébrique sur $\mathbb{M}$.

Nous pouvons donc considérer le triple $(\mathbb{M}, \mathbb{M}(l), \mathbb{F})$ qui vérifie les hypothèses du lemme 6.125. Il existe donc un morphisme de corps $\sigma: \mathbb{M}(l) \rightarrow \mathbb{F}$ tel que $\sigma|_{\mathbb{M}} = \varphi$.

Nous avons

$$\sigma \circ \alpha = \sigma|_{\sigma(\mathbb{K})} \circ \alpha = \sigma|_{\mathbb{M}} \circ \alpha = \varphi \circ \alpha = \beta. \quad (6.199)$$

Donc l'élément $(\mathbb{M}(l), \sigma)$ majore $(\mathbb{M}, \varphi)$ dans $\mathcal{A}$.

Par maximalité, nous déduisons que $\mathbb{M} = \mathbb{L}$. Donc le morphisme $\varphi: \mathbb{L} \rightarrow \mathbb{F}$ vérifie $\varphi \circ \alpha = \beta$, ce qu'il nous fallait. $\square$

Théorème 6.127 (Steinitz[139, 140]).

À propos de clôture algébrique.

(1) Tout corps possède une clôture algébrique.

(2) Si $\alpha_1: \mathbb{K} \rightarrow \mathbb{F}_1$ et $\alpha_2: \mathbb{K} \rightarrow \mathbb{F}_2$ sont deux clôtures algébriques du même corps $\mathbb{K}$, alors il existe un isomorphisme de corps $\varphi: \mathbb{F}_1 \rightarrow \mathbb{F}_2$ tel que $\varphi \circ \alpha_1 = \alpha_2$.

Démonstration. Nous commençons par l'existence, en plusieurs points.

Un ensemble Nous considérons un ensemble Ω qui contient $\mathbb{K}$, qui est strictement surpotent⁴⁷ à $\mathbb{K}$ et qui est infini non dénombrable si $\mathbb{K}$ est fini. Par exemple $\mathcal{P}(\mathbb{K}) \cup \mathbb{K}$ si $\mathbb{K}$ est infini et $\mathbb{R} \cup \mathbb{K}$ si $\mathbb{K}$ est fini (voir le théorème de Cantor 1.124).

L'ensemble pour Zorn Nous considérons l'ensemble des extensions algébriques de $\mathbb{K}$ contenues dans Ω , c'est à dire

$$\mathcal{A} = \left\{ (\mathbb{L}, +_{\mathbb{L}}, \times_{\mathbb{L}}) \text{ tel que } \begin{cases} \mathbb{K} \subset \mathbb{L} \subset \Omega \\ (\mathbb{L}, +_{\mathbb{L}}, \times_{\mathbb{L}}) \text{ est une extension algébrique de } (\mathbb{K}, +, \times). \end{cases} \right\} \quad (6.200)$$

Nous ordonnons $\mathcal{A}$ par l'inclusion : nous disons que

$$(\mathbb{L}_1, +_1, \times_1) < (\mathbb{L}_2, +_2, \times_2) \quad (6.201)$$

lorsque $(\mathbb{L}_2, +_2, \times_2)$ est un sur-corps de $(\mathbb{L}_1, +_1, \times_1)$ (en particulier $\mathbb{L}_1 \subset \mathbb{L}_2$).

A est inductif Soit une partie $\mathcal{F} = \{(\mathbb{L}_i, +_i, \times_i)\}_{i \in I}$ de $\mathcal{A}$ que nous supposons être totalement ordonnées. Nous allons lui trouver un majorant dans $\mathcal{A}$. Nous posons $\mathbb{L} = \bigcup_{i \in I} \mathbb{L}_i$, et si $a \in \mathbb{L}_1$, $b \in \mathbb{L}_j$, alors nous définissons

$$\begin{cases} a +_{\mathbb{L}} b = a +_k b \\ a \times_{\mathbb{L}} b = a \times_k b \end{cases} \quad (6.202a)$$

$$\quad (6.202b)$$

où $k \in I$ est sélectionné de telle façon à avoir $(\mathbb{L}_i, +_i, \times_i) < (\mathbb{L}_k, +_k, \times_k)$ et $(\mathbb{L}_j, +_j, \times_j) < (\mathbb{L}_k, +_k, \times_k)$. Vu que tous les corps $\mathbb{L}_i$ sont des sous-corps les uns des autres, cela est une bonne définition.

Lemme de Zorn Nous utilisons le lemme de Zorn 1.17. Nous notons $(\mathbb{F}, +, \times)$ un élément maximal de $\mathcal{A}$. Vu que $\mathbb{K}$ en est un sous-corps, il n'y a pas d'ambiguïté de noter $+$ et $\times$ ses opérations.

Stratégie pour la suite Nous allons montrer que si $\mathbb{E}$ est une extension algébrique de $\mathbb{F}$, alors $\mathbb{E} = \mathbb{F}$ (le but est d'utiliser le lemme 6.118).

Un peu de cardinalité D'abord, vu que $\mathbb{F}$ est algébrique sur $\mathbb{K}$, l'ensemble $\mathbb{F}$ est équipotent à $\mathbb{K}$ si $\mathbb{K}$ est infini, et au plus dénombrable sur $\mathbb{K}$ est fini ; c'est la proposition 6.123. En bref :

- Si $\mathbb{K}$ est infini, $\mathbb{K} \approx \mathbb{F} \approx \mathbb{E} < \Omega$.
- Si $\mathbb{K}$ est fini, $\mathbb{K} \leq \mathbb{F} \leq \mathbb{E} < \Omega$ où $\mathbb{E}$ est au maximum dénombrable et Ω est indénombrable.

Dans tous les cas, Ω est strictement surpotent à $\mathbb{F}$, et le lemme 1.133 permet de dire

$$\mathbb{E} \setminus \mathbb{F} \leq \mathbb{E} < \Omega \approx \Omega \setminus \mathbb{F}. \quad (6.203)$$

47. Définition 1.93.

Quelques injections Il existe donc une injection $\varphi: \mathbb{E} \setminus \mathbb{F} \rightarrow \Omega \setminus \mathbb{F}$. Nous posons

$$f: \mathbb{E} \rightarrow \Omega$$

$$x \mapsto \begin{cases} x & \text{si } x \in \mathbb{F} \\ \varphi(x) & \text{si } x \notin \mathbb{F}. \end{cases} \quad (6.204)$$

Nous montrons que f est injective. Soient $x, y \in \mathbb{E}$ tels que $f(x) = f(y)$. Si $x, y \in \mathbb{F}$, alors $x = f(x) = f(y) = y$. Si $x \in \mathbb{F}$ et $y \notin \mathbb{F}$, alors $x = \varphi(y)$ alors que $x \in \mathbb{F}$ et $\varphi(y) \in \Omega \setminus \mathbb{F}$; ce cas est impossible. Enfin si x et y sont hors de $\mathbb{F}$, alors $f(x) = \varphi(x)$ et $f(y) = \varphi(y)$; donc $\varphi(x) = \varphi(y)$ et $x = y$ par injectivité de φ .

Nous avons donc bien une injection $f: \mathbb{E} \rightarrow \Omega$.

La maximalité Nous pouvons mettre sur $f(\mathbb{E}) \subset \Omega$ la structure de corps venant de $\mathbb{E}$. Vu que $f(\mathbb{F}) = \mathbb{F}$, le corps $f(\mathbb{E})$ est une extension algébrique de $\mathbb{F}$. Par maximalité, $f(\mathbb{E}) = \mathbb{F}$.

Mais si $x \in \mathbb{E} \setminus \mathbb{F}$, alors $f(x) \in \Omega \setminus \mathbb{F}$. Donc en réalité nous avons aussi $\mathbb{E} \subset \mathbb{F}$.

Conclusion En conclusion $\mathbb{E} = \mathbb{F}$ et le lemme 6.118 termine en disant que $\mathbb{F}$ est une clôture algébrique de $\mathbb{K}$.

Nous passons à la partie « unicité » de la clôture algébrique. Étant donné que $\mathbb{F}_1$ est une extension algébrique de $\mathbb{K}$ et que $\mathbb{F}_2$ est algébriquement clos, le lemme 6.126 nous donne un morphisme de corps $\sigma: \mathbb{F}_1 \rightarrow \mathbb{F}_2$ tel que $\sigma \circ \alpha_1 = \alpha_2$.

Nous sommes donc dans la situation où $\sigma: \mathbb{F}_1 \rightarrow \mathbb{F}_2$ est une extension de corps où $\mathbb{F}_1$ est algébriquement clos et $\mathbb{F}_2$ est algébrique. Le lemme 6.73 conclut que $\sigma(\mathbb{F}_1) = \mathbb{F}_2$, c'est à dire que σ est surjectif. En tant que morphisme de corps, σ était déjà injective; elle est donc bijective.

Donc $\sigma: \mathbb{F}_1 \rightarrow \mathbb{F}_2$ est un isomorphisme de corps vérifiant $\sigma \circ \alpha_1 = \alpha_2$. $\square$

6.128.

Bien que $\mathbb{C}$ soit une extension algébriquement close de $\mathbb{Q}$, l'ensemble $\mathbb{C}$ n'est pas une clôture algébrique de $\mathbb{Q}$. C'est ce que nous montrons maintenant.

Lemme 6.129.

Le corps $\mathbb{C}$ n'est pas une clôture algébrique⁴⁸ de $\mathbb{Q}$.

Démonstration. Nous montrons qu'il existe des éléments de $\mathbb{C}$ qui ne sont pas des racines de polynômes à coefficients rationnels. L'ensemble $\mathbb{Q}$ est dénombrable par la proposition 1.265. L'ensemble des polynômes de degré n à coefficients dans $\mathbb{Q}$ est en bijection avec les n -uples de rationnels, c'est-à-dire avec $\mathbb{Q}^n$ qui est également dénombrable par la proposition 1.116. Enfin l'ensemble des polynômes à coefficients sur $\mathbb{Q}$ est l'union des polynômes de degré fixés, donc dénombrable par la proposition 1.114.

Jusqu'ici nous avons prouvé que l'ensemble des polynômes à coefficients rationnels était dénombrable. Or chaque polynôme possède une quantité finie de racines par le corolaire 3.144. Donc la partie de $\mathbb{C}$ constituée des nombres qui sont des racines de polynômes à coefficients dans $\mathbb{Q}$ est dénombrable. Mais $\mathbb{C}$ n'est pas dénombrable, donc possède des éléments qui ne sont pas des racines de polynômes. $\square$

6.4.9 Polynômes à plusieurs variables

Nous avons déjà vu $A[X, Y]$ lorsque A est un anneau en la définition 3.51.

Définition 6.130.

Soit un corps $\mathbb{K}$. Le corps $\mathbb{K}(X_1, \dots, X_n)$ est le corps des fractions de l'anneau $\mathbb{K}[X_1, \dots, X_n]$.

Définition 6.131.

Soient un corps $\mathbb{K}$ et une extension $\mathbb{L}$ de $\mathbb{K}$ contenant les éléments $\alpha_1, \dots, \alpha_n$ de $\mathbb{K}$. Nous définissons $\mathbb{K}(\alpha_1, \dots, \alpha_n)$ comme étant l'intersection de tous les sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et les α_i .

48. Clôture algébrique, définition 6.69.

La proposition suivante est analogue à 6.85(2).

Lemme 6.132 ([1]).

Soient un corps $\mathbb{K}$, une extension $\mathbb{L}$ et des éléments $\alpha_1, \dots, \alpha_n$ dans $\mathbb{L}$. Alors

$$\mathbb{K}(\alpha_1, \dots, \alpha_n) = \{r(\alpha_1, \dots, \alpha_n) \text{ tel que } r \in \mathbb{K}(X_1, \dots, X_n)\}. \quad (6.205)$$

Démonstration. Ce que nous avons à droite est un corps : par exemple pour l'inverse, si $r = P/Q$ alors $r(\alpha_1, \dots, \alpha_n) = P(\alpha_1, \dots, \alpha_n)Q(\alpha_1, \dots, \alpha_n)^{-1}$. Cet élément a un inverse en la personne de $(Q/P)(\alpha_1, \dots, \alpha_n)$.

Donc à droite nous avons un sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ ainsi que les α_i . Donc

$$\mathbb{K}(\alpha_1, \dots, \alpha_n) \subset \{r(\alpha_1, \dots, \alpha_n) \text{ tel que } r \in \mathbb{K}(X_1, \dots, X_n)\}. \quad (6.206)$$

D'autre part, tout corps contenant $\mathbb{K}$ et les α_i doit contenir tous les $P(\alpha_1, \dots, \alpha_n)$ ($P \in \mathbb{K}[X_1, \dots, X_n]$), leurs inverses ainsi que leurs produits ; bref doit contenir tous les $r(\alpha_1, \dots, \alpha_n)$ avec $r \in \mathbb{K}[X_1, \dots, X_n]$. $\square$

6.4.10 Corps de décomposition

Définition 6.133.

Soit $\mathbb{K}$ un corps commutatif et $F = (P_i)_{i \in I}$ une famille d'éléments non constants de $\mathbb{K}[X]$. Un **corps de décomposition** de F est une extension $\mathbb{L}$ de $\mathbb{K}$ telle que

- (1) les P_i sont scindés sur $\mathbb{L}$,
- (2) $\mathbb{L} = \mathbb{K}(R)$ où $R = \bigcup_{i \in I} \{x \in \mathbb{L} \text{ tel que } P_i(x) = 0\}$.

C'est-à-dire que $\mathbb{L}$ étend $\mathbb{K}$ par toutes les racines de tous les polynômes de F .

Proposition 6.134 ([141]).

Tout polynôme admet un corps de décomposition. Plus précisément, soit un corps $\mathbb{K}$ et un polynôme $P \in \mathbb{K}[X]$ de degré n . Il existe un corps de décomposition $\mathbb{D}$ de la forme $\mathbb{D} = \mathbb{K}(\alpha_1, \dots, \alpha_n)$ où les α_i sont des racines de P dans $\mathbb{D}$.

Notons que rien dans l'énoncé ne prétend que les α_i soient tous distincts, ni même que certains (voire tous) ne seraient pas dans $\mathbb{K}$.

Démonstration. Soient un corps $\mathbb{K}$ et un polynôme $P \in \mathbb{K}[X]$. Si le degré de P est 0 ou 1, alors $\mathbb{K}$ est un corps de décomposition pour P . Pour le reste nous faisons une récurrence sur le degré de P .

Il y a deux possibilités, soit il existe $\alpha \in \mathbb{K}$ tel que $P(\alpha) = 0$, soit non.

Si racine dans $\mathbb{K}$ Alors le corolaire 6.102 nous permet de factoriser $X - \alpha$:

$$P = (X - \alpha)Q \quad (6.207)$$

avec $\deg(Q) = \deg(P) - 1$. Dans ce cas, $\mathbb{K}$ est un corps de rupture de P .

Si pas de racines dans $\mathbb{K}$ Nous prenons alors un corps de rupture $\mathbb{L} = \mathbb{K}(\alpha)$ avec $P(\alpha) = 0$ (c'est la proposition 6.112 qui donne l'existence d'un corps de rupture). Dans $\mathbb{L}_1$ nous avons

$$P = (X - \alpha)Q \quad (6.208)$$

avec $Q \in \mathbb{L}_1[X]$ et $\deg(Q) = \deg(P) - 1$.

Dans les deux cas Dans les deux cas, par hypothèse de récurrence nous avons un corps de décomposition pour Q qui se présente sous la forme

$$\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_{n-1}). \quad (6.209)$$

De plus, $\mathbb{L}$ est une extension de $\mathbb{L}_1$ parce que c'est une extension du corps sur lequel est Q .

Pour terminer la preuve nous prouvons que

$$\mathbb{D} = \mathbb{K}(\alpha_1, \dots, \alpha_{n-1}, \alpha) \quad (6.210)$$

est un corps de décomposition de P . Vu que $\mathbb{D}$ contient $\mathbb{K}(\alpha)$ (comme cas particulier du lemme 6.132), dans $\mathbb{D}$ nous avons l'égalité $P = (X - \alpha)Q$. Et vu que $\mathbb{D}$ contient également $\mathbb{K}(\alpha_1, \dots, \alpha_{n-1})$, toujours dans $\mathbb{D}$ nous avons aussi

$$Q = (X - \alpha_1) \dots (X - \alpha_{n-1}). \quad (6.211)$$

Donc nous avons dans $\mathbb{D}$ l'égalité

$$P = (X - \alpha)(X - \alpha_1) \dots (X - \alpha_{n-1}). \quad (6.212)$$

□

Lemme 6.135 ([1]).

Soit un polynôme $P \in \mathbb{K}[X]$, et un corps $\mathbb{L}$ dans lequel P est scindé. Si $P = P_1 \dots P_r$ est la décomposition de P en irréductibles dans $\mathbb{K}$, alors chacun des P_i est scindé dans $\mathbb{L}$.

Démonstration. Juste pour le mentionner, le fait que P ait une décomposition en irréductibles est le fait que $\mathbb{K}[X]$ soit factoriel, c'est-à-dire la proposition 6.30.

Le polynôme P est scindé dans $\mathbb{L}$, c'est-à-dire que, en notant n le degré de P ,

$$P = \prod_{i=1}^n (X - \lambda_i) \quad (6.213)$$

avec $\lambda_i \in \mathbb{L}$.

Soit $\mathbb{L}_1$, une extension de $\mathbb{L}$ dans laquelle P_1 est scindé. Ensuite, $\mathbb{L}_2$ une extension de $\mathbb{L}_1$ dans laquelle P_2 est scindé et ainsi de suite. Nous avons construit $\mathbb{L}_r$, une extension de $\mathbb{L}$ dans laquelle tous les P_i sont scindés ainsi que P lui-même. Dans ce corps nous avons l'égalité

$$P = \prod_{k=1}^n (X - \mu_k) \quad (6.214)$$

où les μ_k sont des éléments des diverses extensions $\mathbb{L}_i$, et sont les racines des P_i . En tout cas, tous sont dans $\mathbb{L}_r$.

Les deux décompositions (6.213) et (6.214) sont des décompositions dans $\mathbb{L}_r[X]$ du polynôme P . Vu que ce dernier est factoriel, en réalité les deux décompositions sont identiques (se souvenir de la définition 3.68), et nous avons $\mu_k \in \mathbb{L}$ pour tout k . Toutes les extensions $\mathbb{L}_i$ sont en réalité triviales, et nous avons $\mathbb{L}_r = \mathbb{L}$.

Bref, tout cela pour dire que les P_i ont toutes leurs racines dans $\mathbb{L}$. □

Théorème 6.136 ([130]).

Soient :

- un isomorphisme de corps $\tau: \mathbb{K} \rightarrow \mathbb{K}'$;
- un polynôme non constant $P \in \mathbb{K}[X]$ de degré n ;
- un corps de décomposition $\mathbb{L}$ de P sur $\mathbb{K}$;
- un corps de décomposition $\mathbb{L}'$ de P sur $\mathbb{K}'$;

Alors τ se prolonge en un isomorphisme $\sigma: \mathbb{L} \rightarrow \mathbb{L}'$.

Démonstration. Soit m le nombre de racines de P dans $\mathbb{L} \setminus \mathbb{K}$. Nous faisons une récurrence sur m .

Si $m = 0$ alors $\mathbb{K}$ est un corps de rupture de P ; nous avons

$$P = (X - \lambda_1) \dots (X - \lambda_n) \quad (6.215)$$

avec $\lambda_i \in \mathbb{K}$. Dans ce cas nous avons aussi

$$\tau(P) = (X - \tau(\lambda_1)) \dots (X - \tau(\lambda_n)) \quad (6.216)$$

avec $\tau(\lambda_i) \in \mathbb{K}'$. Nous avons donc $\mathbb{L}' = \mathbb{K}'$ et prendre $\sigma = \tau$ fonctionne.

Nous supposons à présent que $m > 0$. Plus précisément nous considérons un polynôme possédant exactement m racines dans $\mathbb{L} \setminus \mathbb{K}$. Soit

$$P = P_1 \dots P_r \quad (6.217)$$

sa décomposition en irréductibles dans $\mathbb{K}[X]$ (notons que $r \leq n$ parce que chacun des facteurs est de degré au moins 1). Au moins un des P_i est de degré plus grand ou égal à 2. Nous savons de la proposition 6.30 que $\mathbb{K}[X]$ est un anneau factoriel. Le lemme 6.135 nous assure que les polynômes P_i sont également scindés dans $\mathbb{L}$. Et l'unicité de la décomposition fait en sorte que les racines des P_i sont celles de P .

Soit $\alpha \in \mathbb{L}$, une racine de P_1 . Vu que P_1 est irréductible sur $\mathbb{K}$, l'application suivante est un isomorphisme de corps par le lemme 6.76 :

$$\begin{aligned} \psi: \mathbb{K}[X]/(P_1) &\rightarrow \mathbb{K}[\alpha] \\ \bar{Q} &\mapsto Q(\alpha). \end{aligned} \quad (6.218)$$

Notons que le lemme parle du quotient par le polynôme minimal, mais ici nous avons un irréductible. Un polynôme annulateur irréductible est multiple du polynôme minimal, et l'idéal engendré est le même.

Nous avons aussi la décomposition

$$\tau(P) = \tau(P_1) \dots \tau(P_r), \quad (6.219)$$

et chacun des $\tau(P_i)$ a ses racines dans $\mathbb{L}'$. Soit β , une racine de $\tau(P_1)$ dans $\mathbb{L}'$. Alors nous avons l'isomorphisme

$$\psi': \mathbb{K}'[X]/(\tau(P_1)) \rightarrow \mathbb{K}'[\beta]. \quad (6.220)$$

De plus, par le lemme 6.42, nous savons que τ passe aux classes :

$$\phi_\tau: \mathbb{K}[X]/(P_1) \rightarrow \mathbb{K}'[X]/(\tau(P_1)) \quad (6.221)$$

est un isomorphisme d'anneaux. Et enfin, dernier résultat externe à invoquer, la proposition 6.90 nous assure que $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$ et $\mathbb{K}'[\beta] = \mathbb{K}'(\beta)$. Posons pour l'occasion $\mathbb{K}_1 = \mathbb{K}(\alpha)$ et $\mathbb{K}'_1 = \mathbb{K}'(\beta)$.

Nous avons l'enchaînement suivant d'isomorphismes de corps⁴⁹ :

$$\tau_1 = \psi' \circ \phi_\tau \circ \psi^{-1}: \mathbb{K}_1 \rightarrow \mathbb{K}[X]/(P_1) \rightarrow \mathbb{K}'[X]/(\tau(P_1)) \rightarrow \mathbb{K}'_1. \quad (6.222)$$

Cet isomorphisme $\tau_1: \mathbb{K}_1 \rightarrow \mathbb{K}'_1$ prolonge τ . Si vous aimez les diagrammes, en voici un sur lequel les i représentent des inclusions et où τ et τ_1 sont des isomorphismes

$$\begin{array}{ccccc} \mathbb{K} & \xrightarrow{i} & \mathbb{K}_1 & \xrightarrow{i} & \mathbb{L} \\ \tau \downarrow & & \downarrow \tau_1 & & \\ \mathbb{K}' & \xrightarrow{i} & \mathbb{K}'_1 & \xrightarrow{i} & \mathbb{L}' \end{array} \quad (6.223)$$

Le corps $\mathbb{L}$ est un corps de décomposition de P sur $\mathbb{K}_1$, et le nombre de racines de P dans $\mathbb{L} \setminus \mathbb{K}_1$ est strictement plus petit que m parce qu'il y en a exactement m dans $\mathbb{L} \setminus \mathbb{K}$ et que $\mathbb{K}_1$ en a au moins une de plus que $\mathbb{K}$. Même raisonnement pour $\mathbb{K}'$, $\mathbb{K}'_1$ et $\mathbb{L}'$.

Résumons la situation :

49. En réalité il est plus exact de dire « isomorphisme d'anneaux », parce que la structure de corps n'est en réalité aucune nouvelle structure par rapport à l'anneau.

- $\tau_1: \mathbb{K}_1 \rightarrow \mathbb{K}'_1$ est un isomorphisme de corps ;
- $P \in \mathbb{K}_1[X]$ est un polynôme non constant ;
- $\mathbb{L}$ est un corps de décomposition de P sur $\mathbb{K}_1$;
- $\mathbb{L}'$ est un corps de décomposition de P sur $\mathbb{K}'_1$;
- le nombre de racines de P dans $\mathbb{L} \setminus \mathbb{K}_1$ est strictement inférieur à m .

Donc, par hypothèse de récurrence sur m , il existe un isomorphisme $\sigma: \mathbb{L} \rightarrow \mathbb{L}'$ qui prolonge τ_1 . Vu que τ_1 prolonge τ , nous avons également σ qui prolonge τ . $\square$

L'énoncé le plus compact pour l'unicité du corps de décomposition (à isomorphisme près) est le suivant :

Proposition 6.137.

Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$. Soient $\mathbb{L}$ et $\mathbb{F}$ deux corps de décomposition de P . Alors il existe un isomorphisme $f: \mathbb{L} \rightarrow \mathbb{F}$ tel que $f|_{\mathbb{K}} = \text{Id}$.

Démonstration. C'est un cas particulier du théorème 6.136, où nous considérons $\mathbb{K} = \mathbb{K}'$ muni de l'isomorphisme identité. $\square$

Cependant le passage par l'énoncé plus compliqué 6.136 est nécessaire pour les besoins de la récurrence.

6.138.

À propos de terminologie. Lorsque nous disons « un corps de décomposition » nous référons à la définition 6.133 et il n'y a pas vraiment unicité. Si nous disons « le corps de décomposition » nous référons en général à celui construit dans la proposition 6.134 qui n'est en réalité même pas très explicite.

Quoi qu'il en soit, nous nous permettons de dire « le » corps de décomposition lorsque nous parlons de propriétés invariantes par isomorphisme.

6.139.

La construction du corps de décomposition d'un polynôme fonctionne en prenant successivement le corps de rupture des facteurs irréductibles. Nous insistons sur le fait que cette opération se fait sur chaque facteur irréductible séparément.

L'exemple suivant montre dans quel ordre se passent les choses.

Exemple 6.140.

Soit le polynôme $P = X^4 - 5X^2 + 6$. Sa factorisation en irréductibles est :

$$P = (X^2 - 2)(X^2 - 3). \quad (6.224)$$

Ce polynôme n'est pas irréductible sur $\mathbb{Q}$ et il ne s'agit donc pas de prendre brutalement un corps de rupture pour P . Il s'agit de poser $P = P_1 P_2$ avec

$$P_1 = X^2 - 2 \quad (6.225a)$$

$$P_2 = X^2 - 3, \quad (6.225b)$$

de remarquer que P_1 et P_2 sont irréductibles sur $\mathbb{Q}$ et de chercher des corps de rupture pour eux. On commence par P_1 . Nous avons le corps de rupture $\mathbb{L}_1 = \mathbb{Q}(\sqrt{2})$ et la factorisation

$$P_1 = (X + \sqrt{2})(X - \sqrt{2}). \quad (6.226)$$

Ensuite nous considérons P_2 dans $\mathbb{L}_1[X]$. Ce P_2 est encore irréductible. Nous lui cherchons un corps de rupture, et c'est $\mathbb{L}_2 = \mathbb{L}_1(\sqrt{3})$ dans lequel nous avons

$$P_2 = (X - \sqrt{3})(X + \sqrt{3}). \quad (6.227)$$

Nous savons (par le lemme 6.117) que

$$\mathbb{L}_2 = \mathbb{L}_1(\sqrt{3}) = (\mathbb{Q}(\sqrt{2}))(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}). \quad (6.228)$$

Nous pouvons donc écrire en toute confiance, dans $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ la factorisation

$$P = (X + \sqrt{2})(X - \sqrt{2})(X + \sqrt{3})(X - \sqrt{3}). \quad (6.229)$$

Et nous notons que si nous avons commencé par P_2 au lieu de P_1 , nous aurions eu le même résultat final. $\triangle$

Corolaire 6.141 ([1]).

Le corps de décomposition d'un polynôme est une extension finie.

Démonstration. Soient un corps $\mathbb{K}$, un polynôme $P \in \mathbb{K}[X]$ et un corps de décomposition $\mathbb{D}$ de P de la forme $\mathbb{D} = \mathbb{K}(\alpha_1, \dots, \alpha_n)$ où les α_i sont les racines de P dans $\mathbb{D}$. Cela existe par la proposition 6.134.

Vu que le lemme 6.117 donne

$$\mathbb{K}(\alpha_1, \dots, \alpha_n) = (\mathbb{K}(\alpha_1, \dots, \alpha_{n-1}))(\alpha_n), \quad (6.230)$$

le corps $\mathbb{D}$ se construit comme une pile d'extensions finies. Les degrés se composant par le lemme 6.58, au final ce corps de décomposition est une extension finie.

Soit maintenant un corps de décomposition quelconque $\mathbb{L}$. La proposition 6.137 donne un isomorphisme de corps⁵⁰ $f: \mathbb{L} \rightarrow \mathbb{D}$ tel que f soit l'identité sur $\mathbb{K}$.

Si $\{v_i\}_{i \in I}$ est une base de $\mathbb{D}$ comme espace vectoriel sur $\mathbb{K}$, êtes-vous prêts à parier que $\{f(v_i)\}_{i \in I}$ est une base de $\mathbb{L}$ comme espace vectoriel sur $\mathbb{K}$ ⁵¹? $\square$

6.4.11 Non irréductible ou pas corps ?

Nous avons déjà mentionné que nous ne définissons le corps de rupture d'un polynôme que dans le cas de polynôme irréductible à coefficients dans un corps.

D'abord si P n'est pas irréductible, la question de chercher un corps de rupture n'a pas beaucoup de sens.

Si A est un anneau intègre et si P est un polynôme irréductible sur A , nous pouvons considérer le corps des fractions de A , dire $P \in \text{Frac}(A)[X]$ et continuer. Étendre la définition de corps de rupture de cette façon aux polynômes à coefficients dans un anneau intègre n'est pas une grande révolution.

Au lieu de cela, nous pouvons nous demander dans quel cas nous aurions que $A[X]/(P)$ est directement un corps.

Exemple 6.142.

Soit le polynôme constant $P = 2$ dans $\mathbb{Z}[X]$. Il y est irréductible parce qu'il ne peut pas être écrit comme produit de deux non inversibles. Ce polynôme a deux propriétés ennuyeuses :

- Il n'est plus irréductible sur $\mathbb{Q}$,
- Il n'existe aucun corps contenant une racine de P tout en contenant $\mathbb{Z}$ comme sous-anneau.

$\triangle$

6.4.12 Clôture algébrique

Théorème 6.143.

Tout corps $\mathbb{K}$ possède une clôture algébrique⁵² Ω . De plus si $\mathbb{L}$ est une extension de $\mathbb{K}$, alors $\mathbb{L}$ est $\mathbb{K}$ -isomorphe à un sous corps de Ω .

⁵⁰. Un isomorphisme de corps est juste un isomorphisme d'anneaux.

⁵¹. Personnellement, je n'ai pas vérifié. Vérifiez vous-même et écrivez-moi pour dire si c'est bon ou non.

⁵². Définition 6.69.

Les deux parties de ce théorème utilisent l'axiome du choix.

Notons en particulier que si Ω' est une autre clôture algébrique de $\mathbb{K}$, alors Ω et Ω' sont des sous corps l'un de l'autre et sont donc $\mathbb{K}$ -isomorphes.

Lemme 6.144.

Les polynômes $P, Q \in \mathbb{K}[X]$ ne sont pas premiers entre eux si et seulement s'ils ont une racine commune dans la clôture algébrique Ω de $\mathbb{K}$.

Démonstration. Soit A un polynôme non inversible divisant P et Q . Par définition de Ω , ce polynôme A a une racine dans Ω qui est alors une racine commune à P et Q dans Ω .

Pour le sens inverse, si α est une racine commune de P et Q , alors le polynôme $X - \alpha$ divise P et Q et donc P et Q ne sont pas premiers entre eux. $\square$

Exemple 6.145.

Soit p un nombre premier. Montrons que le polynôme

$$Q(X) = X^p - X + 1 \quad (6.231)$$

est irréductible dans $\mathbb{F}_p$.

Nous supposons qu'il n'est pas irréductible, c'est-à-dire que

$$Q(X) = R(X)S(X) \quad (6.232)$$

avec R et S , des polynômes de degrés ≥ 1 dans $\mathbb{F}_p[X]$

Soit $\bar{\mathbb{F}}_p$ une clôture algébrique⁵³ de $\mathbb{F}_p$ et $\alpha \in \bar{\mathbb{F}}_p$ tel que $R(\alpha) = 0$. Pour tout $a \in \mathbb{F}_p$, nous avons

$$Q(\alpha + a) = (\alpha + a)^p - (\alpha + a) + 1 \quad (6.233a)$$

$$= \alpha^p + a^p - \alpha - a + 1 \quad (6.233b)$$

$$= \alpha^p - \alpha + 1 \quad (6.233c)$$

$$= Q(\alpha) \quad (6.233d)$$

$$= 0 \quad (6.233e)$$

où nous avons utilisé le fait que $a^p = a$ et que α était une racine de Q . Ce que nous venons de prouver est que l'ensemble des racines de Q dans $\bar{\mathbb{F}}_p$ est donné par $\{\alpha + a \text{ tel que } a \in \mathbb{F}_p\}$.

Les polynômes R et S sont donc formés de produits de termes $X - (\alpha + a)$ avec $a \in \mathbb{F}_p$. L'un des deux –disons R pour fixer les idées– doit bien en avoir plus que 1. Nous avons alors

$$R(X) = \prod_{i=1}^k (X - (\alpha + a_i)) \quad (6.234)$$

où les a_i sont les éléments de $\mathbb{F}_p$. En développant un peu,

$$R(X) = X^k - \sum_{i=1}^k (\alpha + a_i^{k-1}) + \text{termes de degré plus bas en } X. \quad (6.235)$$

Le coefficient devant X^{k-1} n'est autre que $k\alpha + \sum_i a_i$. Étant donné que $k \neq 0$ et que $R \in \mathbb{F}_p[X]$, nous devons avoir $\alpha \in \mathbb{F}_p$. Par conséquent nous avons $\alpha^p = \alpha$ et une contradiction :

$$Q(\alpha) = \alpha^p - \alpha + 1 = 1 \neq 0. \quad (6.236)$$

Le polynôme $X^p - X + 1$ est donc irréductible sur $\mathbb{F}_p$. $\triangle$

53. Définition 6.69. Pour l'existence c'est le théorème 6.143.

6.4.13 Extensions séparables

Notons que dans ce qui va suivre nous allons parler de $\mathbb{K}[X]$, l'ensemble des polynômes sur un corps. Cela ne s'applique donc pas à $\mathbb{Z}[X]$ par exemple.

Une des choses intéressantes avec les extensions séparables c'est qu'elles vérifient le théorème de l'élément primitif 6.158.

Définition 6.146.

Soit $\mathbb{K}$ un corps. Un polynôme irréductible $P \in \mathbb{K}[X]$ est **séparable** sur $\mathbb{K}$ si dans un corps de décomposition, ses racines sont distinctes, c'est-à-dire que si P est de degré n , alors il possède n racines distinctes dans un corps de décomposition.

Si P est un polynôme non constant dont la décomposition en irréductibles est $P = P_1 \dots P_r$, nous disons qu'il est **séparable** si tous les P_i le sont.

La proposition suivante donne un sens à la définition de polynôme irréductible séparable.

Proposition 6.147.

Soit P irréductible dans $\mathbb{K}[X]$ ayant des racines distinctes dans le corps de décomposition $\mathbb{L}$. Si $\mathbb{L}'$ est un autre corps de décomposition pour P , alors P a aussi ses racines distinctes dans $\mathbb{L}'$.

Démonstration. L'ingrédient est la proposition 6.137 qui donne l'unicité du corps de décomposition à $\mathbb{K}$ -isomorphisme près. Soit donc $\psi: \mathbb{L} \rightarrow \mathbb{L}'$ un isomorphisme laissant invariant les éléments de $\mathbb{K}$. D'une part, étant donné que P est à coefficients dans $\mathbb{K}$, nous avons $\psi(P) = P$. D'autre part dans $\mathbb{L}$ le polynôme P s'écrit

$$P = a(X - \alpha_1) \dots (X - \alpha_n) \quad (6.237)$$

avec $a \in \mathbb{K}$ et $\alpha_i \in \mathbb{L}$. Nous avons donc

$$P = \psi(P) = a(X - \psi(\alpha_1)) \dots (X - \psi(\alpha_n)). \quad (6.238)$$

Donc les racines de P dans $\mathbb{L}'$ sont les éléments $\psi(\alpha_i)$ qui sont distincts. $\square$

Exemple 6.148.

Un polynôme peut être séparable sur un corps, mais non séparable sur un autre. Soit $\mathbb{L} = \mathbb{F}_p(T)$ et $\mathbb{K} = \mathbb{F}_p(T^p)$. Nous considérons le polynôme

$$P = X^p - T^p \quad (6.239)$$

dans $\mathbb{K}[X]$. Par le morphisme de Frobenius nous avons

$$P = (X - T)^p \quad (6.240)$$

dans $\mathbb{L}[X]$. Le polynôme P est irréductible sur $\mathbb{K}[X]$ parce que ses diviseurs sont de la forme $(X - T)^k$ qui contiennent T^k qui n'est pas dans $\mathbb{K}$ (sauf si $k = n$ ou $k = 0$).

Ce polynôme n'est pas séparable sur $\mathbb{K}$ parce que dans le corps de décomposition $\mathbb{L}$, la racine T est multiple. Notons bien le raisonnement : P étant irréductible, pour savoir s'il est séparable, on le regarde dans un corps de décomposition.

Par contre si nous regardons P dans $\mathbb{L}[X]$ alors P n'est plus irréductible parce que ses facteurs irréductibles sont $(X - T)$. N'étant pas irréductible, nous regardons les racines de *ses facteurs irréductibles*. Or chacun des facteurs irréductibles étant $X - T$, les racines sont simples. $\triangle$

Exemple 6.149.

Le polynôme $(X - 1)^3$ est séparable sur $\mathbb{Q}$ parce que ses facteurs irréductibles dans $\mathbb{Q}[X]$ sont $X - 1$ et $X^2 + X + 1$, et ces deux polynômes ont des racines simples (dans $\mathbb{Q}(i)$). $\triangle$

Exemple 6.150.

Le polynôme $(X^2 + 1)^2$ est séparable dans $\mathbb{Q}[X]$. En effet, il a pour facteurs irréductibles le polynôme $X^2 + 1$ (en deux exemplaires), et ce polynôme a pour racines $\pm i$ dans l'extension $\mathbb{Q}(i)$, racines qui sont simples pour ce polynôme. $\triangle$

Proposition 6.151 ([142]).

Soit $P \in \mathbb{K}[X]$ un polynôme non constant. Les propriétés suivantes sont équivalentes.

- (1) P a une racine multiple dans une extension de $\mathbb{K}$. C'est-à-dire qu'il existe une extension de $\mathbb{K}$ dans laquelle P a une racine multiple.
- (2) P a une racine multiple dans tout corps de décomposition.
- (3) P et P' ont une racine commune dans une extension de $\mathbb{K}$.
- (4) le degré de $\text{pgcd}(P, P')$ est ≥ 1 .

Démonstration. **(1) $\Rightarrow$ (2)** Soit a , une racine multiple de P dans une extension $\mathbb{L}$ de $\mathbb{K}$, et $\mathbb{E}$, un corps de décomposition de P . Alors nous voulons prouver que P ait une racine multiple dans $\mathbb{E}$.

Nous pouvons voir $P \in \mathbb{L}[X]$, et construire un corps de décomposition $\mathbb{E}'$ qui est une extension de $\mathbb{L}$. Vu que $\mathbb{E}$ et $\mathbb{E}'$ sont deux corps de décomposition de P nous avons un isomorphisme $\psi: \mathbb{E}' \rightarrow \mathbb{E}$. Si $a \in \mathbb{E}$ est une racine multiple de P , alors $\psi(a)$ est une racine multiple de P dans $\mathbb{E}'$ parce que

$$P(\psi(a)) = \psi(P(a)). \quad (6.241)$$

(2) $\Rightarrow$ (3) Soit $\mathbb{L}$ un corps de décomposition de P sur $\mathbb{K}$ et $a \in \mathbb{L}$, une racine multiple de P . On a alors $P = (X - a)^2 Q$ avec $Q \in \mathbb{L}[X]$. En dérivant,

$$P' = 2(X - a)Q + (X - a)^2 Q', \quad (6.242)$$

et donc a est également une racine de P' .

(3) $\Rightarrow$ (4) Soit D un pgcd de P et P' . D'après le théorème de Bézout il existe $A, B \in \mathbb{K}[X]$ tels que

$$AP + BP' = D. \quad (6.243)$$

Si a est une racine commune de P et P' dans une extension $\mathbb{L}$, alors c'est aussi une racine de D et donc $\deg(D) \geq 1$.

(4) $\Rightarrow$ (1) Si le degré de D est plus grand ou égal à 1, alors nous considérons une racine a de D dans $\mathbb{L}$ (une extension de $\mathbb{K}$). Étant donné que D divise P et P' , l'élément a est une racine commune de P et P' . Nous montrons maintenant que a est alors une racine multiple de P . Vu que $P(a) = 0$ nous avons

$$P = (X - a)Q, \quad (6.244)$$

et $P' = Q + (X - a)Q'$. Mais alors $P'(a) = Q(a)$ et donc $Q(a) = 0$ et donc a est une racine double de P . Par conséquent a est une racine multiple de P dans $\mathbb{K}$. □

Notons que si P est irréductible, cette proposition donne des conditions pour que P ne soit pas séparable.

Proposition 6.152.

Soit $P \in \mathbb{K}[X]$ irréductible. Le polynôme P est séparable si et seulement si $P' \neq 0$.

Démonstration. Soit $D = \text{pgcd}(P, P')$ et nous voudrions prouver que $\deg(D) \geq 1$ si et seulement si $P' = 0$. Si $P' = 0$, alors $\text{pgcd}(P, P') = P$ est donc $\deg(D) \geq 1$.

Dans l'autre sens, si P est irréductible, il est associé à D parce qu'il n'a pas d'autres diviseurs que lui-même et le polynôme constant 1. Ainsi, $D \in \mathbb{K}$, ou bien $P = \lambda D$ avec $\lambda \in \mathbb{K}$. et donc $\deg(P) \geq 1$. Dans les deux cas, P' est nécessairement non-nul. □

Corolaire 6.153.

Si $\mathbb{K}$ est de caractéristique nulle, alors tout polynôme de $\mathbb{K}[X]$ est séparable.

Démonstration. Il suffit de montrer que les irréductibles sont séparables. Soit P un polynôme irréductible et unitaire de degré d . Le terme de plus haut degré de P' est alors dX^{d-1} qui est non nul parce que $d \neq 0$ en caractéristique nulle. Donc $P' \neq 0$ et donc P est séparable par la proposition 6.151. $\square$

Définition 6.154.

Soit $\mathbb{L}$ une extension algébrique de $\mathbb{K}$.

- (1) On dit que l'élément $a \in \mathbb{L}$ est **séparable** sur $\mathbb{K}$ si son polynôme minimal dans $\mathbb{K}[X]$ est séparable sur $\mathbb{K}$ (définition 6.146).
- (2) L'extension $\mathbb{L}$ est **séparable** si tous ses éléments sont séparables.

Proposition 6.155.

Soit $\mathbb{K}$ un corps. Les conditions suivantes sont équivalentes :

- (1) toutes les extensions algébriques de $\mathbb{K}$ sont séparables ;
- (2) tout polynôme irréductible de $\mathbb{K}[X]$ est séparable.

En particulier les extensions algébriques des corps de caractéristique nulle sont toutes séparables.

Démonstration. En plusieurs parties.

(1) implique (2) Soit un polynôme irréductible P de $\mathbb{K}[X]$, et un corps de décomposition $\mathbb{L}$ de P . Cela est une extension algébrique par le corolaire 6.141. Elle est donc séparable par hypothèse.

Voilà une première chose de dite.

Maintenant, nous voudrions montrer que P est un polynôme séparable. Dans $\mathbb{L}$ nous avons

$$P = \prod_{i=1}^n (X - a_i), \quad (6.245)$$

et tout le défi est de prouver que les a_i sont tous distincts.

Soient deux racines $a, b \in \mathbb{L}$ de P . Nous considérons les polynômes minimaux μ_a et μ_b dans $\mathbb{K}[X]$. Ces deux polynômes divisent P parce que P est à la fois dans l'idéal annulateur de a et de b . Mais comme P est irréductible, il existe $k_a, k_b \in \mathbb{K}$ tels que $P = k_a \mu_a$ et $P = k_b \mu_b$. Donc les polynômes μ_a, μ_b et P sont multiples les uns des autres. Vu que μ_a et μ_b sont unitaires, $\mu_a = \mu_b$.

Nous avons :

$$P = k\mu = \prod_{i=1}^n (X - a_i). \quad (6.246)$$

Or le polynôme μ est irréductible par la proposition 6.62(1), et l'extension $\mathbb{L}$ est séparable, donc μ n'a que des racines simples, Donc tous les a_i sont distincts.

(2) implique (1) Soit une extension algébrique $\mathbb{L}$ de $\mathbb{K}$. Soit $a \in \mathbb{L}$. Nous devons prouver que le polynôme minimal de a dans $\mathbb{K}$ est séparable, c'est-à-dire qu'il n'a que des racines simples.

Le polynôme minimal $\mu_a \in \mathbb{K}[X]$ de a est irréductible et donc séparable. Donc $\mathbb{L}$ est séparable.

La dernière phrase est une conséquence du corolaire 6.153. $\square$

Corolaire 6.156.

Toute les extensions algébriques de $\mathbb{Q}$ sont séparables.

Démonstration. Le corps $\mathbb{Q}$ est de caractéristique nulle (définition 1.231). Le corolaire 6.153 dit alors que tout polynôme sur $\mathbb{Q}$ est séparable. La proposition 6.155 conclut en disant que toutes les extensions algébriques de $\mathbb{Q}$ sont séparables. $\square$

Théorème 6.157 ([76]).

Soit $\mathbb{K}$ un corps (pas spécialement fini). Tout sous-groupe fini de $\mathbb{K}^*$ est cyclique.

Démonstration. Soit G un sous-groupe fini de $\mathbb{K}^*$ et ω son exposant (qui est le PPCM des ordres des éléments de G). Étant donné que $|G|$ est divisé par tous les ordres, il est divisé par le PPCM des ordres. Bref, nous avons

$$x^\omega = 1 \quad (6.247)$$

pour tout $x \in G$. Mais ce polynôme possède au plus ω racines dans $\mathbb{K}$. Du coup $|G| \leq \omega$. Et comme on avait déjà vu que $\omega \mid |G|$, on a $\omega = |G|$. Il suffit plus que trouver un élément d'ordre effectivement ω . Cela est fait par le lemme 3.32. $\square$

Théorème 6.158 (Théorème de l'élément primitif[76]).

Toute extension de corps séparable finie admet un élément primitif⁵⁴.

Autrement dit, soient des éléments algébriques $\alpha_1, \dots, \alpha_n$ séparables⁵⁵ sur $\mathbb{K}$, et soit l'extension engendrée $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_n)$. Alors $\mathbb{L}$ admet un élément primitif, c'est-à-dire un élément θ tel que $\mathbb{L} = \mathbb{K}(\theta)$.

Démonstration. Si le corps $\mathbb{K}$ est fini, alors $\mathbb{L}$ est également fini. Donc $\mathbb{L}^*$ est cyclique par le théorème 6.157. Si θ est un générateur de $\mathbb{L}^*$, alors $\mathbb{L} = \mathbb{K}(\theta)$.

Passons au cas où $\mathbb{K}$ est infini. Il suffit d'examiner le cas $n = 2$; en effet pour $n = 1$ c'est trivial et si $n > 2$, alors

$$\mathbb{K}(\alpha_1, \dots, \alpha_n) = \mathbb{K}(\alpha_1, \dots, \alpha_{n-1})(\alpha_n), \quad (6.248)$$

et donc si $\mathbb{K}(\alpha_1, \dots, \alpha_{n-1}) = \mathbb{K}(\theta)$, nous avons

$$\mathbb{K}(\alpha_1, \dots, \alpha_n) = \mathbb{K}(\theta, \alpha_n) \quad (6.249)$$

et nous sommes réduit au cas $n = 2$ par récurrence.

Soit donc $\mathbb{L} = \mathbb{K}(\alpha, \beta)$; soit P le polynôme minimal de α sur $\mathbb{K}$ et Q celui de β . Nous nommons $\mathbb{E}$, un corps de décomposition de PQ . Nous avons $\mathbb{L} \subset \mathbb{E}$. Vu que P et Q sont polynômes minimaux d'éléments qui sont par hypothèse séparables, les polynômes P et Q sont séparables. Donc dans $\mathbb{E}$ les racines de P sont distinctes parce que P est irréductible (et idem pour Q). Soient les racines

$$\alpha_1 = \alpha, \alpha_2, \dots, \alpha_r \quad (6.250)$$

de P dans $\mathbb{E}$ et les racines

$$\beta_1 = \beta, \beta_2, \dots, \beta_s \quad (6.251)$$

de Q dans $\mathbb{E}$. Ici r et s sont les degrés de P et Q .

Si $s = 1$ alors $Q = X - \beta$ et donc $\beta \in \mathbb{K}$ (parce que $Q \in \mathbb{K}[X]$). Du coup nous avons $\mathbb{L} = \mathbb{K}(\alpha)$ et le théorème est démontré. Nous supposons donc maintenant que $s \geq 2$.

Pour chaque $(i, j) \in \llbracket 1, r \rrbracket \times \llbracket 2, s \rrbracket$, l'équation $\alpha_i + x\beta_k = \alpha_1 + x\beta_1$ pour $x \in \mathbb{K}$ a au plus⁵⁶ une solution donnée le cas échéant par

$$x = (\alpha_i - \alpha_1)(\beta_1 - \beta_k)^{-1} \quad (6.252)$$

Notons que cela est de toutes façons dans $\mathbb{L}$ et qu'étant donné que $\beta_1 \neq \beta_k$, cette solution a un sens (ici on utilise l'hypothèse de séparabilité). Étant donné que $\mathbb{K}$ est infini nous pouvons donc trouver un $c \in \mathbb{K}$ qui ne résout aucune des équations (6.252) :

$$\alpha_i + c\beta_k \neq \alpha_1 + c\beta_1. \quad (6.253)$$

Nous posons $\theta = \alpha_1 + c\beta_1$ et nous prétendons que $\mathbb{L} = \mathbb{K}(\theta)$.

Pour cela, commençons par montrer que $\beta_1 \in \mathbb{K}(\theta)$. On considère, dans $\mathbb{K}(\theta)[T]$, les polynômes $Q(T)$ et $S(T) = P(\theta - cT)$, et on nomme R le PGCD de ces deux polynômes. Alors, une racine

⁵⁴. Définition 6.94.

⁵⁵. Définition 6.154(1).

⁵⁶. La solution (6.252) peut être dans $\mathbb{L}$ et non dans $\mathbb{K}$. L'équation peut donc très bien ne pas avoir de solutions $x \in \mathbb{K}$.

de R doit être une racine de Q , et est donc un des β_i . Or, d'une part, le choix de θ fait que β_1 est une racine de R parce que

$$S(\beta_1) = P(\theta - c\beta_1) = P(\alpha_1 + c\beta_1 - c\beta_1) = P(\alpha_1) = 0. \quad (6.254)$$

D'autre part, si $k \geq 2$, alors

$$S(\beta_k) = P(\alpha_1 + c\beta_1 - c\beta_k) = P(\alpha_1 + c(\beta_1 - \beta_k)) \neq 0 \quad (6.255)$$

parce que $\alpha_1 + c(\beta_1 - \beta_k)$ ne vaut ni α_1 (le second terme est non-nul), ni un autre α_i (à cause de (6.253)).

Il s'ensuit que Q et S n'ont qu'une racine commune $\beta_1 = \beta$, qui est donc l'unique racine de R . Ainsi,

$$R = X - \beta \in \mathbb{K}(\theta)[T], \quad (6.256)$$

et donc $\beta \in \mathbb{K}(\theta)$.

Dès lors $\alpha = \alpha_1 = \theta - c\beta$ est alors immédiatement dans $\mathbb{K}(\theta)$; puisque les deux éléments α et β sont dans $\mathbb{K}(\theta)$, nous avons obtenu $\mathbb{L} = \mathbb{K}(\alpha, \beta) = \mathbb{K}(\theta)$. □

Exemple 6.159.

Le théorème de l'élément primitif 6.158 ne tient pas pour les corps non commutatifs. Considérons par exemple le corps $\mathbb{K}$ des quaternions et le groupe à 8 éléments $G = \{\pm 1, \pm i, \pm j, \pm k\}$. Ce dernier groupe n'est pas cyclique alors qu'il est un groupe fini dans $\mathbb{K}^*$. △

Exemple 6.160.

Il est aussi possible pour un groupe fini d'avoir $\omega(G) = |G|$ sans pour autant que G soit cyclique. Par exemple pour $G = S_3$, nous avons $|S_3| = 6$ alors que les éléments de S_3 sont soit d'ordre 2 soit d'ordre 3 et $\omega(G) = \text{ppcm}(2, 3) = 6$. Pourtant S_3 n'est pas cyclique. △

6.5 Idéal maximum

6.5.1 Idéal maximum

Définition 6.161.

Une $\mathbb{K}$ -algèbre est de **type fini** si elle est le quotient de $\mathbb{K}[X_1, \dots, X_n]$ par un idéal (pour un certain n).

Théorème 6.162 ([143]).

Soit $\mathbb{K}$ un corps et B , une $\mathbb{K}$ -algèbre de type fini. Si B est un corps, alors c'est une extension algébrique finie de $\mathbb{K}$.

Théorème 6.163 ([143]).

Si $\mathbb{K}$ est un corps algébriquement clos, les idéaux maximaux de $\mathbb{K}[X_1, \dots, X_n]$ sont de la forme

$$(X_1 - a_1, \dots, X_n - a_n) \quad (6.257)$$

où les a_i sont des éléments de $\mathbb{K}$.

Démonstration. Nous commençons par montrer que

$$J = (X_1 - a_1, \dots, X_n - a_n) \quad (6.258)$$

est un idéal maximum. Pour cela nous considérons le morphisme surjectif d'anneaux

$$\begin{aligned} \phi: \mathbb{K}[X_1, \dots, X_n] &\rightarrow \mathbb{K} \\ P &\mapsto P(a_1, \dots, a_n). \end{aligned} \quad (6.259)$$

Soit $P \in \ker(\phi)$; nous écrivons la division euclidienne de P par $X - a_1$ puis celle du reste par $X - a_2$ et ainsi de suite :

$$P = (X - a_1)Q_1 + \cdots + (X_n - a_n)Q_n + R \quad (6.260)$$

où R doit être une constante parce que le premier reste est de degré zéro en X_1 , le second est de degré zéro en X_1 et X_2 , etc. Afin d'identifier cette constante, nous appliquons l'égalité (6.260) à $(a_1, \dots, a_n)$ et en nous rappelant que $P \in \ker(\phi)$ nous obtenons

$$0 = P(a_1, \dots, a_n) = R, \quad (6.261)$$

donc $R = 0$ et $P = (X_1 - a_1)Q_1 + \cdots + (X_n - a_n)Q_n$, c'est-à-dire $P \in J$. Nous avons donc $\ker(\phi) \subset J$. Par ailleurs $J \subset \ker(\phi)$ est évident, donc $J = \ker(\phi)$.

Vu que J est le noyau de l'application $\mathbb{K}[X_1, \dots, X_n] \rightarrow \mathbb{K}$, nous avons

$$\frac{\mathbb{K}[X_1, \dots, X_n]}{J} = \mathbb{K}. \quad (6.262)$$

Donc J est un idéal maximal parce que tout polynôme n'étant pas dans J doit avoir un terme indépendant non nul et donc être dans $\mathbb{K}$ vis à vis du quotient $\mathbb{K}[X_1, \dots, X_n]/J$.

Nous montrons maintenant l'implication inverse. Nous supposons que I est un idéal maximum et nous montrons qu'il doit être égal à J (pour un certain choix de $a_1, \dots, a_n$).

Le quotient

$$\frac{\mathbb{K}[X_1, \dots, X_n]}{I} \quad (6.263)$$

est une $\mathbb{K}$ -algèbre de type fini (définition 6.161). De plus c'est un corps par la proposition 3.50. C'est donc une extension algébrique finie de $\mathbb{K}$ par le théorème 6.162. Mais $\mathbb{K}$ étant algébriquement clos, il est sa propre et unique extension algébrique ; nous en déduisons que

$$\frac{\mathbb{K}[X_1, \dots, X_n]}{I} = \mathbb{K}. \quad (6.264)$$

Donc pour tout $1 \leq i \leq n$, il existe $a_i \in \mathbb{K}$ tel que $X_i - a_i \in I$, sinon le monôme X_i ne se projetterait pas sur un élément dans $\mathbb{K}$ dans le quotient. Cela prouve que J est contenu dans I ; par maximalité nous avons donc $I = J$. $\square$

Corolaire 6.164.

Soit $\mathbb{K}$ un corps algébriquement clos et I , un idéal de $\mathbb{K}[X_1, \dots, X_n]$. Si nous notons

$$V(I) = \{x \in \mathbb{K}^n \text{ tel que } P(x_1, \dots, x_n) = 0\} \quad (6.265)$$

l'ensemble des racines communes à tous les éléments de I , on a $V(I) = \emptyset$ si et seulement si $I = \mathbb{K}[X_1, \dots, X_n]$.

Démonstration. Si $I = \mathbb{K}[X_1, \dots, X_n]$ en particulier $1 \in I$ et nous avons évidemment $V(I) = \emptyset$. Le sens difficile est l'autre sens.

Supposons que $I \neq \mathbb{K}[X_1, \dots, X_n]$ et que K est un idéal maximum contenu dans I . Nous savons déjà par le théorème 6.163 que K est de la forme $K = (X_1 - a_1, \dots, X_n - a_n)$. Un élément de I est dans K , donc si $P \in I$ nous avons

$$P(a_1, \dots, a_n) = 0, \quad (6.266)$$

c'est-à-dire que $(a_1, \dots, a_n) \in V(I)$ et donc que $V(I) \neq \emptyset$. $\square$

6.6 Polynômes symétriques et alternés

6.6.1 Polynômes symétriques, alternés ou semi-symétriques

Nous rappelons que le groupe symétrique S_n agit sur l'anneau des polynômes de n variables sur l'anneau A par le lemme 1.247.

Définition 6.165.

Un polynôme Q en n indéterminées est

- (1) **symétrique** si $Q = \sigma \cdot Q$ pour tout $\sigma \in S_n$;
- (2) **alterné** si $\sigma \cdot Q = \epsilon(\sigma)Q$ pour tout $\sigma \in S_n$;
- (3) **semi-symétrique** si $\sigma \cdot Q = Q$ pour tout $\sigma \in A_n$

Le polynôme $T_1 + T_2$ est symétrique ; le polynôme $T_1 + T_2^2$ ne l'est pas.

6.6.2 Polynôme symétrique élémentaire

Définition 6.166.

Le k -ième **polynôme symétrique élémentaire** à n inconnues est le polynôme

$$\sigma_k(T_1, \dots, T_n) = \sum_{s \in F_k} \prod_{i=1}^k T_{s(i)} \quad (6.267)$$

où F_k est l'ensemble des fonctions strictement croissantes $\{1, 2, \dots, k\} \rightarrow \{1, 2, \dots, n\}$.

Une autre façon de décrire ces polynômes élémentaires est

$$\sigma_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} X_{i_1} \dots X_{i_k}. \quad (6.268)$$

Par exemple

$$\sigma_1(T_1, \dots, T_n) = T_1 + T_2 + \dots + T_n \quad (6.269a)$$

$$\sigma_2(T_1, \dots, T_n) = T_1 T_2 + \dots + T_1 T_n + T_2 T_3 + \dots + T_2 T_n + \dots + T_{n-1} T_n \quad (6.269b)$$

$$\sigma_n(T_1, \dots, T_n) = T_1 \dots T_n. \quad (6.269c)$$

En particulier, $\sigma_2(x, y, z) = xy + yz + xz$.

Théorème 6.167 ([144]).

Si Q est un polynôme symétrique en $T_1, \dots, T_n$, alors il existe un et un seul polynôme P en n indéterminées tel que

$$Q(T_1, \dots, T_n) = P(\sigma_1(T_1, \dots, T_n), \dots, \sigma_n(T_1, \dots, T_n)). \quad (6.270)$$

Exemple 6.168.

Nous voulons décomposer $P(x, y, z) = x^3 + y^3 + z^3$ en polynômes symétriques élémentaires, c'est-à-dire en

$$\begin{cases} \sigma_1 = x + y + z & (6.271a) \\ \sigma_2 = xy + xz + yz & (6.271b) \\ \sigma_3 = xyz. & (6.271c) \end{cases}$$

Étant donné que P est de degré 3, les seules combinaisons des σ_i qui peuvent intervenir sont σ_1^3 , $\sigma_1 \sigma_2$ et σ_3 . Étant donné que dans P le coefficient de x^3 est un, il est obligatoire d'avoir un coefficient 1 devant σ_1^3 . Nous le calculons :

```

-----
| Sage Version 4.8, Release Date: 2012-01-20                               |
| Type notebook() for the GUI, and license() for information.             |
-----

sage: var('x,y,z')
(x, y, z)
sage: P=x**3+y**3+z**3
sage: S1=x+y+z
sage: S2=x*y+x*z+y*z
sage: S3=x*y*z
sage: (S1**3).expand()
x^3 + 3*x^2*y + 3*x^2*z + 3*x*y^2 + 6*x*y*z + 3*x*z^2 + y^3
      + 3*y^2*z + 3*y*z^2 + z^3
sage: (S1**3-P).expand()
3*x^2*y + 3*x^2*z + 3*x*y^2 + 6*x*y*z + 3*x*z^2 + 3*y^2*z + 3*y*z^2
x^3 + 3*x^2*y + 3*x^2*z + 3*x*y^2 + 6*x*y*z + 3*x*z^2
      + y^3 + 3*y^2*z + 3*y*z^2 + z^3

```

Dans la différence $\sigma_1^3 - P$ nous voyons que le terme en xyz est $6xyz$; par conséquent nous savons que le coefficient de σ_3 sera -6 . Il nous reste :

```

sage: (S1**3+6*S3-P).expand()
3*x^2*y + 3*x^2*z + 3*x*y^2 + 12*x*y*z + 3*x*z^2 + 3*y^2*z + 3*y*z^2

```

que nous identifions facilement avec $3\sigma_1\sigma_2$. Nous avons donc

$$P = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3. \quad (6.272)$$

△

Lemme 6.169 ([90]).

Soit $\mathbb{K}$ une extension de degré δ de $\mathbb{Q}$ et $P \in \mathbb{K}[T_1, \dots, T_m]$. Alors il existe $\bar{P} \in \mathbb{Q}[T_1, \dots, T_m]$ tel que

- (1) $\deg \bar{P} = \delta \deg(P)$
- (2) pour tout $(z_1, \dots, z_m) \in \mathbb{C}^m$ tel que $P(z_1, \dots, z_m) = 0$, on a $\bar{P}(z_1, \dots, z_m) = 0$.

Démonstration. En vertu de la proposition 6.155 et du corolaire 6.156, $\mathbb{K}$ est une extension séparable de $\mathbb{Q}$, et donc vérifie le théorème de l'élément primitif (6.158). Il existe $\theta \in \mathbb{K}$ tel que $\mathbb{K} = \mathbb{Q}(\theta)$. Soit $P_\theta \in \mathbb{Q}[X]$ le polynôme minimal de θ . L'extension $\mathbb{K}$ étant de degré δ , et θ étant un générateur, une base de $\mathbb{K}$ comme espace vectoriel sur $\mathbb{Q}$ est

$$\{1, \theta, \dots, \theta^{\delta-1}\}. \quad (6.273)$$

Mais par ailleurs la proposition 6.90(2) nous indique qu'une base de $\mathbb{Q}(\theta)$ sur $\mathbb{Q}$ est donnée par

$$\{1, \theta, \dots, \theta^{n-1}\} \quad (6.274)$$

où n est le degré de P_θ . Donc P_θ est de degré δ . Nous nommons $\theta_1, \dots, \theta_\delta$ les racines de P_θ dans un corps de décomposition. Ici nous notons $\theta = \theta_1$ et nous ne prétendons pas que $\theta_k \in \mathbb{K}$. Notons que ces θ_i sont toutes des racines simples de P_θ , sinon nous aurions un facteur irréductible $(X - \theta_k)^2$, et P_θ ne serait pas irréductible sur $\mathbb{Q}$.

Soit σ_k le morphisme canonique

$$\begin{aligned} \sigma_k: \mathbb{Q}(\theta) &\rightarrow \mathbb{Q}(\theta_k) \\ \sum_i q_i \theta^i &\mapsto \sum_i q_i \theta_k^i \end{aligned} \quad (6.275)$$

Nous avons $\sigma_1: \mathbb{K} \rightarrow \mathbb{K}$ qui est l'identité.

Notons N le degré du polynôme $P \in \mathbb{K}[T_1, \dots, T_m]$ dont il est question dans l'énoncé. Nous le décomposons alors en

$$P = \sum_{l=0}^N \sum_{i=1}^m c_{il} T_i^l \quad (6.276)$$

avec $c_{il} \in \mathbb{K}$. Nous voyons $c_{i\cdot}$ comme un élément de $\mathbb{K}^m$ et donc nous écrivons⁵⁷

$$P = \sum_{l=0}^N \sum_{i=1}^m c_l(\theta)_i T_i^l \quad (6.277)$$

où $c_l \in \mathbb{Q}[X]^m$. Nous pouvons choisir $\deg(c_l) < \delta$ parce que les puissances plus grandes de θ ne génèrent rien de nouveau.

Nous posons aussi

$$P^{\sigma_k} = \sum_{l,i} c_l(\theta_k)_i T_i^l \in \mathbb{Q}(\theta_k)[T_1, \dots, T_m], \quad (6.278)$$

et $\bar{P} = PP^{\sigma_2} \dots P^{\sigma_k}$. Le coefficient de T_i^l dans $\bar{P}$ est

$$\bar{c}_l(\theta_1, \dots, \theta_\delta)_i = \sum_{l_1 + \dots + l_\delta = l} c_{l_1}(\theta_1)_i \dots c_{l_\delta}(\theta_\delta)_i. \quad (6.279)$$

Ce dernier est un polynôme en les θ_k à coefficients dans $\mathbb{Q}$. Qui plus est, c'est un polynôme symétrique. En effet un terme contenant $\theta_k^a \theta_l^b$ provenant de $c_{l_i}(\theta_k) c_{l_j}(\theta_l)$ a un terme correspondant $\theta_k^b \theta_l^a$ provenant de $c_{l_j}(\theta_k) c_{l_i}(\theta_l)$.

C'est donc le moment d'utiliser le théorème 6.167 à propos des polynômes symétriques élémentaires qui nous dit que les coefficients de $\bar{P}$ sont en réalité des polynômes en ceux de P_θ qui sont dans $\mathbb{Q}$. Donc $\bar{P} \in \mathbb{Q}[T_1, \dots, T_m]$. Par ailleurs nous avons que

$$\deg(\bar{P}) = \delta \deg(P) \quad (6.280)$$

parce que $\bar{P}$ est le produit de δ « copies » de P . De plus $P = P^{\sigma_1}$ divise $\bar{P}$ donc on a bien que si $P(z) = 0$ alors $\bar{P}(z) = 0$. Le polynôme $\bar{P}$ est celui que nous cherchions. $\square$

6.6.3 Relations coefficients racines

Théorème 6.170 (Relations coefficients-racines).

Soit le polynôme $P = a_n X^n + \dots + a_1 X + a_0$ et r_i ses n racines. Alors nous avons pour chaque $1 \leq k \leq n$ la relation

$$\sigma_k(r_1, \dots, r_n) = (-1)^k \frac{a_{n-k}}{a_n} \quad (6.281)$$

où σ_k est le k^{e} polynôme symétrique défini en 6.166.

Exemple 6.171.

Soit le polynôme

$$P(x) = x^3 + 2x^2 + 3x + 4 \quad (6.282)$$

et ses racines que nous nommons a, b, c . Nous voudrions calculer $a^2 + b^2 + c^2$. D'abord nous décomposons $Q(a, b, c) = a^2 + b^2 + c^2$ en polynômes symétriques élémentaires : $Q(a, b, c) = \sigma_1(a, b, c)^2 - 2\sigma_2(a, b, c)$.

Mais les relations coefficients-racines⁵⁸ nous donnent $\sigma_1(a, b, c) = -2$ et $\sigma_2(a, b, c) = 3$, donc

$$a^2 + b^2 + c^2 = (-2)^2 - 2 \cdot 3 = -2. \quad (6.283)$$

Cela nous assure déjà qu'au moins une des solutions n'est pas réelle.

Nous pouvons en avoir une vérification directe en calculant explicitement les racines (ce qui est possible pour le degré 3) :

⁵⁷. Il me semble qu'il manque la somme sur i dans [90].

⁵⁸. Théorème 6.170

```

1 sage: P(x)=x**3+2*x**2+3*x+4
2 sage: S=solve( P(x)==0,x )
3 sage: sols=[ s.rhs() for s in S ]
4 sage: Q=[ s**2 for s in sols ]
5 sage: s=sum(Q)
6 sage: s.simplify_full()
7 -2

```

tex/frido/VAYVmNRpolynomeSym.py

Notez qu'il faut un peu chipoter pour isoler les solutions depuis la réponse de la fonction `solve`. $\triangle$

En suivant le même cheminement que dans l'exemple, si P est un polynôme de degré n et si r_i sont ses racines, il est facile de calculer $Q(r_1, \dots, r_n)$ pour n'importe quel polynôme symétrique Q

Proposition 6.172 (Annulation de fonctions polynomiales[145]).

Soit $\mathbb{K}$ un corps et P un polynôme à n indéterminées. Nous supposons que P s'annule sur un ensemble de la forme $A_1 \times \dots \times A_n$ avec $\text{Card}(A_j) > \deg_{X_j}(P)$ pour tout j . Alors $P = 0$.

De plus si $P = 0$ alors tous ses coefficients sont nuls⁵⁹.

Démonstration. Nous prouvons le résultat par récurrence sur le nombre n d'indéterminées. Si $n = 1$, cela est le théorème 6.103. Nous classons les monômes du polynôme P par ordre de puissance de X_n et nous le factorisons :

$$P = \sum_{i=1}^m P_i X_n^i \quad (6.284)$$

avec $P_i \in \mathbb{K}[X_1, \dots, X_{n-1}]$. Soit $(a_1, \dots, a_{n-1}) \in A_1 \times \dots \times A_{n-1}$ et posons

$$Q(T) = P(a_1, \dots, a_{n-1}, T) = \sum_{i=1}^m P_i(a_1, \dots, a_{n-1}) T^i. \quad (6.285)$$

Le polynôme Q s'annule sur A_n avec $\deg(Q) = \deg_{X_n}(P) < \text{Card}(A_n)$ et le théorème 6.103 nous donne $Q = 0$. Or les coefficients des différentes puissances de T dans $Q(T)$ sont les $P_i(a_1, \dots, a_{n-1})$; ils sont donc nuls.

Nous avons montré que le polynôme P_i s'annule pour tout élément de $A_1 \times \dots \times A_{n-1}$, mais nous avons

$$\deg_{X_j}(P_i) \leq \deg_{X_j} P < \text{Card}(A_j), \quad (6.286)$$

donc l'hypothèse de récurrence donne $P_i = 0$. Par suite, $P = 0$ également. $\square$

6.7 Minuscule morceau sur la théorie de Galois

Vous trouverez des détails et des preuves à propos de la théorie de Galois dans [146, 76].

Définition 6.173.

Soit $\mathbb{K}$, un corps.

Le **groupe de Galois** d'une extension $\mathbb{L}$ de $\mathbb{K}$ est le groupe des automorphismes de $\mathbb{L}$ laissant $\mathbb{K}$ invariant.

Le groupe de Galois d'un polynôme sur $\mathbb{K}$ est le groupe de Galois de son corps de décomposition sur $\mathbb{K}$.

59. L'intérêt de cela est qu'un polynôme de $\mathbb{Z}[X_1, \dots, X_n]$ peut s'évaluer sur un élément de n'importe quel corps ; il restera le polynôme nul.

Définition 6.174.

Des éléments $b_1, \dots, b_n$ d'une extension de $\mathbb{K}$ sont **algébriquement indépendants** si ils ne satisfont à aucune relation du type

$$\sum \alpha_{i_1 \dots i_n} b_1^{i_1} \dots b_n^{i_n} = 0 \quad (6.287)$$

avec $\alpha_{i_1 \dots i_n} \in \mathbb{K}$.

Nous disons que l'équation

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0 \quad (6.288)$$

est l'**équation générale** de degré n si les coefficients a_i sont algébriquement indépendants sur $\mathbb{K}$.

Théorème 6.175.

Le groupe de Galois d'un polynôme de degré n est isomorphe au groupe symétrique S_n .

Corolaire 6.176 ([147]).

L'équation générale de degré n est résoluble par radicaux si et seulement si $n \leq 5$.

Chapitre 7

Topologie générale

7.1 Éléments généraux de topologie

7.1.1 Définitions et propriétés de base

Définition 7.1 ([148]).

Soit X , un ensemble et $\mathcal{T}$, une partie de l'ensemble de ses parties qui vérifie les propriétés suivantes.

- (1) Les ensembles $\emptyset$ et X sont dans $\mathcal{T}$,
- (2) Une union quelconque¹ d'éléments de $\mathcal{T}$ est dans $\mathcal{T}$.
- (3) Une intersection finie d'éléments de $\mathcal{T}$ est dans $\mathcal{T}$.

Un tel choix $\mathcal{T}$ de sous-ensembles de X est une **topologie** sur X , et les éléments de $\mathcal{T}$ sont appelés des **ouverts**. On dit aussi que $(X, \mathcal{T})$ (voire simplement X lorsqu'il n'y a pas d'ambiguïté) est un **espace topologique**.

Deux espaces topologique sont isomorphes quand il existe une bijection continue d'inverse continue. Nous verrons ça en la définition 7.90.

7.1.2 Base de topologie

Proposition-Définition 7.2 (Base de topologie[149, 150]).

Soit un espace topologique $(X, \mathcal{T})$. Soit une partie $\mathcal{B}$ de $\mathcal{T}$. Les propriétés suivantes sont équivalentes :

- (1) Tout élément de $\mathcal{T}$ est une réunion d'éléments de $\mathcal{B}$.
- (2) Pour tout $x \in X$ et pour tout ouvert $\mathcal{O}$ contenant x , il existe $B \in \mathcal{B}$ tel que

$$x \in B \subset \mathcal{O}. \quad (7.1)$$

Une partie $\mathcal{B}$ de $\mathcal{T}$ qui vérifie ces propriétés est une **base de topologie** pour X .

Démonstration. En deux parties.

(1) implique (2) Soient $x \in X$ et $\mathcal{O}$ un ouvert contenant x . Étant donné que $\mathcal{O}$ est une réunion d'éléments de $\mathcal{B}$, il y a au moins un $A \in \mathcal{B}$ contenant x . Ce A vérifie $x \in A \subset \mathcal{O}$.

(2) implique (1) Soit $\mathcal{O}$ un ouvert de X ; pour chaque $x \in \mathcal{O}$ nous considérons un ouvert $B(x) \in \mathcal{B}$ tel que $x \in B(x) \subset \mathcal{O}$. Nous avons alors $\mathcal{O} = \bigcup_{x \in \mathcal{O}} B(x)$.

□

1. Par « quelconque » nous entendons vraiment quelconque : c'est-à-dire indicée par un ensemble qui peut autant être $\mathbb{N}$ que $\mathbb{R}$ qu'un ensemble encore considérablement plus grand.

7.1.3 Fermés

Définition 7.3.

Si X est un espace topologique, un sous-ensemble F de X est dit **fermé** si son complémentaire, F^c , est ouvert.

Définition 7.4.

Si $a \in X$, on dit que $V \subset X$ est un **voisinage** de a s'il existe un ouvert $\mathcal{O} \in \mathcal{T}$ tel que $a \in \mathcal{O}$ et $\mathcal{O} \subset V$.

Définition 7.5 (Base de voisinage[151]).

Soient un espace topologique X ainsi que $a \in X$. Un ensemble $\{U_i\}_{i \in I}$ de voisinages de a est une **base de voisinages** de a si pour tout voisinage V de a , il existe $k \in I$ tel que $U_k \subset V$.

Lemme 7.6.

Union et intersection de fermés.

- (1) Une intersection quelconque de fermés est fermée.
- (2) Une union finie de fermés est fermée.

Démonstration. Soit $\{F_i\}_{i \in I}$ un ensemble de fermés ; nous avons

$$\left(\bigcap_{i \in I} F_i \right)^c = \bigcup_{i \in I} F_i^c. \quad (7.2)$$

Le membre de droite est une union d'ouverts, c'est donc un ouvert ; donc l'intersection qui apparaît dans le membre de gauche est le complémentaire d'un ouvert : c'est donc un fermé.

De la même manière, le complémentaire d'une union finie de fermés est une intersection finie de complémentaires de fermés, et est donc ouvert². $\square$

Dans un espace topologique, nous avons une caractérisation très importante des ouverts.

Théorème 7.7.

Une partie d'un espace topologique est ouverte si et seulement si elle contient un ouvert autour de chacun de ses éléments.

Démonstration. Soit X un espace topologique et $A \subset X$. Le sens direct est évident : A lui-même est un ouvert autour de $x \in A$, qui est inclus dans A .

Pour le sens inverse, nous supposons que A contienne un ouvert autour de chacun de ses points. Pour chaque $x \in A$, choisissons $\mathcal{O}_x \subset A$ un ouvert autour de x . Alors,

$$A = \bigcup_{x \in A} \mathcal{O}_x \quad (7.3)$$

en effet, d'une part, $A \subset \bigcup_{x \in A} \mathcal{O}_x$ parce que chaque élément x de A est dans le $\mathcal{O}_x$ correspondant, par construction ; et d'autre part, $\bigcup_{x \in A} \mathcal{O}_x \subset A$ parce que chacun des $\mathcal{O}_x$ est inclus dans A .

Ainsi, A est égal à une union d'ouverts, cela prouve que A est un ouvert. $\square$

Le lemme 7.132 est une version particulière de celui-ci, pour l'espace topologique $\mathbb{R}$. Une autre application typique est la proposition 7.2 et le théorème 7.79.

7.1.4 Quelques exemples

7.1.4.1 Une première vague

Exemple 7.8.

Pour un ensemble X quelconque, on considère l'ensemble $\mathcal{T} = \{\emptyset; X\}$. Avec cet ensemble, on confère à X une structure d'espace topologique - même si elle nous apprend peu de choses... La topologie ainsi posée sur X est appelée **topologie grossière**. $\triangle$

2. Un bon exercice est d'écrire ces unions et intersections, pour se convaincre que ça fonctionne.

Exemple 7.9.

Pour un ensemble X quelconque, on considère l'ensemble $\mathcal{T}$ constitué de toutes les parties de X . Avec cet ensemble, on confère à nouveau une structure d'espace topologique à X ; toutes les parties sont des ouverts, et aussi des fermés. La topologie ainsi posée sur X est appelée **topologie discrète**. $\triangle$

Exemple 7.10 (Toutes les topologies d'un ensemble à 3 éléments).

On pose $X = \{1, 2, 3\}$. Alors on peut munir X de 29 topologies différentes[152] ; saurez-vous les retrouver toutes ? $\triangle$

7.1.4.2 Topologie engendrée**Proposition-Définition 7.11** (Topologie engendrée, prébase[153]).

Soient un ensemble X et $\mathcal{T}_0$ un ensemble de parties de X . Nous définissons $\tau(\mathcal{T}_0)$ comme étant l'union quelconque d'intersections finies d'éléments de $\mathcal{T}_0$.

Plus précisément, nous faisons les constructions suivantes :

- (1) Nous notons $\{\mathcal{O}_i\}_{i \in I}$ les éléments de $\mathcal{T}_0$ indexés par l'ensemble I .
- (2) Soit $B(\mathcal{T}_0)$ l'ensemble des intersections finies d'éléments de $\mathcal{T}_0$:

$$B(\mathcal{T}_0) = \left\{ \bigcap_{j \in J} \mathcal{O}_j \right\}_{J \text{ fini dans } I} \quad (7.4)$$

où nous convenons que $\bigcap_{j \in \emptyset} \mathcal{O}_j = X$ ³.

- (3) Soit A un ensemble qui indexe $B(\mathcal{T}_0)$:

$$B(\mathcal{T}_0) = \{B_\alpha\}_{\alpha \in A}. \quad (7.5)$$

- (4) Nous posons

$$\tau(\mathcal{T}_0) = \left\{ \bigcup_{\alpha \in S} B_\alpha \right\}_{S \subset A}. \quad (7.6)$$

Alors $\tau(\mathcal{T}_0)$ est une topologie sur X , qu'on appelle **topologie engendrée** par $\mathcal{T}_0$. La partie $\mathcal{T}_0$ est appelée **prébase** de la topologie $\tau(\mathcal{T}_0)$.

Démonstration. Nous devons montrer les différents points de la définition 7.1 d'une topologie.

- (1) L'ensemble vide est dans $\tau(\mathcal{T}_0)$ parce que $\emptyset = \bigcup_{\alpha \in \emptyset} B_\alpha$. L'ensemble X est également dans $\tau(\mathcal{T}_0)$ parce que $X \in B(\mathcal{T}_0)$.
- (2) Soient $\{D_l\}_{l \in L}$ des éléments de $\tau(\mathcal{T}_0)$ indexés par un ensemble L . Pour chaque l nous avons un ensemble $S \subset A$ tel que $D_l = \bigcup_{\alpha \in S_l} B_\alpha$. En posant $S = \bigcup_{l \in L} S_l$ nous avons

$$\bigcup_{l \in L} D_l = \bigcup_{\alpha \in S} B_\alpha \in \tau(\mathcal{T}_0). \quad (7.7)$$

Donc $\tau(\mathcal{T}_0)$ est stable par union quelconque.

- (3) Soient D_1 et D_2 des éléments de $\tau(\mathcal{T}_0)$. Nous posons $D_i = \bigcup_{\alpha \in S_i} B_\alpha$. Alors nous avons

$$\bigcup_{\alpha \in S_1} B_\alpha \cap \bigcup_{\beta \in S_2} B_\beta = \bigcup_{\alpha, \beta \in S_1 \times S_2} (B_\alpha \cap B_\beta). \quad (7.8)$$

Mais B_α et B_β sont dans $B(\mathcal{T}_0)$. Donc $B_\alpha \cap B_\beta \in B(\mathcal{T}_0)$. Donc (7.8) est un union d'éléments de $B(\mathcal{T}_0)$.

Au final nous avons prouvé que $\tau(\mathcal{T}_0)$ est une topologie sur X . $\square$

3. Bref, nous mettons X dans $B(\mathcal{T}_0)$.

Lemme 7.12.

Soient un ensemble X et un ensemble $\mathcal{T}_0$ de parties de X . Toute topologie sur X contenant $\mathcal{T}_0$ contient $\tau(\mathcal{T}_0)$.

Démonstration. Soit une topologie μ sur X contenant $\tau(\mathcal{T}_0)$. Vu que μ est une topologie, les intersections finies d'éléments de μ sont dans μ , donc, en suivant les notations de 7.11, $B(\mathcal{T}_0) \subset \mu$.

Vu que toutes les unions d'éléments de μ sont dans μ , l'inclusion de $B(\mathcal{T}_0)$ dans μ implique celle de $\tau(\mathcal{T}_0)$. $\square$

Dès que nous avons une topologie nous avons une notion de convergence de suite.

Définition 7.13 (Convergence de suite).

Une suite (x_n) d'éléments de E **converge** vers un élément y de E si pour tout ouvert $\mathcal{O}$ contenant y , il existe un $K \in \mathbb{N}$ tel que $k > K$ implique $x_k \in \mathcal{O}$.

La proposition suivante montre que vérifier la convergence d'une suite sur une prébase suffit pour vérifier la convergence.

Proposition 7.14.

Soit $\mathcal{T}_0$ un ensemble de parties de l'ensemble X . Soient une suite (x_n) dans X ainsi que $x \in X$. Nous supposons que la suite (x_n) satisfasse la propriété suivante : pour tout $A \in \mathcal{T}_0$ tel que $x \in A$, il existe $K \in \mathbb{N}$ tel que $k \geq K$ implique $x_k \in A$.

Alors nous avons la convergence de suite⁴

$$x_n \xrightarrow{(X, \tau(\mathcal{T}_0))} x. \quad (7.9)$$

Démonstration. Nous considérons la topologie $\tau(\mathcal{T}_0)$ sur X . Soit un ouvert $\mathcal{O}$ contenant x . Nous le décomposons en suivant (à l'envers) la construction de la définition 7.11 :

$$\mathcal{O} = \bigcup_{\alpha \in S} B_\alpha \quad (7.10)$$

avec $B_\alpha \in B(\mathcal{T}_0)$. Donc pour chaque α , il existe un ensemble fini J_α tel que

$$B_\alpha = \bigcap_{j \in J_\alpha} A_j \quad (7.11)$$

avec $A_j \in \mathcal{T}_0$. Vu que $x \in \mathcal{O}$, nous avons un α_0 tel que $x \in B_{\alpha_0}$. Donc $x \in A_j$ pour tous les $j \in J_{\alpha_0}$.

Pour chaque $j \in J_{\alpha_0}$, il existe $K_j \in \mathbb{N}$ tel que $k \geq K_j$ implique $x_k \in A_j$. Vu que J_{α_0} est un ensemble fini, nous pouvons poser $K = \max_{j \in J_{\alpha_0}} K_j$.

Maintenant, si $k \geq K$, nous avons $x_k \in A_j$ pour tout j , et donc $x_k \in B_{\alpha_0}$. Par conséquent aussi $x_k \in \mathcal{O}$. $\square$

7.1.5 Topologie produit**Définition 7.15** (Produit d'espaces topologiques, thème 9).

Soient $\{(X_i, \tau_i)\}_{i=1, \dots, n}$ des espaces topologiques. Leur **produit** est l'ensemble

$$X = \prod_{i=1}^n X_i \quad (7.12)$$

muni de la topologie obtenue en disant que $U \subset X$ est un ouvert si et seulement si pour tout $x \in U$, il existe $U_i \in \tau_i$ tels que

$$x \in U_1 \times \dots \times U_n \subset U. \quad (7.13)$$

4. Définition 7.13.

Proposition 7.16 (Convergence composante par composante).

Soient des espaces topologiques X_i ($i = 1, \dots, n$) et une suite $(a_k^{(1)}, \dots, a_k^{(n)})$ dans $X_1 \times \dots \times X_n$. Nous avons la convergence

$$(a_k^{(1)}, \dots, a_k^{(n)}) \xrightarrow{X_1 \times \dots \times X_n} (a^{(1)}, \dots, a^{(n)}) \quad (7.14)$$

si et seulement si $a_k^{(i)} \rightarrow a^{(i)}$ pour chaque i .

Démonstration. En deux parties.

Sens direct Soient des ouverts $\mathcal{O}_i$ autour de $a^{(i)}$ dans X_i . Vu que $\mathcal{O}_1 \times \dots \times \mathcal{O}_n$ est un ouvert autour de $(a^{(1)}, \dots, a^{(n)})$, il existe $K \in \mathbb{N}$ tel que si $k \geq K$ nous avons $(a_k^{(1)}, \dots, a_k^{(n)}) \in \mathcal{O}_1 \times \dots \times \mathcal{O}_n$. Pour ce K nous avons séparément $a_k^{(i)} \in \mathcal{O}_i$ pour chaque i .

Sens inverse Une prébase de la topologie sur $X_1 \times \dots \times X_n$ est donné par les $\mathcal{O}_1 \times \dots \times \mathcal{O}_n$ où $\mathcal{O}_i$ est un ouvert de X_i . Voir la définition 7.15 de la topologie produit et la définition 7.11 de ce qu'est une prébase.

La proposition 7.14 nous permet de ne vérifier la convergence de $(a_k^{(1)}, \dots, a_k^{(n)})$ que sur la prébase. Soit donc $\mathcal{O} = \mathcal{O}_1 \times \dots \times \mathcal{O}_n$ avec $(a^{(1)}, \dots, a^{(n)}) \in \mathcal{O}$. Vu que $(a_k^{(i)})_{k \in \mathbb{N}} \rightarrow a^{(i)}$, pour chaque i , il existe $K_i \in \mathbb{N}$ tel que si $k \geq K_i$ alors $a_k^{(i)} \in \mathcal{O}_i$.

En posant $K = \max_i(K_i)$, nous avons $(a_k^{(1)}, \dots, a_k^{(n)}) \in \mathcal{O}_1 \times \dots \times \mathcal{O}_n$ pour tout $k \geq K$.

La proposition 7.14 permet de conclure. □

7.1.5.1 Topologie induite

Proposition-Définition 7.17 (Topologie induite[154]).

Soit un espace topologique (X, τ_X) , et soit $Y \subset X$. Nous définissons

$$\tau_Y = \{Y \cap \mathcal{O} \text{ tel que } \mathcal{O} \in \tau_X\}. \quad (7.15)$$

L'ensemble τ_Y est une topologie sur Y .

Elle est la **topologie induite**.

Démonstration. Il s'agit de vérifier les conditions de la définition 7.1.

$Y \in \tau_Y$ Parce que $Y = Y \cap Y$ et que Y est un ouvert de X .

$\emptyset \in \tau_Y$ Parce que $\emptyset = Y \cap \emptyset$ et que $\emptyset$ est un ouvert de X .

Union quelconque Soient des ouverts A_i de X . Nous avons

$$\bigcup_{i \in I} Y \cap A_i = Y \cap \left(\bigcup_{i \in I} A_i \right). \quad (7.16)$$

Vu que les A_i sont des ouverts de X , leur union est encore un ouvert de X . Donc (7.16) est encore dans τ_Y .

Intersection finie Nous avons

$$\bigcap_{i \in I} Y \cap A_i = Y \cap \left(\bigcap_{i \in I} A_i \right). \quad (7.17)$$

□

Lemme 7.18 ([1]).

Soit (X, τ_X) un espace topologique et $S \subset X$, un fermé de X sur lequel nous considérons la topologie induite τ_S . Si F est un fermé de (S, τ_S) alors F est fermé de (X, τ_X) .

Démonstration. Nous savons que le complémentaire de F dans S est un ouvert de (S, τ_S) : il existe un ouvert $\Omega \in \tau_X$ tel que $S \setminus F = S \cap \Omega$. Si maintenant nous considérons le complémentaire de S dans X nous avons

$$F^c = (S \setminus F) \cup (X \setminus S) = (S \cap \Omega) \cup S^c = (S \cap \Omega) \cup (S^c \cap \Omega) \cup S^c = \Omega \cup S^c. \quad (7.18)$$

Vu que Ω et S^c sont des ouverts de X , l'union est un ouvert. Donc $F^c \in \tau_X$ et F est un fermé de X . $\square$

Lemme 7.19.

Si $B \subset A$ alors la fermeture de B pour la topologie de A (induite de X) que nous noterons $\tilde{B}$ est

$$\tilde{B} = \bar{B} \cap A \quad (7.19)$$

où $\bar{B}$ est la fermeture de B pour la topologie de X .

Démonstration. Si $a \in \bar{B} \cap A$, un ouvert de A autour de a est un ensemble de la forme $\mathcal{O} \cap A$ où $\mathcal{O}$ est un ouvert de X . Vu que $a \in \bar{B}$, l'ensemble $\mathcal{O}$ intersecte B et donc $(\mathcal{O} \cap A) \cap B \neq \emptyset$. Donc a est bien dans l'adhérence de B au sens de la topologie de A .

Pour l'inclusion inverse, soit $a \in \tilde{B}$, et montrons que $a \in \bar{B} \cap A$. Par définition $a \in A$, parce que $\tilde{B}$ est une fermeture dans l'espace topologique A . Il faut donc seulement montrer que $a \in \bar{B}$. Soit donc $\mathcal{O}$ un ouvert de X contenant a ; par hypothèse $\mathcal{O} \cap A$ intersecte B (parce que tout ouvert de A contenant a intersecte B). Donc $\mathcal{O}$ intersecte B . Cela signifie que tout ouvert (de X) contenant a intersecte B , ou encore que $a \in \bar{B}$. $\square$

Si A est un ouvert de X , on pourrait croire que la topologie induite n'a rien de spécial. Il est vrai que B sera ouvert dans A si et seulement s'il est ouvert dans X , mais certaines choses surprenantes se produisent tout de même.

Exemple 7.20.

Prenons $X = \mathbb{R}$ et $A =]0, 1[$. Si $B =]\frac{1}{2}, 1[$, alors la fermeture de B dans A sera $\tilde{B} = [\frac{1}{2}, 1[$ et non $[\frac{1}{2}, 1]$ comme on l'aurait dans $\mathbb{R}$. $\triangle$

Prendre la topologie induite de $\mathbb{R}$ vers un fermé de $\mathbb{R}$ donne des boules un peu spéciales comme le montre l'exemple suivant.

Exemple 7.21.

Quid de la boule ouverte $B(1, \epsilon)$ dans le compact ⁵ $[0, 1]$? Par définition c'est

$$B(1, \epsilon) = \{x \in [0, 1] \text{ tel que } |x - 1| < \epsilon\} =]1 - \epsilon, 1]. \quad (7.20)$$

Oui, cela est *ouvert* dans $[0, 1]$. C'est d'ailleurs un des ouverts de la topologie induite de $\mathbb{R}$ sur $[0, 1]$.

Donc pour la topologie de $[0, 1]$, toutes les boules ouvertes $B(x, \delta)$ avec $x \in [0, 1]$ sont incluses à $[0, 1]$. $\triangle$

7.1.6 Adhérence, fermeture, intérieur, point d'accumulation et isolé

Définition 7.22.

Soient un espace topologique X et une partie A de X .

- (1) Un point $x \in X$ est **intérieur** à A s'il est contenu dans un ouvert inclus dans A .
- (2) L'**intérieur** de A , notée $\text{Int}(A)$, est l'union de tous les ouverts de X contenus dans A .

Lemme 7.23.

Quelques propriétés en vrac.

- (1) L'intérieur de A est l'ensemble de tous les points intérieurs de A .

5. Définition (5).

- (2) Pour tout $A \subset X$, l'ensemble $\text{Int}(A)$ est un ouvert.
 (3) On a $\text{Int}(A) \subset A$
 (4) Nous avons $\text{Int}(A) = A$ si et seulement si A est un ouvert.

Démonstration. En plusieurs morceaux.

- (1) Si $a \in \text{Int}(A)$, alors a est dans un ouvert contenu dans A , et donc a est un point intérieur à A .
 Dans l'autre sens, si a est un point intérieur à A , alors il existe un ouvert $\mathcal{O} \subset A$ contenant a . Vu que $\mathcal{O}$ est un ouvert dans A , nous avons $\mathcal{O} \subset \text{Int}(A)$, et en particulier $a \in \text{Int}(A)$.
 (2) C'est une union d'ouverts.
 (3) L'ensemble $\text{Int}(A)$ est une union d'ensembles contenus dans A .
 (4) Supposons que $\text{Int}(A) = A$. Vu que $\text{Int}(A)$ est ouvert (point (3)), A est ouvert aussi.
 Dans l'autre sens, nous supposons que A est ouvert. Vu que A est un ouvert contenu dans A , nous avons $A \subset \text{Int}(A)$. Mais comme $\text{Int}(A) \subset A$, nous avons l'égalité.

□

7.1.6.1 Adhérence et fermeture

Disons-le tout de suite : « adhérence » et « fermeture » sont synonymes. Dans le Frido, nous allons nous évertuer à utiliser le mot « adhérence » et la notation $\text{Adh}(A)$ au lieu de $\bar{A}$ que l'on rencontre assez souvent. Le fait que est $\bar{z}$ est le conjugué complexe de z . Dans certains cas, ça peut mener à des confusions.

Définition 7.24.

Soient un espace topologique X et une partie A de X . Un point $x \in X$ est **adhérent** à A si tout ouvert de X contenant x a une intersection non vide avec A . L'ensemble des points d'adhérence de A est noté $\text{Adh}(A)$.

Lemme 7.25.

L'adhérence de A est l'intersection de tous les fermés de X contenant A .

Par ailleurs, nous avons le lien

$$(\text{Int}(A))^c = \text{Adh}(A^c). \quad (7.21)$$

Démonstration. Commençons par prouver la dernière égalité d'ensembles. On a les équivalences entre les éléments suivants, pour tout $x \in X$:

- x n'est pas dans $\text{Int}(A)$;
- il n'y a aucun ouvert contenant x et inclus dans A ;
- tout ouvert contenant x a une intersection non-vide avec A^c ;
- x est dans $\overline{A^c}$.

Nous allons à présent montrer l'égalité d'ensembles $\text{Adh}(A) = \bar{A}$ en prouvant la double inclusion par contraposée.

Si $x \in \bar{A}$ alors $x \in \text{Adh}(A)$ Si x n'est pas dans $\bar{A}$ alors nous avons un fermé F contenant A et pas x . Le complémentaire F^c est un ouvert qui contient x et dont l'intersection avec A est vide. Donc x n'est pas dans $\text{Adh}(A)$.

Si $x \in \bar{A}$ alors $x \in \text{Adh}(A)$ Si x n'est pas dans $\text{Adh}(A)$ alors il existe un ouvert $\mathcal{O}$ contenant x et n'intersectant pas A . Le complémentaire $\mathcal{O}^c$ est un fermé qui contient A et qui ne contient pas x .

Vu que $\bar{A}$ est l'intersection de tous les fermés contenant A , nous avons $\bar{A} \subset \mathcal{O}^c$ et donc x n'est pas dans $\bar{A}$.

□

Remarque 7.26.

Comme corolaire du lemme précédent, et grâce aux remarques faites pour les intérieurs, on obtient que pour $A \subset X$:

- (1) l'ensemble $\bar{A}$ est fermé : c'est en effet le complémentaire d'un ouvert, précisément l'intérieur de A^c ;
- (2) A est fermé si et seulement si $\bar{A} = A$: en effet, A est fermé si et seulement si A^c est ouvert, si et seulement si l'intérieur de A^c est A^c lui-même ; or, l'intérieur de A^c est le complémentaire de $\bar{A}$ par le lemme 7.25, si bien que A est fermé si et seulement si $(\bar{A})^c = A^c$, ou encore... ce qu'on affirmait au début.

Définition 7.27.

Soit X un espace topologique. Un sous-ensemble A de X est **dense** dans X si $\bar{A} = X$.

7.1.6.2 Frontière**Définition 7.28.**

Soit X un espace topologique, et $A \subset X$. La **frontière** de A , notée ∂A , est l'ensemble des points adhérents de A qui ne sont pas intérieurs à A . Ainsi,

$$\partial A = \bar{A} \setminus \text{Int}(A). \quad (7.22)$$

7.1.6.3 Points d'accumulation et isolés**Définition 7.29.**

Soient un espace topologique X et une partie A de X . Un point $s \in X$ est un **point d'accumulation** de A si tout ouvert contenant s contient au moins un élément de $A \setminus \{s\}$.

Quelle est la différence entre un point d'accumulation et un point d'adhérence ? La différence est que tous les points de A sont des points d'adhérence de A , parce que tout voisinage de $a \in A$ contient au moins a lui-même, alors que certains points de A peuvent ne pas être des points d'accumulation de A . Voir l'exemple 7.147.

Notons qu'un point d'accumulation de A dans X n'est pas spécialement dans A .

Définition 7.30.

Soient un espace topologique X et une partie A de X . Un point $s \in A$ est un **point isolé** de A si il existe un voisinage ouvert $\mathcal{O}$ de s dans X tel que $A \cap \mathcal{O} = \{s\}$.

7.2 Suites et convergence**7.31.**

À propos de notations. La pire notation possible pour une suite est $(a_n)_n$. Mais que vient faire le second indice n ? Il peut être raisonnable d'écrire $(a_n)_{n \in I}$ lorsqu'on veut dire dans quel ensemble se déplace n . Si nous parlons de *suite*, il faut une sérieuse raison de prendre autre chose que $\mathbb{N}$ comme ensemble d'indices.

Une suite étant une fonction, de la même façon qu'on ne devrait pas dire « la fonction $f(x)$ », mais « la fonction f » ou « la fonction $x \mapsto f(x)$ », nous devrions simplement écrire a pour désigner la suite dont les éléments sont a_n .

Par conséquent, il est parfaitement légal, et même conseillé, d'écrire « $a + b$ » pour la somme des suites a et b . Et il est tout aussi légal d'écrire « $\lim a$ » au lieu de $\lim_{n \rightarrow \infty} a_n$.

Le hic est que nous écrivons souvent x la limite de la suite $n \mapsto x_n$. Dans ce cas, nous sommes évidemment obligé d'écrire l'indice n pour parler de la suite.

Tout cela pour dire qu'il faut être souple avec les notations.

7.2.1 Convergence dans un fermé

Proposition 7.32 ([1]).

Une suite contenue dans un fermé ne peut converger que vers un élément de ce fermé.

Démonstration. Soient un espace topologique X et un fermé F dans X . Nous supposons que la suite (x_k) soit contenue dans F . Nous allons prouver qu'aucun élément de F^c ne peut être limite.

Soit $a \in F^c$. Vu que le complémentaire de F est un ouvert, et vu le théorème 7.7, il existe un ouvert $\mathcal{O}_a$ contenant a , et contenu dans F^c . Le voisinage $\mathcal{O}_a$ de a ne contient donc aucun élément de la suite (x_k) , qui ne peut donc pas converger vers a . $\square$

Corolaire 7.33.

Soit A un sous-ensemble d'un espace topologique X . Toute suite d'éléments de A qui converge, admet pour limite un élément de $\bar{A}$.

Démonstration. Une fois la suite (x_n) fixée, il suffit de remarquer que tous les x_n sont dans $\bar{A}$, et puis d'appliquer la proposition 7.32. $\square$

Lemme 7.34.

Soit $A \subset X$ muni de la topologie induite de X et (x_n) une suite dans A . Si (x_n) converge vers un élément x dans A , alors elle converge aussi vers x dans X .

Démonstration. Soit $\mathcal{O}$ un ouvert autour de x dans X . Alors $A \cap \mathcal{O}$ est un ouvert autour de x dans A et il existe $N \in \mathbb{N}$ tel que si $n \geq N$, alors $x_n \in A \cap \mathcal{O} \subset \mathcal{O}$. $\square$

7.2.2 Pour des limites uniques : séparabilité

Notons que l'on a parlé d'une limite de suite jusqu'à présent : en effet, s'il existe deux éléments distincts x et y tels que tout ouvert contenant x contient y , alors la définition 7.13 dit que toute suite convergeant vers y converge aussi vers x ...

Exemple 7.35.

Oui, il y a moyen de converger vers plusieurs points distincts si l'espace n'est pas super cool. Nous pouvons par exemple [155] considérer la droite réelle munie de sa topologie usuelle et y ajouter un point $0'$ (qui clone le réel 0) dont les voisinages sont les voisinages de 0 dans lesquels nous remplaçons 0 par $0'$. Dans cet espace, la suite $(1/n)$ converge à la fois vers 0 et $0'$.

En fait, on « voit » le problème : on ne peut pas distinguer d'un point de vue topologique le 0 et le $0'$. $\triangle$

Nous posons la définition suivante, qui nous permettra de donner une assez grande classe d'espaces topologiques dans lesquels nous avons unicité de la limite⁶.

Définition 7.36 (Espace topologique séparé).

*Si deux points distincts admettent toujours deux voisinages disjoints⁷, nous disons que l'espace est **séparé** ou **Hausdorff**.*

Attention, cette notion est à ne pas confondre avec :

Définition 7.37 (Espace topologique séparable).

*Un espace topologique est **séparable** s'il possède une partie dénombrable⁸ dense⁹.*

Proposition 7.38.

Dans un espace séparé, si une suite converge, alors sa limite est unique.

6. Voir la proposition 7.73.

7. Définition 1.3.

8. Définition 1.105.

9. Définition 7.27.

Démonstration. Supposons que la suite (x_k) converge vers deux éléments distincts x et y . L'espace étant séparé, il existe deux ouverts $\mathcal{O}_x$ et $\mathcal{O}_y$, disjoints, contenant respectivement x et y . La suite convergeant à la fois vers x et y , il existe k_x et k_y , tels que, si $k \geq \max\{k_x, k_y\}$, l'élément x_k est (à la fois) dans $\mathcal{O}_x$ et $\mathcal{O}_y$. Cela est en contradiction avec le fait que ces deux ensembles sont disjoints. $\square$

7.39.

Donc, on pourra parler, avec des espaces séparés, de « la limite d'une suite ». On notera $x_n \rightarrow a$, ou $\lim_{n \rightarrow \infty} x_n = a$, pour signifier que la suite (x_n) converge vers a .

Proposition 7.40 ([1]).

La convergence de suite pour la topologie de l'espace produit¹⁰ est équivalente à la convergence des suites « composante par composante ».

Démonstration. En deux parties

Sens direct Pour simplifier les notations, nous allons considérer le produit de deux espaces. Soit donc $(x_k, y_k) \xrightarrow{X \times Y} (x, y)$ et des ouverts $\mathcal{O}_1$ dans X autour de x et $\mathcal{O}_2$ autour de y dans Y .

La partie $\mathcal{O}_1 \times \mathcal{O}_2$ est ouverte dans $X \times Y$. Donc il existe K tel que $k > K$ implique $(x_k, y_k) \in \mathcal{O}_1 \times \mathcal{O}_2$.

Nous avons prouvé que pour tout ouvert $\mathcal{O}_1$ autour de x il existe K tel que $k > K$ implique $x_k \in \mathcal{O}_1$. Donc $x_k \xrightarrow{X} x$. Idem pour y .

Dans l'autre sens klm

$\square$

Lemme 7.41 ([1]).

Soit un espace topologique X . Soient dans X une suite (x_n) et un élément x tels que toute sous-suite de (x_n) contient une sous-suite convergente vers x . Alors $x_n \rightarrow x$.

Démonstration. Supposons que (x_n) ne converge pas vers x . Il existe alors un ouvert $\mathcal{O}$ autour de x tel que pour tout $N > 0$, il existe $n \geq N$ tel que x_n n'est pas dans $\mathcal{O}$.

Cela nous permet de construire une sous-suite de (x_n) composée d'éléments hors de $\mathcal{O}$. Aucune sous-suite de cette sous-suite ne peut converger vers x . $\square$

7.2.3 Fonctions équivalentes

Proposition-Définition 7.42 ([156]).

Soit un espace topologique X et $D \subset X$. Soient encore des fonctions $f, g: D \rightarrow \mathbb{C}$ et un point $a \in \text{Adh}(D)$ ¹¹.

Nous définissons sur $\text{Fun}(D, \mathbb{C})$ la relation $f \sim g$ lorsque qu'il existe un voisinage V de a dans X et une fonction $\alpha: V \rightarrow \mathbb{R}$ telles que

$$\begin{aligned} (1) \quad & \lim_{x \rightarrow a} \alpha(x) = 0, \\ (2) \quad & \text{pour tout } x \in (V \cap D) \setminus \{a\}, \\ & f(x) = (1 + \alpha(x))g(x). \end{aligned} \tag{7.23}$$

Cette relation est une relation d'équivalence.

Lorsque $f \sim g$, nous disons que f et g sont **équivalentes** en a .

Démonstration. Nous devons prouver les trois conditions de la définition 1.23 de relation d'équivalence.

Réflexive Il suffit de poser $\alpha(x) = 0$.

10. Définition 7.15.

11. Adhérence ou fermeture, c'est la même chose. Voir la définition 7.24 et le lemme 7.25.

Symétrique Si $f \sim g$, il existe une fonction α vérifiant ce qu'il faut telle que

$$f(x) = (1 + \alpha(x))g(x). \quad (7.24)$$

Vu que $\lim_{x \rightarrow a} \alpha(x) = 0$, il y a un voisinage de a sur lequel $|\alpha(x)| < 1$; il n'y a donc pas de problèmes de dénominateur en écrivant

$$g(x) = \frac{1}{1 + \alpha(x)} f(x). \quad (7.25)$$

Nous posons alors $\beta(x) = -\alpha(x)/(1 + \alpha(x))$. Cela vérifie

$$g(x) = (1 + \beta(x))f(x). \quad (7.26)$$

Et

$$\lim_{x \rightarrow a} \beta(x) = 0 \quad (7.27)$$

parce que le dénominateur dans β tend vers 1.

Transitive Soit $f \sim g$ et $g \sim h$. Sur un voisinage V de a nous avons

$$f(x) = (1 + \alpha(x))g(x), \quad (7.28)$$

sur un voisinage W de a nous avons

$$g(x) = (1 + \beta(x))h(x). \quad (7.29)$$

Sur le voisinage $V \cap W$ nous avons

$$f(x) = (1 + \beta(x) + \alpha(x) + (\alpha\beta)(x))h(x). \quad (7.30)$$

Donc la fonction $\gamma(x) = \beta(x) + \alpha(x) + (\alpha\beta)(x)$ fait l'affaire.

□

Notons que la notion d'équivalence de fonctions, de même que la notion de limite, ne dépend pas des valeurs exactes atteintes par les fonctions au point.

Lemme 7.43.

Si f et g sont équivalentes en a , et si g ne s'annule pas sur un voisinage de a , alors pour tout $\epsilon > 0$, il existe r tel que

$$\frac{f(x)}{g(x)} \in B(1, \epsilon) \quad (7.31)$$

pour tout $x \in B(a, r)$.

Démonstration. Nous considérons un voisinage V de a sur lequel en même temps :

- la fonction α de la définition d'équivalence est définie,
- $|\alpha(x)| < \epsilon$ pour tout $x \in V$,
- $g(x) \neq 0$, pour tout $x \in V$.

Ensuite nous considérons $r > 0$ tel que $B(a, r) \subset V$. En divisant la condition (7.23) par $g(x)$ nous trouvons

$$\frac{f(x)}{g(x)} = 1 + \alpha(x). \quad (7.32)$$

Donc

$$\left| \frac{f(x)}{g(x)} - 1 \right| = |\alpha(x)| \leq \epsilon, \quad (7.33)$$

ce qu'il fallait prouver.

□

7.3 Connexité

L'idée de la connexité, c'est de s'assurer qu'un ensemble est « d'un seul tenant ».

Définition 7.44.

Lorsque E est un espace topologique, nous disons qu'un sous-ensemble A est **non connexe** quand on peut trouver des ouverts O_1 et O_2 disjoints tels que

$$A = (A \cap O_1) \cup (A \cap O_2), \quad (7.34)$$

et tels que $A \cap O_1 \neq \emptyset$, et $A \cap O_2 \neq \emptyset$. Si un sous-ensemble n'est pas non-connexe, alors on dit qu'il est **connexe**.

Une autre façon d'exprimer la condition (7.34) est de dire que A n'est pas connexe quand il est contenu dans la réunion de deux ouverts disjoints qui intersectent tous les deux A .

Proposition-Définition 7.45 ([157]).

Soient un espace topologique E et un point $x \in E$.

- (1) La réunion de toutes les parties connexes de E contenant x est connexe.
- (2) Cette réunion est la plus grande (au sens de la relation d'inclusion) de toutes les parties connexes de E contenant x .

La réunion de toutes les parties connexes de E contenant x est nommée **composante connexe** de x dans E .

Démonstration. Pas de preuve pour l'instant. Si vous en connaissez une vous pouvez soit l'ajouter, soit me l'envoyer. $\square$

Proposition 7.46.

Soit X un espace topologique. Les conditions suivantes sont équivalentes.

- (1) L'espace X est connexe.
- (2) Si $X = A \cup B$ avec A et B fermés disjoints dans X , alors $A = \emptyset$ ou $B = \emptyset$.
- (3) Si $A \subset X$ avec A ouvert et fermé en même temps, alors $A = \emptyset$ ou $A = X$.

Nous verrons plus tard (proposition 7.94) une autre caractérisation de la connexité.

Proposition 7.47.

Si $A \subset X$ est connexe et si $A \subset B \subset \bar{A}$, alors B est connexe.

Proposition 7.48.

Stabilité de la connexité par union.

- (1) Une union quelconque de connexes ayant une intersection non vide est connexe.
- (2) Pour tout $n \in \mathbb{N}, n > 0$, si $A_1, \dots, A_n$ sont des connexes de X avec $A_i \cap A_{i+1} \neq \emptyset$, alors l'union $\bigcup_{i=1}^n A_i$ est connexe.

Démonstration. Point par point.

- (1) Soient $\{C_i\}_{i \in I}$ un ensemble de connexes et un point p dans l'intersection : $p \in \bigcap_{i \in I} C_i$. Supposons que l'union ne soit pas connexe. Alors nous considérons A et B , deux ouverts disjoints recouvrant tous les C_i et ayant chacun une intersection non vide avec l'union. Supposons pour fixer les idées que $p \in A$ et prenons $x \in B \cap \bigcup_{i \in I} C_i$. Il existe un $j \in I$ tel que $x \in C_j$. Avec tout cela nous avons
 - (1a) $C_j \subset A \cup B$ parce que $A \cup B$ recouvre tous les C_i ,
 - (1b) $C_j \cap A \neq \emptyset$ parce que p est dans l'intersection,
 - (1c) $C_j \cap B \neq \emptyset$ parce que x est dans cette intersection.
 Cela contredit le fait que C_j soit connexe.

- (2) Pour la seconde partie nous procédons de proche en proche¹². D'abord $A_1 \cup A_2$ est connexe par la première partie, ensuite $(A_1 \cup A_2) \cup A_3$ est connexe parce que les connexes $A_1 \cup A_2$ et A_3 ont un point d'intersection par hypothèse, et ainsi de suite.

□

7.4 Compacité

La compacité est le thème 12.

7.4.1 Définition et notions connexes

Soit E , un sous-ensemble de $\mathbb{R}$. Nous pouvons considérer les ouverts suivants :

$$\mathcal{O}_x = B(x, 1) \quad (7.35)$$

pour chaque $x \in E$. Évidemment,

$$E \subseteq \bigcup_{x \in E} \mathcal{O}_x. \quad (7.36)$$

Cette union contient en général de nombreuses redondances. Si par exemple $E = [-10, 10]$, l'élément $3 \in E$ est contenu dans $\mathcal{O}_{3.5}$, $\mathcal{O}_{2.7}$ et bien d'autres. Pire : même si on enlève par exemple $\mathcal{O}_2$ de la liste des ouverts, l'union de ce qui reste continue à être tout E . La question est : *est-ce qu'on peut en enlever suffisamment pour qu'il n'en reste qu'un nombre fini ?*

Définition 7.49.

Soit E , un sous-ensemble de $\mathbb{R}$. Une collection d'ouverts $\mathcal{O}_i$ est un **recouvrement** de E si $E \subseteq \bigcup_i \mathcal{O}_i$.

Définition 7.50.

Une partie A d'un espace topologique est **compacte** s'il vérifie la propriété de Borel-Lebesgue : pour tout recouvrement de A par des ouverts (c'est-à-dire une collection d'ouverts dont la réunion contient A) on peut extraire un recouvrement fini.

Remarque 7.51.

Certaines sources (dont [wikipédia](#)) disent que pour être compact il faut aussi être séparé¹³. Pour ces sources, un espace qui ne vérifie que la propriété de Borel-Lebesgue est alors dit **quasi-compact**.

7.52.

La définition 7.50 en cache deux. En effet, si la partie A est l'espace topologique lui-même, cela définit un espace topologique compact. Un espace topologique est compact *en soi* lorsque de tout recouvrement par des ouverts, nous pouvons extraire un sous-recouvrement fini. Dans ce cas, si X est l'espace et si $\{A_i\}_{i \in I}$ est le recouvrement, nous avons $X = \bigcup_{i \in I} A_i$ et non une simple inclusion $X \subset \bigcup_{i \in I} A_i$.

Lemme 7.53.

Si K est une partie compacte de l'espace topologie X , alors K est un espace topologique compact pour la topologie induite¹⁴ de X .

Démonstration. Nous notons τ la topologie de X et τ_K la topologie induite de X vers K , c'est-à-dire

$$\tau_K = \{\mathcal{O} \cap K \text{ tel que } \mathcal{O} \in \tau\}. \quad (7.37)$$

12. Parce qu'on a la flemme de faire une preuve par récurrence !

13. Définition 7.36.

14. Définition 7.17.

Soient des ouverts $A_i \in \tau_K$ ($i \in I$ où I est un ensemble quelconque) tels que $\bigcup_i A_i = K$. Pour chaque $i \in I$, il existe un $\mathcal{O}_i \in \tau$ tel que $A_i = K \cap \mathcal{O}_i$. Nous avons

$$K = \bigcup_{i \in I} (K \cap \mathcal{O}_i) \subset \bigcup_{i \in I} \mathcal{O}_i. \quad (7.38)$$

Donc les $\mathcal{O}_i$ forment un recouvrement de K par des ouverts de X . Vu que K est une partie compacte de X , il existe un sous-ensemble fini J de I tel que

$$K \subset \bigcup_{j \in J} \mathcal{O}_j. \quad (7.39)$$

Nous avons donc aussi

$$K \subset \bigcup_{j \in J} K \cap \mathcal{O}_j = \bigcup_{j \in J} A_j. \quad (7.40)$$

Nous avons prouvé que $\{A_j\}_{j \in J}$ est un recouvrement fini de K par des ouverts de K . Donc K est un espace topologique compact. $\square$

Définition 7.54.

Une partie d'un espace topologique est **relativement compact** si son adhérence est compacte.

Définition 7.55.

Un espace topologique est **localement compact** si tout élément possède un voisinage compact.

Définition 7.56 (Séquentiellement compact).

Nous disons qu'un espace topologique est **séquentiellement compact** si toute suite admet une sous-suite convergente.

Définition 7.57.

Un espace topologique est **dénombrable à l'infini** s'il est réunion dénombrable de compacts.

Définition 7.58.

Une famille $\mathcal{A}$ de parties de X a la **propriété d'intersection finie non vide** si tout sous-ensemble fini de $\mathcal{A}$ a une intersection non vide.

Proposition 7.59.

Soient X un espace topologique et $K \subset X$. Les propriétés suivantes sont équivalentes :

- (1) K est compact.
- (2) Si $\{F_i\}$ est une famille de fermés telle que $\bigcap_{i \in I} F_i \cap K = \emptyset$, alors il existe une partie finie non vide A de I tel que $\bigcap_{i \in A} F_i \cap K = \emptyset$.
- (3) Si $\{F_i\}_{i \in I}$ est une famille de fermés telle que pour tout choix de A fini dans I , $\bigcap_{i \in A} F_i \cap K \neq \emptyset$, alors l'intersection complète est non vide : $\bigcap_{i \in I} F_i \cap K \neq \emptyset$.
- (4) Toute famille de fermés de X , à laquelle K est joint, et qui a la propriété d'intersection finie non vide, a une intersection non vide.

Démonstration. Les propriétés (3) et (2) sont équivalentes par contraposition. De plus le point (4) est une simple¹⁵ reformulation en français de la propriété (3).

Prouvons (1) $\Rightarrow$ (2). Soit $\{F_i\}_{i \in I}$ une famille de fermés tels que $K \cap \bigcap_{i \in I} F_i = \emptyset$. Les complémentaires $\mathcal{O}_i$ de F_i dans X recouvrent K et donc on peut en extraire un sous-recouvrement fini :

$$K \subset \bigcup_{i \in A} \mathcal{O}_i \quad (7.41)$$

pour un certain sous-ensemble fini A de I . Pour ce même choix A , nous avons alors aussi

$$\bigcap_{i \in A} F_i \cap K = \emptyset. \quad (7.42)$$

¹⁵. Enfin, simple... il faut remarquer que dans la formulation de (4), les intersections peuvent ne pas faire intervenir K , mais, au final, on s'en moque.

L'implication (2) $\Rightarrow$ (1) est la même histoire de passage aux complémentaires. $\square$

Le théorème 7.209 est en général celui qu'on nomme « théorème des fermés emboîtés », mais le corolaire suivant en mériterait également le nom.

Corolaire 7.60 ([1]).

Soient un espace topologique compact X et une suite $(F_i)_{i \in \mathbb{N}}$ de fermés emboîtés¹⁶ dans X telle que

$$\bigcap_{i \in \mathbb{N}} F_i = \emptyset. \quad (7.43)$$

Alors il existe $j_0 \in \mathbb{N}$ tel que $F_i = \emptyset$ pour tout $i \geq j_0$.

Démonstration. La proposition 7.59 nous dit qu'il existe une partie finie non vide J de $\mathbb{N}$ telle que $\bigcup_{j \in J} F_j = \emptyset$. Si $j_0 = \min(J)$, alors $F_j \subset F_{j_0}$ pour tout $j \in J$ et nous avons

$$\emptyset = \bigcap_{j \in J} F_j = F_{j_0}. \quad (7.44)$$

Dès que $F_{j_0} = \emptyset$, tous les suivants sont également vides. $\square$

7.4.2 Quelques propriétés

Lemme 7.61.

Une partie K d'un espace topologique est compacte si et seulement si de tout recouvrement par des ouverts d'une base de topologie nous pouvons extraire un sous-recouvrement fini.

Remarquons que la partie qui est réellement à prouver est que, si « ça marche » pour des ouverts d'une base de topologie, alors « ça marche » pour tous types d'ouverts.

Démonstration. Soit K une partie d'un espace topologique et $\{\mathcal{O}_i\}_{i \in I}$ un recouvrement de K par des ouverts. Chacun des $\mathcal{O}_i$ est une union d'éléments de la base de topologie par la proposition 7.2 : disons $\mathcal{O}_i = \bigcup_{j \in J_i} A_{(i,j)}$. Soit $J = \{j = (i, j_i) \mid i \in I, j_i \in J_i\}$; alors nous obtenons $\bigcup_{j \in J} A_j = \bigcup_{i \in I} \mathcal{O}_i$.

Par hypothèse nous pouvons extraire un ensemble fini $J_0 \subset J$ tel que $K \subset \bigcup_{j \in J_0} A_j$. Par construction chacun des A_j est inclus dans (au moins) un des $\mathcal{O}_i$. Le choix d'un élément de I pour chacun des éléments de J_0 donne une partie finie I_0 de I telle que $K \subset \bigcup_{j \in J_0} A_j \subset \bigcup_{i \in I_0} \mathcal{O}_i$. $\square$

Exemple 7.62 (Un compact non fermé).

En général, un compact n'est pas toujours fermé. Si nous prenons par exemple un ensemble X de plus de deux points muni de la topologie grossière $\{\emptyset, X\}$. Toutes les parties de cet espace sont compactes, mais les seuls fermés sont $\{\emptyset, X\}$. Toutes les autres parties sont alors compactes et non fermées. $\triangle$

Lemme 7.63 (Compacts et fermés[158]).

À propos de parties fermées dans un compact.

- (1) Une partie fermée d'un compact est compacte.
- (2) Tout compact d'un espace topologique séparé est fermé.

Démonstration. En deux parties.

Pour (1) Soient F fermé dans un compact K et $\{\mathcal{O}_i\}_{i \in I}$ un recouvrement de F par des ouverts.

Vu que F est fermé, F^c est ouvert et $\{\mathcal{O}_i\}_{i \in I} \cup \{K \setminus F\}$ est un recouvrement de K par des ouverts. Si nous en extrayons un sous-recouvrement fini, c'est un recouvrement de F , et en supprimant éventuellement l'ouvert $K \setminus F$, ça reste un sous-recouvrement fini de F tout en étant extrait de $\{\mathcal{O}_i\}_{i \in I}$.

16. C'est-à-dire que $F_{i+1} \subset F_i$.

Pour (2) Soient X un espace séparé et K compact dans X . Nous considérons $y \in \mathbb{C}K$ et, par hypothèse de séparation, pour chaque $x \in K$ nous considérons un voisinage ouvert V_x de x et un voisinage ouvert ¹⁷ W_x de y tels que $V_x \cap W_x = \emptyset$. Bien entendu les V_x forment un recouvrement de K par des ouverts dont nous pouvons extraire un sous-recouvrement fini : soit S fini dans K tel que

$$K \subset \bigcup_{x \in S} V_x. \quad (7.45)$$

L'ensemble $W = \bigcap_{x \in S} W_x$ est une intersection finie d'ouverts autour de y et est donc un ouvert autour de y .

Montrons que $W \cap K = \emptyset$. Soit $a \in K$; par définition de S , il existe $s \in S$ tel que $a \in V_s$. Par conséquent, a n'est pas dans W_s et donc pas non plus dans W .

L'ouvert W prouve que y est dans l'intérieur du complémentaire de K , et comme y est arbitraire, nous concluons que le complémentaire de K est ouvert (théorème 7.7), en d'autres termes, que K est fermé.

□

Proposition 7.64 ([159]).

Dans un espace séparé, toute intersection de compacts est compacte.

Démonstration. Soit un espace topologie séparé X et des compacts $\{K_i\}_{i \in I}$ dans X (I est un ensemble quelconque). Chacun des K_i est fermé par le lemme 7.63(2). Donc l'intersection

$$K = \bigcap_{i \in I} K_i \quad (7.46)$$

est un fermé de X par le lemme 7.6(1). Soit i dans I . Nous avons $K \subset K_i$. Donc K est un fermé dans le compact K_i ; il est donc compact par le lemme 7.63. □

Exemple 7.65 (Intersection de compacts non compacte[159]).

Un exemple d'intersection de compacts qui n'est pas compacte. Vu la proposition 7.64, il va falloir chercher un espace non séparé. Soit $X = \mathbb{N} \cup \{x_1, x_2\}$ où x_1 et x_2 sont deux éléments distincts hors de $\mathbb{N}$. Nous définissons une topologie sur X en disant que les ouverts sont les parties suivantes :

- les parties de $\mathbb{N}$,
- la partie $\mathbb{N} \cup \{x_1\}$,
- la partie $\mathbb{N} \cup \{x_2\}$,
- la partie $\mathbb{N} \cup \{x_1, x_2\}$.

Nous considérons les parties $K_1 = \mathbb{N} \cup \{x_1\}$ et $K_2 = \mathbb{N} \cup \{x_2\}$.

K_i est compact Soit $\{\mathcal{O}_i\}_{i \in I}$ un recouvrement de K_1 par des ouverts de X . Alors il existe $i_0 \in I$ tel que $x_1 \in \mathcal{O}_{i_0}$. Vue la liste des ouverts $\mathcal{O}_{i_0}$ est soit $\mathbb{N} \cup \{x_1\}$ soit $\mathbb{N} \cup \{x_1, x_2\}$. Dans les deux cas, $\{\mathcal{O}_{i_0}\}$ est un sous-recouvrement fini de K_1 .

$K_1 \cap K_2 = \mathbb{N}$ C'est immédiat parce que x_1 et x_2 sont distincts.

$\mathbb{N}$ n'est pas compact Il peut être recouvert par les ouverts $\{\{i\}\}_{i \in \mathbb{N}}$ dont on ne peut pas extraire de sous-recouvrements finis.

△

Proposition 7.66.

Si V est une partie de l'espace topologique X muni de la topologie induite ¹⁸ τ_V de celle de X , et si K est un compact de (V, τ_V) alors K est un compact de (X, τ_X) .

17. Oui, la notation du voisinage peut surprendre, mais elle est quand même pratique pour ce qu'on veut en faire.

18. Définition 7.17.

Démonstration. Soient $(\mathcal{O}_\alpha)_{\alpha \in A}$ des ouverts de X recouvrant K . Alors les ensembles $V \cap \mathcal{O}_\alpha$ recouvrent également K , mais sont des ouverts de V . Donc il en existe un sous-recouvrement fini. Soient donc $(V \cap \mathcal{O}_i)_{i \in I}$ recouvrant K avec I un sous-ensemble fini de A . Les ensembles $(\mathcal{O}_i)_{i \in I}$ recouvrent encore K et sont des ouverts de X . $\square$

Proposition 7.67 ([1]).

Soient des espaces topologique X et Y . Nous considérons des ouverts A de X et B de Y . Soit un compact M dans $A \times B$ ¹⁹. Il existe des compacts K et L dans A et B tels que $M \subset K \times L$.

Démonstration. Nous considérons les « projections » de M sur A et B :

$$K = \{a \in A \text{ tel que } \exists b \in B \text{ tel que } (a, b) \in M\}, \quad (7.47)$$

et

$$L = \{b \in B \text{ tel que } \exists a \in A \text{ tel que } (a, b) \in M\}. \quad (7.48)$$

Nous avons $M \subset K \times L$; il reste à montrer que K et L sont des compacts de leurs espaces respectifs. Soit un recouvrement $\{U_i\}_{i \in I}$ de K par des ouverts de X et $\{V_j\}_{j \in J}$ de L par des ouverts de Y . Alors

$$\{U_i \times V_j\}_{\substack{i \in I \\ j \in J}} \quad (7.49)$$

est un recouvrement de M par des ouverts de $X \times Y$. Vu que M est un compact de $X \times Y$, nous pouvons en extraire un sous-recouvrement fini, c'est à dire I_0 fini dans I et J_0 fini dans J tels que

$$\{U_i \times V_j\}_{\substack{i \in I_0 \\ j \in J_0}} \quad (7.50)$$

soit encore un recouvrement de $K \times L$. Nous prouvons à présent que $\{U_i\}_{i \in I_0}$ est un recouvrement de K , ce qui montrera que K est un compact.

Soit $a \in K$. Il existe $b \in B$ tel que $(a, b) \in M$. Donc il existe $i_0 \in I_0$ et $j_0 \in J_0$ tels que $(a, b) \in U_{i_0} \times V_{j_0}$. En particulier $a \in U_{i_0}$.

Le même raisonnement montre que $\{V_j\}_{j \in J_0}$ est un recouvrement de L . $\square$

7.4.3 Compactifié d'Alexandrov

Proposition-Définition 7.68 ([160]).

Soit un espace topologique séparé localement compact²⁰ X . Nous considérons un élément $\omega \notin X$ et l'ensemble $\hat{X} = X \cup \{\omega\}$. Nous nommons « ouverts de $\hat{X}$ » les parties suivantes :

- les ouverts de X ,
- les parties de la forme $A \cup \{\omega\}$ avec $X \setminus A$ compact dans X .

Alors $\hat{X}$ est un espace topologique compact (cela justifie le nom « ouvert » donné aux parties sus-définies).

Démonstration. La première chose à faire est de prouver que $\hat{X}$ est bien un espace topologique (définition 7.1). Nous notons τ la topologie sur X et $\hat{\tau}$ l'ensemble des « ouverts » de $\hat{X}$. Le but est de prouver que $\hat{\tau}$ est une topologie.

L'espace lui-même $\hat{X} \in \hat{\tau}$ parce que $\hat{X} = X \cup \{\omega\}$ et que $X \setminus X = \emptyset$ est compact.

Le vide $\emptyset \in \tau \subset \hat{\tau}$.

Union quelconque Soient A_i ($i \in I$) des éléments de $\hat{\tau}$. Nous posons $I_1 = \{i \in I \text{ tel que } A_i \subset X\}$ et $I_2 = I \setminus I_1$. Nous avons

$$\bigcup_{i \in I} A_i = \left(\bigcup_{i \in I_1} A_i \right) \cup \left(\bigcup_{i \in I_2} A_i \right) = B \cup \left(\bigcup_{i \in I_2} B_i \cup \{\omega\} \right) \quad (7.51)$$

19. Topologie produit, définition 7.15

20. Définition 7.55.

où B et les B_i sont des ouverts de X tels que $X \setminus B_i$ est compact dans X . Nous récrivons ça sous la forme

$$\bigcup_{i \in I} A_i = B \cup \left(\bigcup_{i \in I_2} B_i \right) \cup \{\omega\}. \quad (7.52)$$

La question est de savoir si

$$X \setminus \left(B \cup \left(\bigcup_{i \in I_2} B_i \right) \right) \quad (7.53)$$

est compact dans X . Un peu de réécriture :

$$X \setminus \left(B \cup \left(\bigcup_{i \in I_2} B_i \right) \right) = (X \setminus B) \cap X \setminus \left(\bigcup_{i \in I_2} B_i \right) = (X \setminus B) \cap \left(\bigcap_{i \in I_2} (X \setminus B_i) \right). \quad (7.54)$$

La partie $X \setminus B$ est fermée dans X parce que B est ouverte. La proposition 7.64 dit qu'une intersection de compacts est compacte (parce que X est séparé). Nous sommes donc en présence de l'intersection entre un compact et un fermé.

Tout compact d'un espace séparé est fermé²¹. Donc nous sommes en présence de l'intersection de deux fermés. Donc $(X \setminus B) \cap \left(\bigcap_{i \in I_2} (X \setminus B_i) \right)$ est fermé. Mais c'est contenu dans le compact $\bigcap_{i \in I_2} (X \setminus B_i)$. Fermé dans un compact, donc compact (lemme 7.63).

Intersection finie Nous considérons les « ouverts » $(A_i)_{i=1, \dots, n}$ de $\hat{X}$. Si ce sont tous des ouverts de X , l'intersection est un ouvert de X et on est bon.

Supposons que tous les A_i soient de la forme $A_i = B_i \cup \{\omega\}$ avec $X \setminus B_i$ compact. Alors

$$\bigcap_{i=1}^n B_i \cup \{\omega\} = \left(\bigcup_{i=1}^n B_i \right) \cup \{\omega\}. \quad (7.55)$$

Mais le lemme 1.19 (appliqué un nombre fini de fois) donne

$$X \setminus \left(\bigcap_{i=1}^n B_i \right) = \bigcup_{i=1}^n (X \setminus B_i) \quad (7.56)$$

qui est compact en tant qu'union finie de compacts.

Enfin, nous supposons que les A_i sont un mélange des deux types, nous les séparons entre ceux qui sont directement des ouverts de X et les autres :

$$\bigcap_{i=1}^n A_i = B \cap \left(\bigcap_{i=1}^m B_i \cup \{\omega\} \right) = B \cap \left(\bigcap_{i=1}^n B_i \right) \quad (7.57)$$

où $B \subset X$ est ouvert et les B_i sont des parties de X telles que $X \setminus B_i$ est compact dans X . En utilisant le cas précédent,

$$B \cap \left(\bigcap_{i=1}^m B_i \cup \{\omega\} \right) = B \cap (E \cup \{\omega\}) = B \cap E \quad (7.58)$$

avec $X \setminus E$ compact dans X .

Vu qu'elle est compacte, la partie $X \setminus E$ est fermée, et donc E est ouvert. Le tout est au final un ouvert de X , et donc dans $\hat{\tau}$.

Nous avons fini de prouver que $(\hat{X}, \hat{\tau})$ est un espace topologique. Nous montrons à présent que $\hat{X}$ est compact.

Soit $\{A_i\}_{i \in I}$ un recouvrement de $\hat{X}$ par des ouverts. Pour au moins un $i_0 \in I$ nous avons $\omega \in A_{i_0}$. Nous posons $A_{i_0} = B \cup \{\omega\}$ avec $X \setminus B$ compact dans X .

21. Lemme 7.63(2).

Les ouverts $\{A_i\}_{i \in I}$ forment un recouvrement de $X \setminus B$ par des ouverts. Nous pouvons en extraire un sous-recouvrement fini :

$$X \setminus B \subset \bigcup_{i \in I_1} A_i. \quad (7.59)$$

Nous avons alors

$$\hat{X} \subset \bigcup_{i \in I_1 \cup \{i_0\}} A_i. \quad (7.60)$$

Et voila que $\hat{X}$ est recouvert par un nombre fini des A_i . Notez que (7.60) est une égalité, mais nous n'en avons pas besoin. $\square$

7.69.

Oh bien entendu les plus fêrus de questions embarrassantes demanderont, si X est l'espace considéré, où prendre ce ω ? Quel « objet » exist en-dehors de X ? Qui m'assure que X n'est pas tellement grand que tout est dedans ? Le fait est qu'il n'existe pas d'ensemble contenant tous les ensembles (c'est le corollaire 1.126). Nous pouvons donc toujours trouver un ensemble ω qui n'est pas dans X .

En ce qui concerne $\mathbb{R}$ auquel nous pouvons attacher deux infinis ($+\infty$ et $-\infty$), ce sera la définition 12.25.

Pour $\mathbb{C}$, nous donnerons une caractérisation de la limite en ∞ dans le lemme 12.80.

7.5 Limites et continuité de fonctions

7.5.1 Limites

Définition 7.70 (Limite d'une fonction, thème 17[161]).

Soient des espaces topologiques X et Y ainsi que $\Omega \subset X$ et $a \in \text{Adh}(\Omega)$. Soit une application $f: \Omega \rightarrow Y$. Nous disons que l'élément ℓ de Y est une **limite** de f en a lorsque pour tout voisinage ouvert V de ℓ , il existe un voisinage ouvert U de a tel que

$$f(U \cap \Omega \setminus \{a\}) \subset V. \quad (7.61)$$

Si un tel élément est unique²², alors nous disons que cet élément est la **limite** de f et nous notons

$$\lim_{x \rightarrow a} f(x) = \ell. \quad (7.62)$$

7.71.

Il aurait été tout aussi bien de définir la limite d'une fonction $f: X \rightarrow Y$ définie sur tout X , puis de considérer Ω avec la topologie induite depuis X .

Remarque 7.72.

Nous ne saurions trop insister sur le fait que la valeur de f en a n'intervient pas dans la définition de la limite de f en a . Il n'est même pas nécessaire que f soit définie en a pour que l'on puisse parler de limite de f en a . Par exemple nous avons

$$\lim_{x \rightarrow 1} \frac{x^2 - 1}{x - 1} = 2, \quad (7.63)$$

alors que la fonction n'est pas définie en $x = 1$.

Plus généralement, un peu par principe, toutes les fois que la notion de limite apporte une information, le point où l'on prend la limite est spécial. Sinon on ne calculerait pas la limite, mais on regarderait directement la valeur de la fonction. Cela est typiquement le cas lorsque nous verrons les dérivées. En effet, regardons (en faisant du semblant d'anticiper) la définition (12.114). Dans la formule

$$f'(a) = \lim_{x \rightarrow a} \frac{f(x) - f(a)}{x - a}, \quad (7.64)$$

la fonction sur laquelle nous prenons la limite n'est *jamais* définie en $x = a$.

22. Rappelons que ce n'est pas toujours le cas, mais que ça l'est si l'espace topologique est séparé – définition 7.36.

Proposition 7.73 (Unicité de la limite pour un espace séparé).

Soient X un espace topologique, A une partie de X et Y un espace topologique séparé²³. Nous considérons une fonction $f: A \rightarrow Y$. Si $a \in \bar{A}$, alors f admet au plus une limite en a .

Démonstration. Soient y et y' des limites de f en a , ainsi que des voisinages V et V' de y et y' . Nous prenons également les voisinages W et W' correspondants :

$$\begin{cases} f(W \cap A) \subset V & (7.65a) \\ f(W' \cap A) \subset V'. & (7.65b) \end{cases}$$

Quitte à prendre des sous-ensembles nous pouvons supposer que W et W' sont ouverts. Il s'ensuit alors que :

- l'ensemble $W \cap W'$ est un ouvert contenant a et intersecte donc A ;
- l'ensemble $(W \cap W') \cap A$ est donc non vide;
- et donc, $f(W \cap W' \cap A)$ est aussi non vide.

Mais

$$f(W \cap W' \cap A) \subset f(W \cap A) \subset V, \quad (7.66)$$

et

$$f(W \cap W' \cap A) \subset f(W' \cap A) \subset V', \quad (7.67)$$

d'où V et V' ont une intersection. Puisque ces ensembles sont arbitraires, nous avons prouvé que tout voisinage de y et tout voisinage de y' ont une intersection non vide ; étant donné que Y est séparé, nous devons avoir $y = y'$. $\square$

Lemme 7.74 (Changement de variables).

Soient un espace vectoriel topologique X ainsi qu'un espace séparé Y et une application $f: X \rightarrow Y$. Nous supposons que $\lim_{x \rightarrow a} f(x) = \ell$. Alors $\lim_{x \rightarrow b} f(x + a - b)$ existe et vaut ℓ .

Démonstration. Soit un voisinage V de ℓ dans Y . Il existe un voisinage U de a tel que $f(U) \subset V$. Nous posons $U' = U - a + b$. C'est un voisinage de b . En posant $g(x) = f(x + a - b)$ nous avons

$$g(U') = f(U - a + b + a - b) = f(U) \subset V. \quad (7.68)$$

Donc $\lim_{x \rightarrow b} g(x) = \ell$. C'est cette égalité qui signifie $\lim_{x \rightarrow b} f(x + a - b)$. $\square$

7.5.2 Continuité

7.5.2.1 Définitions et propriétés

La définition suivante est la définition de la continuité dans tous les cas.

Définition 7.75 (Fonction continue[162]).

Deux définitions :

- (1) Soient une fonction $f: X \rightarrow Y$ entre les espaces topologiques X et Y et un point $a \in X$. Nous disons que f est **continue** en a si pour tout ouvert W contenant $f(a)$, il existe un voisinage V de a dans X tel que $f(V) \subset W$.
- (2) Une fonction $f: X \rightarrow Y$ est **continue** sur X si pour tout ouvert $\mathcal{O}$ de Y , l'ensemble

$$f^{-1}(\mathcal{O}) = \{x \in X \text{ tel que } f(x) \in \mathcal{O}\} \quad (7.69)$$

est ouvert dans X .

23. Définition 7.36.

7.76.

Lorsque nous écrivons $f: X \rightarrow Y$, nous entendons que f est définie sur tout X , mais pas qu'elle soit surjective sur Y . En particulier, pour que f soit continue en a , il faut que a soit dans le domaine de f .

Dans le cas de fonctions $\mathbb{R} \rightarrow \mathbb{R}$, l'espace X sera la partie de $\mathbb{R}$ sur laquelle f sera définie, et la topologie sera la topologie induite de $\mathbb{R}$.

Proposition 7.77 ([163]).

Soient deux espaces topologiques X et Y . Une application $f: X \rightarrow Y$ est continue si et seulement si pour tout $x \in X$ et pour tout voisinage²⁴ V de $f(x)$, la partie $f^{-1}(V)$ est un voisinage de x dans X .

Démonstration. En deux parties.

$\Rightarrow$ Soient $x \in X$ et un voisinage V de x dans X . Vu que V est un voisinage de $f(x)$, il existe un ouvert $\mathcal{O}$ de Y tel que $x \in \mathcal{O} \subset V$.

La partie $f^{-1}(\mathcal{O})$ vérifie :

- $f^{-1}(\mathcal{O})$ est un ouvert de X parce que f est continue.
- $x \in f^{-1}(\mathcal{O})$
- $f^{-1}(\mathcal{O}) \subset f^{-1}(V)$.

Donc $f^{-1}(V)$ contient un ouvert contenant x . Donc $f^{-1}(V)$ est un voisinage de x dans X .

$\Leftarrow$ Soit un ouvert $\mathcal{O}$ de Y . Nous devons prouver que $f^{-1}(\mathcal{O})$ est un ouvert de X . Pour cela nous prouvons que $f^{-1}(\mathcal{O})$ contient un ouvert autour de chacun de ses éléments et utiliser le théorème 7.7.

Soit donc $x \in f^{-1}(\mathcal{O})$. La partie $\mathcal{O}$ est un voisinage de $f(x)$. Donc $f^{-1}(\mathcal{O})$ est un voisinage de x . Il existe donc un ouvert V de X tel que

$$x \in V \subset f^{-1}(\mathcal{O}). \quad (7.70)$$

Nous en déduisons que $f^{-1}(\mathcal{O})$ contient bien un ouvert autour de chacun de ses points.

□

Exemple 7.78 ([1]).

Un truc bien avec la définition 7.75(1) est que la continuité de f en un point est définie pour tout point du domaine ; pas seulement les points d'accumulation. Soit par exemple une fonction simple

$$\begin{aligned} f: \{a\} &\rightarrow \mathbb{R} \\ a &\mapsto 4. \end{aligned} \quad (7.71)$$

Si W est un ouvert de $\mathbb{R}$ contenant 4, nous avons l'ouvert $V = \{a\}$ tel que $f(V) \subset W$. Donc f est continue au point 4.

Mais f est également continue sur $\{4\}$ en tant qu'espace topologique. En effet, si W est un ouvert de $\mathbb{R}$, l'ensemble $f^{-1}(W)$ est soit $\emptyset$ soit $\{a\}$. Dans les deux cas c'est un ouvert. $\triangle$

La proposition 7.208 donnera des détails sur ce qu'il se passe lorsque l'espace est métrique.

Théorème 7.79.

Une fonction $f: X \rightarrow Y$ est une fonction continue si et seulement si elle est continue en chacun des points de X .

Démonstration. En deux parties.

Sens direct Nous supposons que f est une fonction continue. Soient $a \in X$ et W un voisinage de $f(a)$. Nous considérons $\mathcal{O}$, un voisinage ouvert de $f(a)$ contenu dans W ; l'ensemble $f^{-1}(\mathcal{O})$ est alors un ouvert contenant a , et l'image de $f^{-1}(\mathcal{O})$ par f est bien entendu contenue dans W .

24. Définition 7.4

Sens inverse Soit $\mathcal{O}$ un ouvert de Y . Pour prouver que $f^{-1}(\mathcal{O})$ est un ouvert de X , nous allons considérer un élément $a \in f^{-1}(\mathcal{O})$ et montrer qu'il existe un voisinage ouvert de a contenu dans $f^{-1}(\mathcal{O})$; le théorème 7.7 nous assurera alors que $f^{-1}(\mathcal{O})$ est ouvert.

L'ensemble $\mathcal{O}$ est un voisinage ouvert de $f(a)$ parce que a a été choisi dans $f^{-1}(\mathcal{O})$. Donc la continuité de f en a nous assure qu'il existe un voisinage W de a tel que $f(W) \subset \mathcal{O}$. En prenant un ouvert contenant a à l'intérieur de W nous avons un voisinage ouvert de a contenu dans $f^{-1}(\mathcal{O})$. □

Remarque 7.80.

À cause de l'éventuelle non unicité de la limite, deux fonctions continues et égales sur un sous-ensemble dense ne sont pas spécialement égales. Ce sera vrai sur les espaces métriques et plus généralement pour les espaces séparés. Voir l'exemple 7.35 et la proposition 7.73.

Lemme 7.81 ([1]).

Soient une fonction $f: X \rightarrow Y$, et un point d'accumulation $a \in X$ ²⁵. La fonction f est continue en a si et seulement si $f(a)$ est une limite de f en a .

Démonstration. En deux parties.

Sens direct Nous supposons que f est continue en $a \in X$. Soit un voisinage W de $f(a)$ dans Y . Par continuité de f en a , il existe un voisinage V de A tel que $f(V) \subset W$. A fortiori, $f(V \setminus a) \subset W$ comme le demande la définition de la limite.

Sens inverse Nous supposons que $f(a)$ est une limite de $f(x)$ lorsque x tend vers a . Si W est un ouvert de Y contenant $f(a)$, il existe un voisinage V de a dans X tel que $f(V \setminus a) \subset W$. Mais vu que $f(a) \in W$, nous avons $f(V) \subset W$. □

7.5.2.2 Continuité séquentielle

Définition 7.82.

Si X et Y sont deux espaces topologiques, une fonction $f: X \rightarrow \mathbb{R}$ est **séquentiellement continue** en un point a si pour toute suite convergente $x_n \rightarrow a$ dans X nous avons $f(x_n) \rightarrow f(a)$ dans Y .

7.83.

Nous allons maintenant voir deux résultats disant que si une fonction est continue, alors elle peut être permutée avec une limite de suite. Dans le cas des espaces métriques, la proposition 7.164 montrera la réciproque : si pour toute suite $x_n \rightarrow a$, nous avons $\lim_{n \rightarrow \infty} f(x_n) = y$, alors f a une limite en a qui vaut y .

Proposition 7.84 (Permuter limite et fonction continue[1]).

Soient deux espaces topologiques X et Y ainsi qu'une fonction $f: X \rightarrow Y$. Soit $a \in X$ et $\ell \in Y$. Si

$$\lim_{x \rightarrow a} f(x) = \ell, \quad (7.72)$$

alors, pour toute suite (x_k) telle que $x_k \rightarrow a$, on a

$$\lim f(x_k) = \ell. \quad (7.73)$$

Démonstration. Nous considérons une suite (x_k) qui converge vers a dans X . Soient V un voisinage de ℓ et W un voisinage de a tels que $f(W) \subset V$ (définition 7.70 de la continuité en un point). Par la convergence $a_k \rightarrow a$, il existe N tel que pour tout $k > N$, $a_k \in W$, et donc tel que $f(a_k) \in V$, ce qui donne la continuité séquentielle de f . □

25. Un point d'accumulation de X n'est pas spécialement dans X , si X est un sous-espace d'un autre. Par exemple 0 est un point d'accumulation de $]0, 1[$ dans $\mathbb{R}$. Ici nous supposons que $a \in X$, sinon il n'y a de toutes façons pas de continuité en a .

Corolaire 7.85 (Caractérisation séquentielle de la continuité en un point[1]).

Un application entre deux espaces topologiques est continue en un point y est séquentiellement continue.

Démonstration. Soit une application $f: X \rightarrow Y$ entre les espaces topologies X et Y . Nous supposons que f est continue en $a \in X$. Soit une suite convergente $x_k \xrightarrow{X} a$. Nous devons prouver que $f(x_k) \rightarrow f(a)$.

Soit un voisinage V de $f(a)$ dans Y . Le fait que f soit continue en a signifie²⁶ que $f(a)$ est une limite de f en a , c'est-à-dire²⁷ qu'il existe un voisinage W de a tel que $f(W \setminus \{a\}) \subset V$.

Vu que $x_k \rightarrow a$, il existe N tel que $x_k \in W$ pour tout $k \geq N$. Pour ces valeurs de k , nous avons $f(x_k) \in V$.

Nous avons prouvé que pour tout voisinage V de $f(a)$ dans Y , il existe N tel que $f(x_k) \in V$ dès que $k \geq N$. Cela signifie exactement que $f(x_k) \rightarrow f(a)$. $\square$

7.5.2.3 Application réciproque

Définition 7.86 (injection, surjection, bijection).

Soient des ensembles A et B ainsi qu'une application $f: A \rightarrow B$.

- (1) *La fonction f est **injective** si $f(x_1) = f(x_2)$, implique $x_1 = x_2$.*
- (2) *La fonction f est **surjective** si tous les éléments de B sont atteints, c'est-à-dire si pour tout $y \in B$ il existe $x \in A$ tel que $f(x) = y$.*
- (3) *La fonction f est une **bijection** entre A et B si elle est injective et surjective, c'est-à-dire si pour tout $y \in B$ il existe un unique $x \in A$ tel que $f(x) = y$.*

La surjection et l'injection sont des propriétés bien différentes qu'il convient de prouver séparément. De plus une même « formule » peut définir une application injective, surjective, bijective ou non selon le domaine sur laquelle nous la considérons.

Définition 7.87.

*Soit $f: A \rightarrow B$ une bijection. L'**application réciproque** de f est la fonction*

$$\begin{aligned} f^{-1}: B &\rightarrow A \\ y &\mapsto \text{le } x \in A \text{ tel que } f(x) = y. \end{aligned} \tag{7.74}$$

Plus généralement si $f: X \rightarrow Y$ est une application quelconque et si $S \subset Y$ nous notons

$$f^{-1}(S) = \{x \in X \text{ tel que } f(x) \in S\}, \tag{7.75}$$

et dans le cas où S est réduit à un unique élément y , nous notons $f^{-1}(y)$ au lieu de $f^{-1}(\{y\})$. Si de plus $f^{-1}(S)$ est un singleton x , nous noterons $f^{-1}(S) = x$ et non $f^{-1}(S) = \{x\}$.

Les plus acharnés parmi les lecteurs se rendront compte de la différence ontologique fondamentale entre x et $\{x\}$.

Proposition 7.88.

Soit $f: A \subset \mathbb{R}^n \rightarrow B \subset \mathbb{R}^m$ une bijection continue. Si A est compact, alors $f^{-1}: B \rightarrow A$ est continue.

Proposition 7.89.

Soient I un intervalle dans $\mathbb{R}$ et $f: I \rightarrow \mathbb{R}$ une fonction continue strictement monotone. Alors la fonction réciproque $f^{-1}: f(I) \rightarrow \mathbb{R}$ est continue sur l'intervalle $f(I)$.

26. C'est la définition 7.75 de la continuité en un point.

27. Définition 7.70 d'être une limite.

7.5.2.4 Homéomorphisme

Définition 7.90 (homéomorphisme).

Un **homéomorphisme** est une application bijective continue entre deux espaces topologiques dont la réciproque est continue. Deux espaces topologiques X et Y pour lesquels il existe un homéomorphisme entre X et Y , sont dits **isomorphes**.

7.5.3 Continuité et topologie induite

Proposition 7.91 ([1]).

Soit une fonction $f: X \rightarrow Y$, continue sur l'ouvert A de X au sens où elle est continue en chaque point de A . Alors la fonction restriction $\tilde{f}: A \rightarrow Y$ est également continue pour la topologie sur A , induite²⁸ de X .

Démonstration. Soit $a \in A$, et montrons que $\tilde{f}$ est continue en a , c'est-à-dire que $\tilde{f}(a) = f(a)$ soit une limite de $\tilde{f}$ en a . Soit un voisinage V de $\tilde{f}(a)$ dans Y . Par la continuité de f , nous avons un ouvert W de X tel que

$$f(W \setminus \{a\}) \subset V. \quad (7.76)$$

La partie $W \cap A$ est un voisinage de a pour la topologie de A , et vérifie

$$f(W \cap A \setminus \{a\}) \subset V. \quad (7.77)$$

donc $f(a)$ est une limite de $\tilde{f}$ pour $x \rightarrow a$. La fonction $\tilde{f}: A \rightarrow Y$ est continue en chaque point de A . $\square$

Au niveau de la notion de continuité, il n'y a pas trop de changements en passant de $\mathbb{R}$ à $\mathbb{Q}$ muni de la topologie induite.

Exemple 7.92.

Que signifie d'être continue pour une fonction $f: \mathbb{Q} \rightarrow \mathbb{R}$? D'après le théorème 7.79, il s'agit d'être continue en chaque point de $\mathbb{Q}$. Il s'agit donc, par la définition 7.75 que pour tout $q \in \mathbb{Q}$, le nombre $f(q)$ soit une limite de f pour $x \rightarrow q$.

L'espace d'arrivée étant $\mathbb{R}$, un voisinage de $f(q)$ est pris comme une boule de taille ϵ . La continuité de f exige qu'il y ait un voisinage W de q dans $\mathbb{Q}$ tel que pour tout $q' \in W$ (différent que q), $|f(q) - f(q')| < \epsilon$.

Qu'est-ce qu'un ouvert dans $\mathbb{Q}$? D'après la définition 7.17 de la topologie induite, ce sont les ensembles $\mathbb{Q} \cap \mathcal{O}$ avec $\mathcal{O}$ ouvert dans $\mathbb{R}$. Tout cela pour dire que pour tout $\epsilon > 0$, il doit exister $\delta > 0$ tel que pour tout $q' \in \mathbb{Q}$ tel que $0 < |q - q'| < \delta$, nous ayons $|f(q) - f(q')| < \epsilon$.

Bref, c'est exactement le mécanisme usuel de la continuité sur $\mathbb{R}$, sauf qu'il faut seulement considérer les rationnels. $\triangle$

Lemme 7.93 (Application partielle[1]).

Soient trois espaces topologiques X_1 , X_2 et Y . Nous considérons une fonction continue $f: X_1 \times X_2 \rightarrow Y$ ainsi que $x_1 \in X_1$. Alors l'application

$$\begin{aligned} g: X_2 &\rightarrow Y \\ x_2 &\mapsto f(x_1, x_2) \end{aligned} \quad (7.78)$$

est continue.

Démonstration. Soit un ouvert $\mathcal{O}$ de Y ; par hypothèse sur f , la partie $f^{-1}(\mathcal{O})$ est ouverte dans $X_1 \times X_2$. Notre but est de prouver que $g^{-1}(\mathcal{O})$ est un ouvert de X_2 . Nous avons :

$$g^{-1}(\mathcal{O}) = \{x_2 \in X_2 \text{ tel que } (x_1, x_2) \in f^{-1}(\mathcal{O})\}. \quad (7.79)$$

28. Définition 7.17.

Nous considérons $x_2 \in g^{-1}(\mathcal{O})$ et nous prouvons qu'il existe dans X_2 un voisinage de x_2 entièrement contenu dans $g^{-1}(\mathcal{O})$.

Étant donné que (x_1, x_2) est dans $f^{-1}(\mathcal{O})$ qui est ouvert, la définition 7.15 de la topologie sur $X_1 \times X_2$ nous donne des ouverts A_1 dans X_1 et A_2 dans X_2 tels que

$$(x_1, x_2) \in A_1 \times A_2 \subset f^{-1}(\mathcal{O}). \quad (7.80)$$

Nous montrons à présent que $A_2 \subset g^{-1}(\mathcal{O})$. Soit $y_2 \in A_2$. Par construction $(x_1, y_2) \in A_1 \times A_2 \subset f^{-1}(\mathcal{O})$, donc

$$g(y_2) = f(x_1, y_2) \in \mathcal{O}. \quad (7.81)$$

Cela termine la démonstration. $\square$

7.5.4 Continuité et connexité

Proposition 7.94.

Un espace topologique X est connexe si et seulement si toute application continue $X \rightarrow \mathbb{Z}$ est constante.

Proposition 7.95.

L'image d'un ensemble connexe par une fonction continue est connexe.

Démonstration. Soit $f: X \rightarrow Y$ une application continue entre deux espaces topologiques, et E une partie connexe de X . Nous devons montrer que $f(E)$ est connexe dans Y .

Par l'absurde nous considérons A et B , deux ouverts de Y disjoints recouvrant $f(E)$. Étant donné que f est continue, les ensembles $f^{-1}(A)$ et $f^{-1}(B)$ sont ouverts dans X . De plus ces deux ensembles recouvrent E .

Si x est un élément de $f^{-1}(A) \cap f^{-1}(B)$, alors $f(x) \in A \cap B$, ce qui est impossible parce que nous avons supposé que A et B étaient disjoints. Par conséquent $f^{-1}(A)$ et $f^{-1}(B)$ sont deux ouverts disjoints recouvrant E . Contradiction avec la connexité de E . Nous concluons que $f(E)$ est connexe. $\square$

Une application de ce théorème sera le théorème de valeurs intermédiaires 10.80.

Exemple 7.96.

Les espaces topologiques $\mathbb{R}$ et $\mathbb{R}^2$ ne sont pas homéomorphes. $\triangle$

Démonstration. Supposons par l'absurde que $f: \mathbb{R} \rightarrow \mathbb{R}^2$ soit un homéomorphisme. Nous posons $E = f(\mathbb{R} \setminus \{0\})$ et $z_0 = f(0)$. Vu que f est bijective nous avons

$$E = \mathbb{R}^2 \setminus \{z_0\}, \quad (7.82)$$

qui est connexe.

Vu que E est connexe et que f^{-1} est continue, la proposition 7.95 nous dit que $f^{-1}(E)$ est connexe. Mais par définition, $f^{-1}(E) = \mathbb{R} \setminus \{0\}$ qui n'est pas connexe. $\square$

7.5.5 Continuité et compacité

Théorème 7.97.

L'image d'un compact²⁹ par une fonction continue est un compact.

Dans le cadre des espaces vectoriels normés, ce théorème est démontré en la proposition 7.204.

Démonstration. Soit $K \subset X$, un ensemble compact, et regardons $f(K)$; en particulier, nous considérons Ω , un recouvrement de $f(K)$ par des ouverts. Nous avons que

$$f(K) \subseteq \bigcup_{\mathcal{O} \in \Omega} \mathcal{O}. \quad (7.83)$$

29. Définition 7.50.

Par construction, nous avons aussi

$$K \subseteq \bigcup_{\mathcal{O} \in \Omega} f^{-1}(\mathcal{O}), \quad (7.84)$$

en effet, si $x \in K$, alors $f(x)$ est dans un des ouverts de Ω , disons $f(x) \in \mathcal{O}$, et évidemment, $x \in f^{-1}(\mathcal{O})$. Les $f^{-1}(\mathcal{O})$ recouvrent le compact K , et donc on peut en choisir un sous-recouvrement fini, c'est-à-dire un choix de $\{f^{-1}(\mathcal{O}_1), \dots, f^{-1}(\mathcal{O}_n)\}$ tels que

$$K \subseteq \bigcup_{i=1}^n f^{-1}(\mathcal{O}_i). \quad (7.85)$$

Dans ce cas, nous avons que

$$f(K) \subseteq \bigcup_{i=1}^n \mathcal{O}_i, \quad (7.86)$$

ce qui prouve la compacité de $f(K)$. $\square$

7.6 Topologie, distances et normes

Certains ensembles ont plus de structures qu'une topologie. Nous fixons quelques bases maintenant, et nous détaillerons certains résultats plus tard.

7.6.1 Distance et topologie métrique

Définition 7.98.

Si E est un ensemble, une **distance** sur E est une application $d: E \times E \rightarrow \mathbb{R}$ telle que pour tout $x, y \in E$,

- (1) $d(x, y) \geq 0$
- (2) $d(x, y) = 0$ si et seulement si $x = y$,
- (3) $d(x, y) = d(y, x)$
- (4) $d(x, y) \leq d(x, z) + d(z, y)$.

La dernière condition est l'**inégalité triangulaire**.

Un couple (E, d) formé d'un ensemble et d'une distance est un **espace métrique**.

La définition-théorème suivante donne une topologie sur les espaces métriques en partant des boules.

Théorème-Définition 7.99.

Soit (E, d) un espace métrique. Nous définissons les **boules ouvertes** par

$$B(x, r) = \{y \in E \text{ tel que } d(x, y) < r\}. \quad (7.87)$$

pour tout $x \in E$ et $r > 0$. Alors en posant

$$\mathcal{T} = \{\mathcal{O} \subset E \text{ tel que } \forall x \in \mathcal{O}, \exists r > 0 \text{ tel que } B(x, r) \subset \mathcal{O}\} \quad (7.88)$$

nous définissons une topologie sur E .

Cette topologie sur E est la **topologie métrique** de (E, d) . En présence d'une distance, sauf mention explicite du contraire, c'est toujours cette topologie-là que nous utiliserons.

Démonstration. D'abord $\emptyset \in \mathcal{T}$ parce que tout élément de l'ensemble vide ... heu ... enfin parce que d'accord hein³⁰. Ensuite si $(A_i)_{i \in I}$ sont des éléments de $\mathcal{T}$ et si $x \in \bigcup_{i \in I} A_i$ alors il existe $k \in I$ tel que $x \in A_k$. Par hypothèse il existe une boule $B(x, r) \subset A_k \subset \bigcup_{i \in I} A_i$.

Enfin si $(A_i)_{i \in \{1, \dots, n\}}$ sont des éléments de $\mathcal{T}$ alors pour tout i il existe $r_i > 0$ tel que $B(x, r_i) \subset A_i$. En prenant $r = \min\{r_i\}_{i=1, \dots, n}$ nous avons $B(x, r) \subset \bigcap_{i=1}^n A_i$. $\square$

30. Pour qui ne seraient pas d'accord, allez ajouter $\emptyset$ dans la définition des ouverts et puis c'est tout.

Remarque 7.100.

Quatre remarques à propos de cette définition.

- (1) Cette définition est faite exprès pour respecter le théorème 7.7. Même si, à priori, on aurait dû utiliser la topologie engendrée faite à l'exemple 7.11... mais on peut montrer que les deux topologies sont les mêmes.
- (2) Par construction, les boules ouvertes sont une base de la topologie (définition 7.2) des espaces métriques.
- (3) Si V est un voisinage de x , alors il existe r tel que $B(x, r) \subset V$.
- (4) Tout espace métrique est séparé. En effet, si deux éléments x et y sont distincts, alors en posant $r = d(x, y)/3 > 0$, les boules $B(x, r)$ et $B(y, r)$ sont disjointes. Très pratique pour les limites : elles sont uniques, grâce aux propositions 7.38 et 7.73!

7.101.

Si vous avez un peu de temps, vous pouvez vérifier que si $\mathbb{K}$ est un corps totalement ordonné, alors avec toutes les définitions de 1.253, en posant $d(x, y) = |x - y|$ nous avons une distance sur $\mathbb{K}$.

De plus, les boules définies en 1.253 sont alors les mêmes que celles définies en (7.87), ce qui donne à tout corps totalement ordonné une structure d'espace topologique.

7.6.1.1 Les boules, une base de topologie**Proposition 7.102.**

Un espace métrique séparable³¹ accepte une base de topologie³² dénombrable.

Soit A dense et dénombrable dans l'espace métrique séparable (E, d) . Si $\{a_i\}_{i \in \mathbb{N}}$ est une énumération de A et $\{r_i\}_{i \in \mathbb{N}}$ une énumération de $\mathbb{Q}$, alors

$$\mathcal{B} = \{B(a_i, r_j)\}_{i, j \in \mathbb{N}} \quad (7.89)$$

est une base de la topologie³³ de E .

Démonstration. Soient $x \in E$ et V un voisinage de x . Ce dernier contient une boule $B(x, r)$ et quitte à prendre r un peu plus petit nous supposons que $r \in \mathbb{Q}$ (existence d'un tel rationnel par le lemme 1.307).

Soit $a \in A$ avec $\|a - x\| < \frac{r}{3}$ (existe par densité de A dans E) ; nous avons $B(a, \frac{2r}{3}) \subset B(x, r)$ parce que si $y \in B(a, \frac{2r}{3})$ alors

$$\|y - x\| \leq \|y - a\| + \|a - x\| < \frac{2}{3}r + \frac{1}{3}r = r. \quad (7.90)$$

La seconde inégalité est stricte parce que les boules sont ouvertes. Le tout montre que $y \in B(x, r)$. Par ailleurs $x \in B(a, \frac{2}{3}r)$ et nous avons trouvé un élément de $\mathcal{B}$ contenant x tout en étant inclus dans V . Cela prouve que $\mathcal{B}$ est bien une base de la topologie de E . $\square$

Remarque 7.103.

Il est vite vu que les cubes ouverts forment aussi une base de la topologie de $\mathbb{R}^n$. Cela est à mettre en rapport avec le fait que toutes les normes sont équivalentes sur $\mathbb{R}^n$ (proposition 11.52).

Voir aussi le corolaire 14.219 qui donnera tout ouvert comme union de pavés presque disjoints.

Définition 7.104.

Soit (X, d) un espace métrique. Un sous-ensemble $A \subset X$ est **borné** s'il existe une boule de X contenant A .

Proposition 7.105.

Toute réunion finie d'ensembles bornés est un ensemble borné. Toute partie d'un ensemble borné est un ensemble borné.

31. Qui possède une partie dense dénombrable, définition 7.37.

32. Base de topologie, définition 7.2.

33. Définition 7.2.

7.6.1.2 Continuité et compacité

Un résultat important dans la théorie des fonctions sur les espaces vectoriels normés est qu'une fonction continue sur un compact est bornée et atteint ses bornes. Ce résultat sera (dans d'autres cours) énormément utilisé pour trouver des maximums et minimums de fonctions. Le théorème exact est le suivant.

Lemme 7.106 (de Lebesgue[164]).

Soit (X, d) un espace métrique tel que toute suite ait une sous-suite convergente à l'intérieur de l'espace. Si $\{V_i\}$ est un recouvrement par des ouverts de X , alors il existe ϵ tel que pour tout $x \in X$, nous ayons $B(x, \epsilon) \subset V_i$ pour un certain i .

Démonstration. Par l'absurde, nous supposons que pour tout n , il existe un $x_n \in X$ tel que la boule $B(x_n, \frac{1}{n})$ n'est contenue dans aucun des V_i . Ce des x_n nous extrayons une sous-suite convergente (que nous nommons encore (x_n)) et nous posons $x_n \rightarrow x$. Pour n assez grand ($\frac{1}{n} < \epsilon$) nous avons $x_n \in B(x, \epsilon)$, donc tous les x_n suivants sont dans le V_i qui contient x . $\square$

Lemme 7.107 ([164]).

Soit (X, d) un espace métrique tel que toute suite possède une sous-suite convergente. Pour tout $\epsilon > 0$, il existe un ensemble fini $\{x_i\}_{i \in I}$ tel que les boules $B(x_i, \epsilon)$ recouvrent X .

Démonstration. Soit par l'absurde un $\epsilon > 0$ contredisant le lemme. Il n'existe pas d'ensemble fini autour des points duquel les boules de taille ϵ recouvrent X .

Nous construisons par récurrence une suite ne possédant pas de sous-suites convergente. Le premier terme, x_0 est pris arbitrairement dans X . Ensuite si nous en avons N termes, nous savons que les boules de rayon ϵ et centrées en les points $\{x_i\}_{i=1, \dots, N}$ ne recouvrent pas X . Donc nous prenons x_{N+1} hors de l'union de ces boules.

Ainsi nous avons une suite (x_n) dont tous les termes sont à distance plus grande que ϵ les uns des autres. Une telle suite ne peut pas contenir de sous-suite convergente. Contradiction. $\square$

Théorème 7.108 (Bolzano-Weierstrass[164], thème 12).

Un espace métrique est compact si et seulement si toute suite admet une sous-suite qui converge à l'intérieur de l'espace.

Démonstration. Soient X un espace métrique compact et (x_n) une suite dans X . Nous considérons la suite de fermés emboîtés

$$X_n = \overline{\{x_k \text{ tel que } k > n\}}. \quad (7.91)$$

Ce sont des fermés ayant la propriété d'intersection finie non vide, et donc la proposition 7.59 nous dit qu'ils ont une intersection non vide. Un élément de cette intersection est automatiquement un point d'accumulation de la suite³⁴.

Nous passons à l'autre sens. Nous supposons que toute suite dans X contient une sous-suite convergente, et nous considérons $\{V_i\}_{i \in I}$, un recouvrement de X par des ouverts. Par le lemme 7.106, nous considérons un ϵ tel que pour tout x , il existe un $i \in I$ avec $B(x, \epsilon) \subset V_i$. Par le lemme 7.107, nous considérons un ensemble fini $\{y_i\}_{i \in A}$ tel que les boules $B(y_i, \epsilon)$ recouvrent X .

Par construction, chacune de ces boules $B(y_i, \epsilon)$ est contenue dans un des ouverts V_i . Nous sélectionnons donc parmi les V_i le nombre fini qu'il faut pour recouvrir les $B(y_i, \epsilon)$ et donc pour recouvrir X . $\square$

Exemple 7.109 (Non compacité de la boule unité en dimension infinie).

Le théorème de Bolzano-Weierstrass permet de voir tout de suite que la boule unité n'est pas compacte dans un espace vectoriel de dimension infinie : la suite des vecteurs de base ne possède pas de sous-suites convergentes. $\triangle$

Le théorème de Bolzano-Weierstrass 7.108 a l'importante conséquence suivante.

34. Définition 7.29.

Théorème 7.110 (Weierstrass).

Une fonction continue à valeurs réelles définie sur un compact est bornée et atteint ses bornes.

Démonstration. Soient K un compact et $f: K \rightarrow \mathbb{R}$ une fonction continue. Nous désignons par A l'ensemble des valeurs prises par f sur K :

$$A = f(K) = \{f(x) \text{ tel que } x \in K\}. \quad (7.92)$$

Nous considérons le supremum $M = \sup A = \sup_{x \in K} f(x)$ avec la convention comme quoi si A n'est pas borné supérieurement, nous posons $M = \infty$ (voir définition 1.323).

Nous allons maintenant construire une suite (x_n) de deux façons différentes suivant que $M = \infty$ ou non.

- (1) Si $M = \infty$, nous choisissons, pour chaque $n \in \mathbb{N}$, un $x_n \in K$ tel que $f(x_n) > n$. Cela est certainement possible parce que si A n'est pas borné, nous pouvons y trouver des nombres aussi grands que nous voulons.
- (2) Si $M < \infty$, nous savons que pour tout ε , il existe un $y \in A$ tel que $y > M - \varepsilon$. Pour chaque n , nous choisissons donc $x_n \in K$ tel que $f(x_n) > M - \frac{1}{n}$.

Quel que soit le cas dans lequel nous sommes, la suite (x_n) est une suite dans K qui est compact, et donc nous pouvons en extraire une sous-suite convergente à l'intérieur de K par le théorème de Bolzano-Weierstrass 7.108. Afin d'alléger la notation, nous allons noter (x_n) la sous-suite convergente. Nous avons donc

$$x_n \rightarrow x \in K. \quad (7.93)$$

Par la proposition 7.85, nous avons que f prend en x la valeur

$$f(x) = \lim_{n \rightarrow \infty} f(x_n). \quad (7.94)$$

Donc $f(x) < \infty$. Évidemment, si nous avions été dans le cas où $M = \infty$, la suite x_n aurait été choisie pour avoir $f(x_n) > n$ et donc il n'aurait pas été possible d'avoir $\lim_{n \rightarrow \infty} f(x_n) < \infty$. Nous en concluons que $M < \infty$, et donc que f est bornée sur K .

Afin de prouver que f atteint sa borne, c'est-à-dire que $M \in A$, nous considérons les inégalités

$$M - \frac{1}{n} < f(x_n) \leq M. \quad (7.95)$$

En passant à la limite $n \rightarrow \infty$, ces inégalités deviennent

$$M \leq f(x) \leq M, \quad (7.96)$$

et donc $f(x) = M$, ce qui prouve que f atteint sa borne M au point $x \in K$. $\square$

Lemme 7.111 ([1]).

Soient des compacts A, B et une fonction continue $f: A \times B \rightarrow \mathbb{R}$. Alors

$$\sup_{(x,y) \in A \times B} |f(x,y)| = \sup_{x \in A} \left(\sup_{y \in B} |f(x,y)| \right). \quad (7.97)$$

Démonstration. Pour chaque $x \in A$, la fonction $f_x: B \rightarrow \mathbb{R}$ donnée par $f_x(y) = |f(x,y)|$ est continue et atteint donc sa borne³⁵ en $y_M(x)$. Notons que cela ne définit pas univoquement $y_M(x)$ parce que f_x peut atteindre son maximum en plusieurs points. L'important est que pour tout x , le nombre $|f(x, y_M(x))|$ ne dépend pas du choix de $y_M(x)$ parmi les y qui réalisent le maximum.

Notons (x_0, y_0) le point de $A \times B$ sur lequel $|f|$ réalise son maximum³⁶ :

$$\sup_{(x,y) \in A \times B} |f(x,y)| = |f(x_0, y_0)|. \quad (7.98)$$

35. Théorème 7.110.

36. Encore une fois, ce point n'est pas déterminé de façon unique par cette propriété.

Nous avons d'une part

$$\sup_{x \in A} \left(\sup_{y \in B} |f(x, y)| \right) = \sup_{x \in A} |f(x, y_M(x))| \leq |f(x_0, y_0)| \quad (7.99)$$

Et d'autre part,

$$\sup_{x \in A} \left(\sup_{y \in B} |f(x, y)| \right) \leq \sup_{x \in A} \sup_{y \in B} |f(x_0, y_0)| \quad (7.100a)$$

$$= |f(x_0, y_0)| \quad (7.100b)$$

$$\leq |f(x_0, y_M(x_0))| \quad (7.100c)$$

$$\leq \sup_{x \in A} |f(x, y_M(x))| \quad (7.100d)$$

$$\leq \sup_{x \in A} \left(\sup_{y \in B} |f(x, y)| \right). \quad (7.100e)$$

Vu que les premiers et derniers termes des inégalités (7.100) sont égaux, toutes les inégalités sont en réalité des égalités. En particulier, en reprenant (7.98),

$$\sup_{(x, y) \in A \times B} |f(x, y)| = |f(x_0, y_0)| = \sup_{x \in A} \left(\sup_{y \in B} |f(x, y)| \right). \quad (7.101)$$

□

7.6.2 Distance à un ensemble

Définition 7.112.

Si A est une partie de l'espace métrique (X, d) , et si $b \in X$, nous définissons

$$d(b, A) = \inf_{y \in A} d(b, y). \quad (7.102)$$

Lemme 7.113 ([1]).

Si A est fermé dans (X, d) , et si $b \in X$ vérifie $d(b, A) = 0$, alors $b \in A$.

Démonstration. Vu que A est fermé, le complémentaire A^c est ouvert (c'est la définition 7.3). Supposons que $b \in A^c$. Alors il existe $r > 0$ tel que $B(b, r) \subset A^c$. Si $a \in A$ nous avons alors $d(b, A) \geq r$ et donc $d(b, A) \geq r > 0$. Cela contredit l'hypothèse $d(b, A) = 0$.

Nous en déduisons que b n'est pas dans A^c et qu'il est donc dans A . □

Exemple 7.114 (Pas avec un ouvert).

En prenant l'ouvert $A =]0, 1[$ dans $\mathbb{R}$ nous avons $d(0, A) = 0$, alors que 0 n'est pas dans A . △

Lemme 7.115 ([1]).

Soient un espace métrique (X, d) ainsi qu'une partie $A \subset X$. Soit $r > 0$. La partie

$$\mathcal{O} = \{x \in X \text{ tel que } d(x, A) < r\} \quad (7.103)$$

est ouverte.

Démonstration. Soit $y \in \mathcal{O}$; nous avons $d(y, A) < r$. Autrement dit,

$$\inf_{a \in A} d(y, a) < r \quad (7.104)$$

et donc il existe $a \in A$ tel que $d(y, a) < r$. Soit $\delta = d(y, a) < r$. Nous montrons à présent que $B(y, r - \delta)$ est dans $\mathcal{O}$. En effet si $z \in B(y, r - \delta)$, alors

$$d(z, a) \leq d(z, y) + d(y, a) < r - \delta + \delta = r. \quad (7.105)$$

□

Lemme 7.116 ([1]).

Soit un fermé F de l'espace métrique (X, d) . Si $a \in X$ vérifie $d(a, F) = 0$, alors $a \in F$.

Démonstration. Supposons que $d(a, F) = 0$. Cela signifie que $\{d(a, x)\}_{x \in F} = 0$. Il existe donc une suite (x_k) dans F telle que $d(a, x_k) \rightarrow 0$.

Cela signifie que $x_k \xrightarrow{(X, d)} a$. La proposition 7.32 nous dit alors que $a \in F$. $\square$

Lemme 7.117 ([1]).

Si A est une partie de (X, d) , alors la fonction

$$\begin{aligned} f: \Omega &\rightarrow [0, \infty[\\ x &\mapsto d(x, A) \end{aligned} \tag{7.106}$$

est continue.

7.6.3 Norme**Définition 7.118** ([165], thème 7).

Soit E un espace vectoriel (pas spécialement de dimension finie) sur le corps $\mathbb{K}$ ($= \mathbb{R}$ ou $\mathbb{C}$). Une **norme** sur E est une application $N: E \rightarrow \mathbb{R}^+$ telle que

- (1) $N(x) \geq 0$ pour tout x .
- (2) $N(x) = 0$ si et seulement si $x = 0$;
- (3) $N(\lambda x) = |\lambda|N(x)$ pour tout $\lambda \in \mathbb{R}$ et $x \in E$;
- (4) $N(x + y) \leq N(x) + N(y)$

pour tout $x, y \in E$ et pour tout $\lambda \in \mathbb{K}$.

La propriété (4) est appelée **inégalité triangulaire**.

Un espace vectoriel muni d'une norme est un **espace vectoriel normé**.

En prenant $\lambda = -1$ dans la propriété (3), nous trouvons immédiatement que $N(-x) = N(x)$.

Proposition 7.119.

Toute norme N sur l'espace vectoriel E vérifie l'inégalité

$$|N(x) - N(y)| \leq N(x - y) \tag{7.107}$$

pour tout $x, y \in E$.

Démonstration. Nous avons, en utilisant le point (4) de la définition 7.118,

$$N(x) = N(x - y + y) \leq N(x - y) + N(y), \tag{7.108a}$$

$$N(y) = N(y - x + x) \leq N(y - x) + N(x). \tag{7.108b}$$

Supposons d'abord que $N(x) \geq N(y)$. Dans ce cas, en utilisant (7.108a),

$$|N(x) - N(y)| = N(x) - N(y) \leq N(x - y) + N(y) - N(y) = N(x - y). \tag{7.109}$$

Si par contre $N(x) \leq N(y)$, alors nous utilisons (7.108b) et nous trouvons

$$|N(x) - N(y)| = N(y) - N(x) \leq N(y - x) + N(x) - N(x) = N(y - x). \tag{7.110}$$

Dans les deux cas, nous avons retrouvé l'inégalité annoncée. $\square$

Cette proposition signifie aussi que

$$-N(x - y) \leq N(x) - N(y) \leq N(x - y). \tag{7.111}$$

7.120.

Afin de suivre une notation proche de celle de la valeur absolue, à partir de maintenant, la norme d'un vecteur v sera notée $\|v\|$ au lieu de $N(v)$. La proposition 7.119 s'énoncera donc

$$|\|x\| - \|y\|| \leq \|x - y\|. \quad (7.112)$$

Un espace vectoriel E muni d'une norme est, on l'a déjà dit, un **espace vectoriel normé**; on le notera $(E, \|\cdot\|)$ pour distinguer la norme fixée.

Une autre inégalité utile de temps en temps.

Corolaire 7.121.

Si a et b sont dans un espace vectoriel normé, alors

$$|\|a - b\| - \|b\|| \leq \|a\|. \quad (7.113)$$

Démonstration. Il s'agit seulement de la proposition 7.119 avec $x = a - b$ et $y = -b$. $\square$

Lemme-Définition 7.122 (Distance induite par une norme).

Soit un espace vectoriel normé $(E, \|\cdot\|)$. Nous posons

$$d(x, y) = \|x - y\|. \quad (7.114)$$

Alors

(1) d est invariante par translations : $d(a, b) = d(a + u, b + u)$

(2) d est une distance³⁷ sur E .

C'est la **distance induite** par la norme.

Démonstration. Le fait que la formule (7.114) soit invariante par translations est immédiat. En ce qui concerne le fait que ce soit une distance, le seul point délicat à vérifier est l'inégalité triangulaire. Mais, pour tous $x, y, z \in E$, on a

$$d(x, y) = \|x - y\| = \|x - z + z - y\| \leq \|x - z\| + \|z - y\| = d(x, z) + d(z, y). \quad (7.115)$$

$\square$

Définition 7.123.

La topologie associée à une norme est celle associée à la distance donnée en 7.122 par le théorème 7.99.

Corolaire 7.124.

Un espace vectoriel normé est un espace vectoriel topologique : en d'autres mots, l'addition et la multiplication par un élément du corps sont continues.

Nous étudierons plus en détail les espaces vectoriels topologiques à partir de la définition 7.178.

7.6.4 Topologie et matrices**Lemme-Définition 7.125** (Topologie sur les matrices).

Si $\mathbb{K}$ est un corps valué³⁸, alors l'opération

$$\begin{aligned} \|\cdot\|_{\mathbb{M}} : \mathbb{M}(n \times m, \mathbb{K}) &\rightarrow \mathbb{R}^+ \\ M &\mapsto \max_{kl} \|M_{kl}\|_{\mathbb{K}}. \end{aligned} \quad (7.116)$$

est une norme³⁹.

Cette norme est appelée **norme maximum** et nous considérons sur $\mathbb{M}(n \times m, \mathbb{K})$ la topologie associée à cette norme⁴⁰

37. Définition 7.98.

38. Définition 1.334.

39. Définition 7.118.

40. Définition 7.123.

Proposition 7.126.

La multiplication matricielle est une opération continue.

7.7 Produit fini d'espaces vectoriels normés

Dans cette sections nous parlons de produits finis d'espaces. Cela ne signifie pas que chacun des espaces soient séparément de dimension finie.

7.7.1 Distance et norme produit**Proposition-Définition 7.127** (Distance produit).

Si $(E_1, d_1), \dots, (E_n, d_n)$ sont des espaces métriques alors la formule

$$d(x, y) = \max_{i=1, \dots, n} d_i(x_i, y_i) \quad (7.117)$$

définit une distance sur le produit cartésien $E = E_1 \times \dots \times E_n$. Elle est la **distance produit**.

La définition de la norme sur un produit d'espaces vectoriels normés découle immédiatement de la définition de la distance 7.127 :

Lemme-Définition 7.128 ([166]).

Soient V et W deux espaces vectoriels sur $\mathbb{K}$. Si (v_1, w_1) et (v_2, w_2) sont des éléments de $V \times W$ et si λ est un élément de $\mathbb{K}$, alors les opérations suivantes donnent une structure d'espace vectoriel au produit $V \times W$:

- $(v_1, w_1) + (v_2, w_2) = (v_1 + v_2, w_1 + w_2)$
- $\lambda(v_1, w_1) = (\lambda v_1, \lambda w_1)$.

Démonstration. Il faut seulement faire les vérifications d'usage. □

Lemme-Définition 7.129.

Soient deux espaces vectoriels normés V et W .

(1) *L'opération*

$$\|(v, w)\|_{V \times W} = \max\{\|v\|_V, \|w\|_W\}. \quad (7.118)$$

est une norme⁴¹ sur $V \times W$.

(2) *La topologie de cette norme⁴² est la même que la topologie produit⁴³ sur $V \times W$.*

Démonstration. En plusieurs parties.

Norme On doit vérifier les trois conditions de la définition 7.118.

- Soit (v, w) dans $V \times W$ tel que $\|(v, w)\|_{V \times W} = \max\{\|v\|_V, \|w\|_W\} = 0$. Alors $\|v\|_V = 0$ et $\|w\|_W = 0$, donc $v = 0_V$ et $w = 0_W$. Cela implique $(v, w) = (0_v, 0_w) = 0_{V \times W}$.
- Pour tout a dans $\mathbb{R}$ et (v, w) dans $V \times W$, la norme $\|a(v, w)\|_{V \times W}$ se calcule de la façon suivante :

$$\|a(v, w)\|_{V \times W} = \max\{\|av\|_V, \|aw\|_W\} = |a| \max\{\|v\|_V, \|w\|_W\} = |a| \|(v, w)\|_{V \times W}. \quad (7.119)$$

- Soient (v_1, w_1) et (v_2, w_2) dans $V \times W$.

$$\begin{aligned} \|(v_1, w_1) + (v_2, w_2)\|_{V \times W} &= \max\{\|v_1 + v_2\|_V, \|w_1 + w_2\|_W\} \\ &\leq \max\{\|v_1\|_V + \|v_2\|_V, \|w_1\|_W + \|w_2\|_W\} \\ &\leq \max\{\|v_1\|_V, \|w_1\|_W\} + \max\{\|v_2\|_V, \|w_2\|_W\} \\ &= \|(v_1, w_1)\|_{V \times W} + \|(v_2, w_2)\|_{V \times W}. \end{aligned} \quad (7.120)$$

41. Définition 7.118.

42. Topologie associée à une norme : c'est la topologie associée à la distance correspondante, définition 7.123.

43. Topologie produit, définition 7.15.

Dans cette preuve, nous considérons la « topologie de $V \times W$ » comme étant la topologie produit et « la topologie métrique de $V \times W$ » la topologie de la norme produit.

Équivalence Dans un sens La définition 7.15 de la topologie produit dit qu'une prébase de $V \times W$ est donnée par

$$\{B(v, r) \times B(w, s) \text{ tel que } v \in V; w \in W; r, s > 0\}. \quad (7.121)$$

Nous prouvons maintenant que la partie $S = B(v_0, r) \times B(w_0, s)$ est un ouvert de l'espace $(V \times W, \|\cdot\|_{V \times W})$. Pour cela nous prouvons que tout élément de S contient un voisinage métrique contenu dans S .

Soit $(v_1, w_1) \in S$. Nous posons

$$d((v_1, w_1), (v_0, w_0)) = \delta < \max\{r, s\}. \quad (7.122)$$

Nous considérons $\epsilon > 0$ et nous montrons que si ϵ est assez petit, $B((v_1, w_1), \epsilon) \subset S$. Pour cela nous considérons $(v, w) \in B((v_1, w_1), \epsilon)$ et nous calculons un tout petit peu :

$$d((v, w), (v_0, w_0)) \leq d((v, w), (v_1, w_1)) + d((v_1, w_1), (v_0, w_0)) \quad (7.123a)$$

$$< \epsilon + \delta. \quad (7.123b)$$

Si ϵ est assez petit, le tout reste plus petit que $\max\{r, s\}$.

Donc S est bien un ouvert métrique par le théorème 7.7. Vu que la topologie métrique contient une prébase de la topologie produit, tout ouvert de la topologie produit est un ouvert de la topologie métrique.

Dans l'autre sens Soient un ouvert métrique $\mathcal{O}$ ainsi que $(v_0, w_0) \in \mathcal{O}$; il existe $r > 0$ tel que

$$B((v_0, w_0), r) \subset \mathcal{O}. \quad (7.124)$$

Nous affirmons que $B(v_0, r) \times B(w_0, r)$ est contenu dans $\mathcal{O}$, de telle sorte que $\mathcal{O}$ soit un ouvert de la topologie produit. Pour $(v_1, w_1) \in B(v_0, r) \times B(w_0, r)$ nous avons

$$d((v_1, w_1), (v_0, w_0)) = \max\{\|v_1 - v_0\|, \|w_1 - w_0\|\} < r \quad (7.125)$$

parce que $v_1 \in B(v_0, r)$ et $w_1 \in B(w_0, r)$.

Donc tout élément de $\mathcal{O}$ admet un voisinage « produit » contenu dans $\mathcal{O}$; donc $\mathcal{O}$ est ouvert pour la topologie produit. □

7.130.

En particulier, pour la topologie de la norme maximum, la convergence d'une suite implique la convergence « composante par composante » par la proposition 7.40.

7.8 Topologie réelle en dimension n

Nous considérons sur $\mathbb{R}$ la topologie donnée par la valeur absolue, et sur $\mathbb{R}^n$ celle de la topologie produit ou du maximum, qui sont identiques par le lemme 7.129.

En particulier, nous n'avons pas encore la norme donnée par $\|x\| = \sqrt{\sum_i x_i^2}$, parce qu'elle demande la racine carrée, définie en 10.82.

7.8.1 Ouverts et fermés

Proposition 7.131.

Une partie A de $\mathbb{R}^n$ est ouverte si et seulement si pour tout $a \in A$ il existe $r > 0$ tel que $B(a, r) \subset A$.

Cette proposition est évidemment à mettre en rapport avec le théorème 7.7.

Lemme 7.132.

Pour tout $x \in \mathbb{R}^n$ et tout $r > 0$ la boule⁴⁴ $B(x, r)$ est ouverte.

Démonstration. Afin de prouver que la boule est ouverte, nous prenons un point $p \in B(x, r)$, et nous allons montrer qu'il existe une boule autour de p qui est contenue dans $B(x, r)$.

Étant donné que $p \in B(x, r)$, nous avons $d(p, x) < r$. Prouvons que la boule $B(p, r - d(p, x))$ est contenue dans $B(x, r)$. Pour cela, nous prenons $p' \in B(p, r - d(p, x))$, et nous essayons de prouver que $p' \in B(x, r)$. En effet, en utilisant l'inégalité triangulaire,

$$d(x, p') \leq d(x, p) + d(p, p') \leq d(x, p) + r - d(p, x) = r. \quad (7.126)$$

□

7.8.2 Intérieur, adhérence et frontière**7.133.**

La notion d'intérieur est déjà faite dans la définition 7.22.

La notion d'adhérence a déjà été définie en 7.24, et précisé par le lemme 7.25. Dans le cas de $\mathbb{R}^n$ dans lequel les boules forment une base de la topologie nous pouvons encore préciser de la façon suivante :

$$x \in \text{Adh } A \stackrel{\text{def}}{\iff} \forall \epsilon > 0, B(x, \epsilon) \cap A \neq \emptyset \quad (7.127)$$

Proposition 7.134.

Pour $A \subset \mathbb{R}^n$, nous avons

$$\text{Int } A \subseteq A \subseteq \text{Adh } A$$

Définition 7.135.

La **frontière** ou le **bord** de A est défini par $\partial A = \text{Adh } A \setminus \text{Int } A$. L'ensemble A est un **ouvert** si $A = \text{Int } A$, et c'est un **fermé** si $A = \text{Adh } A$.

Lemme 7.136 (Caractérisation équivalente de la frontière).

Soient X un espace topologique et $S \subset X$. Un point $x \in X$ est dans ∂S si et seulement si tout voisinage de x contient un point de S et un point de S^c .

Démonstration. Supposons que tout voisinage de x contienne un point de S et un point de S^c . Alors $x \in \text{Adh}(S)$ (définition 7.24), mais pas dans l'intérieur de S parce que x ne possède pas de voisinage contenu dans S . Donc $x \in \partial S$.

À l'inverse, si $x \in \partial S$ alors x est dans l'adhérence de S et tout voisinage de x contient un point de S . Mais x n'est pas dans l'intérieur de S et tout voisinage de x contient un point qui n'est pas dans S , aka un point de S^c . □

Corolaire 7.137.

Un ensemble et son complémentaire ont même frontière.

Démonstration. Conséquence du lemme 7.136. Les points de $\partial(S^c)$ sont caractérisés par le fait que tout voisinage contient un point de S^c et un point de $(S^c)^c = S$. □

Exemple 7.138.

Soit $X = [0, 1]$ muni de la topologie de la distance $|x - y|$ (définition 7.99). Les points 0 et 1 ne sont pas dans la frontière de X . En effet une boule ouverte autour de 1 est un ensemble de la forme

$$B(1, r) = \{x \in X \text{ tel que } |x - 1| < r\} =]1 - r, 1] \quad (7.128)$$

où nous avons supposé $r < 1$.

Les points 0 et 1 sont par contre sur la frontière de $[0, 1]$ lorsque cet ensemble est vu comme partie de l'espace métrique $\mathbb{R}$. △

44. Définition 7.99.

Lemme 7.139 (Passage de douane[167, 168]).

Dans un espace topologique, toute partie connexe qui rencontre à la fois une partie A et son complémentaire rencontre nécessairement la frontière de A .

Démonstration. Nommons γ la partie connexe qui intersecte A et A^c . Les ouverts $\text{Int}(A)$ et $X \setminus \bar{A}$ ne peuvent pas recouvrir γ parce que ce sont deux ouverts disjoints alors que γ est connexe (voir la définition 7.44 de la connexité). Donc γ doit contenir des points qui sont dans $\bar{A}$ mais pas dans $\text{Int}(A)$. C'est-à-dire des points de ∂A . $\square$

On vérifiera que les notations et les dénominations sont cohérentes en prouvant la proposition suivante.

Proposition 7.140.

Pour $\epsilon > 0$,

- (1) l'adhérence de $B(x, \epsilon)$ est $\bar{B}(x, \epsilon)$,
- (2) l'intérieur de $\bar{B}(x, \epsilon)$ est $B(x, \epsilon)$,
- (3) la boule ouverte $B(x, \epsilon)$ est un ouvert,
- (4) la boule fermée $\bar{B}(x, \epsilon)$ est un fermé.

Nous avons également les liens suivants entre intérieur, adhérence, ouvert, fermé et passage au complémentaire (noté ^{c}) :

Proposition 7.141.

Si $A \subset \mathbb{R}^n$ et $A^c = \mathbb{R}^n \setminus A$, nous avons

- (1) $(\text{Int } A)^c = \text{Adh}(A^c)$ et $(\text{Adh } A)^c = \text{Int}(A^c)$,
- (2) A est ouvert si et seulement si A^c est fermé,
- (3) $\text{Int } A$ est le plus grand ouvert contenu dans A ,
- (4) $\text{Adh } A$ est le plus petit fermé contenant A ,

Exemple 7.142.

Il n'est en général pas vrai que $\overline{A \cap B} = \bar{A} \cap \bar{B}$. Par exemple si $A = [0, 1[$ et $B =]1, 2]$. Dans ce cas, $A \cap B = \emptyset$ alors que $\bar{A} \cap \bar{B} = \{1\}$. $\triangle$

7.8.3 Point d'accumulation, point isolé

Les définitions de point d'accumulation et de point isolé sont 7.29 et 7.30. Nous voyons maintenant ce que ces définitions donnent dans le cas de l'espace topologique $\mathbb{R}$.

Lemme 7.143.

Soit $D \subset \mathbb{R}$. Un point $a \in D$ est isolé dans D si et seulement si il existe $\epsilon > 0$ tel que

$$[a - \epsilon, a + \epsilon] \cap D = \{a\}. \quad (7.129)$$

Autrement dit, il existe un intervalle autour de a dans lequel a est le seul élément de D .

Lemme 7.144.

Un point $a \in \mathbb{R}$ est un point d'accumulation de D si pour tout $\epsilon > 0$,

$$([a - \epsilon, a + \epsilon] \setminus \{a\}) \cap D \neq \emptyset. \quad (7.130)$$

Autrement dit, quel que soit l'intervalle autour de a que l'on considère, le point a n'est pas tout seul dans D .

Exemple 7.145.

Prenons $D = [0, 1[\cup]2, 3]$. Cet ensemble n'a pas de point isolé, et l'ensemble de ses points d'accumulation est $[0, 1] \cup [2, 3]$.

Notez que les points 1 et 2 sont des points d'accumulation de D qui ne font pas partie de D . Il est possible d'être un point d'accumulation de D sans être dans D , mais pour être un point isolé dans D , il faut être dans D . $\triangle$

Exemple 7.146.

Soit $D = \{\frac{1}{n}\}_{n \in \mathbb{N}}$. Tous les points de cet ensemble sont des points isolés (vérifier!). Aucun point de D n'est point d'accumulation. Cependant 0 est un point d'accumulation. $\triangle$

Exemple 7.147.

Soit $D =]1, 2[\cup \{12\}$. Le point 12 est adhérence, mais pas d'accumulation parce que le voisinage $]9, 14[$ n'intersectionne pas $D \setminus \{12\}$. $\triangle$

7.8.4 Limite de suite

Définition 7.148 (Limite d'une suite dans $\mathbb{R}^m$).

Une suite de points (x_n) dans $\mathbb{R}^m$ est dite **convergente** s'il existe un élément $\ell \in \mathbb{R}^m$ tel que

$$\forall \varepsilon > 0, \exists N \in \mathbb{N} \text{ tel que } \forall n \geq N, \|x_n - \ell\| < \varepsilon. \quad (7.131)$$

Dans ce cas, nous disons que ℓ est la **limite** de la suite (x_n) et nous écrivons $\lim x_n = \ell$ ou plus simplement $x_n \rightarrow \ell$.

Notez aussi la similarité avec la définition 10.22.

Remarque 7.149.

Nous n'écrivons pas « $\lim_{n \rightarrow \infty} x_n$ » parce que, lorsqu'on parle de suites, la limite est *toujours* lorsque n tend vers l'infini. Il n'y a aucun intérêt à chercher par exemple $\lim_{n \rightarrow 4} x_n$ parce que cela vaudrait x_4 et rien d'autre.

Ceci est une différence importante avec les limites de fonctions.

Lemme 7.150 (Unicité de la limite).

Il ne peut pas y avoir deux nombres différents qui satisfont à la condition (7.131). En d'autres termes, si ℓ et ℓ' sont deux limites de la suite (x_n) , alors $\ell = \ell'$.

Démonstration. Soit $\varepsilon > 0$. Nous considérons N tel que

$$\|x_n - \ell\| < \varepsilon \quad (7.132)$$

pour tout $n \geq N$, et $N' > 0$ tel que

$$\|x_n - \ell'\| < \varepsilon \quad (7.133)$$

pour tout $n > N'$. Maintenant, nous prenons n plus grand que N et N' de telle façon que les deux équations pour x_n soient vérifiées en même temps. Alors

$$\|\ell - \ell'\| = \|\ell - x_n + x_n - \ell'\| \leq \|\ell - x_n\| + \|x_n - \ell'\| < 2\varepsilon. \quad (7.134)$$

Cela prouve que $\|\ell - \ell'\| = 0$. $\square$

Le théorème de Bolzano-Weierstrass 7.108 dit que dans le cas métrique, la compacité séquentielle est équivalente à la compacité.

7.9 Topologie et distance

Lemme 7.151.

Soient (X_1, d_1) et (X_2, d_2) des espaces métriques séparables. Alors $X_1 \times X_2$ admet une base dénombrable de topologie constituée de produits de boules de X_1 par des boules de X_2 . Plus précisément si A_i est dénombrable et dense dans X_i alors l'ensemble des produits

$$\{B(y_1, r_1) \times B(y_2, r_2)\}_{\substack{y_i \in A_i \\ r_i \in \mathbb{Q}^+}} \quad (7.135)$$

est une base de topologie pour $X_1 \times X_2$.

Démonstration. Soit $\mathcal{O}$ un ouvert de $X_1 \times X_2$ et $(x_1, x_2) \in \mathcal{O}$. Par définition de la topologie produit⁴⁵, il existe $r_1, r_2 \in \mathbb{Q}^+$ tels que $B(x_1, r_1) \times B(x_2, r_2) \subset \mathcal{O}$. Les parties A_i étant denses, il existe $y_i \in B(x_i, r_i/2) \cap A_i$. Avec ces choix nous avons $x_i \in B(y_i, \frac{r_i}{2})$. Nous avons donc

$$(x_1, x_2) \in B(y_1, \frac{r_1}{2}) \times B(y_2, \frac{r_2}{2}). \quad (7.136)$$

Il est facile de voir que $B(y_i, r_i/2) \subset B(x_i, r_i)$. En effet si $z_i \in B(y_i, r_i/2)$ alors

$$d_i(z_i, x_i) \leq d(z_i, y_i) + d(y_i, x_i) \leq \frac{r_i}{2} + \frac{r_i}{2} = r_i. \quad (7.137)$$

Au final,

$$(x_1, x_2) \in B(y_1, \frac{r_1}{2}) \times B(y_2, \frac{r_2}{2}) \subset \mathcal{O}. \quad (7.138)$$

□

Définition 7.152.

Si (X, d_X) et (Y, d_Y) sont des espaces métriques, une **isométrie** est une application bijective $f: X \rightarrow Y$ telle que pour tout $x, y \in X$ nous ayons

$$d_Y(f(x), f(y)) = d_X(x, y). \quad (7.139)$$

Remarque 7.153.

Une application vérifiant (7.139) est automatiquement injective. En pratique, il ne faut donc vérifier que la surjectivité.

Exemple 7.154 (Manque de surjectivité).

Si $X = [0, \infty[$ et $f(x) = x + 1$ alors f vérifie (7.139) pour la distance $d(x, y) = |x - y|$, mais n'est pas surjective. $\triangle$

Proposition-Définition 7.155 (Groupe des isométries).

Si (X, d) est un espace métrique,

- (1) l'ensemble des isométries de X , noté $\text{Isom}(X)$ est un groupe pour la composition.
- (2) Ce groupe agit fidèlement⁴⁶ sur X .

Proposition 7.156.

Une isométrie entre deux espaces métriques est continue.

Démonstration. Soient $f: X \rightarrow Y$ une application isométrique et $\mathcal{O}$ un ouvert de Y . Soit $a \in f^{-1}(\mathcal{O})$; si $d(a, b) < r$, alors $d(f(a), f(b)) < r$ et donc $b \in f^{-1}(B(f(a), r))$. Donc autour de chaque point de $f^{-1}(\mathcal{O})$ nous pouvons trouver une boule ouverte contenue dans $f^{-1}(\mathcal{O})$, ce qui prouve que $f^{-1}(\mathcal{O})$ est ouvert. $\square$

Exemple 7.157.

Si X est un ensemble, nous pouvons écrire la **distance discrète** :

$$d(x, y) = \begin{cases} 0 & \text{si } x = y \\ 1 & \text{si } x \neq y. \end{cases} \quad (7.140)$$

La topologie résultante est la topologie discrète, côtoyée dans l'exemple 7.9⁴⁷.

Pour cette métrique, le groupe des isométries est le groupe symétrique de X , c'est-à-dire le groupe de toutes les bijections de X sur lui-même. $\triangle$

45. Définition 7.15.

46. Si vous ne savez pas ce que c'est, alors vous avez zappé la définition 2.49.

47. Vérifiez-le tout de même!

7.9.0.1 Distance point-ensemble

Définition 7.158.

Si A est une partie de l'espace métrique (X, d) et si $x \in X$, nous disons que la **distance** entre A et x est le nombre

$$d(x, A) = \inf_{a \in A} d(x, a). \quad (7.141)$$

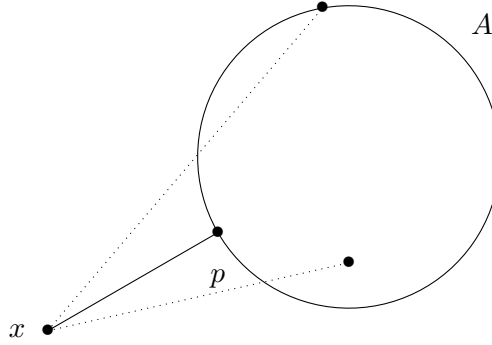


FIGURE 7.1 – La distance entre x et A est donnée par la distance entre x et p . Les distances entre x et les autres points de A sont plus grandes que $d(x, p)$.

7.9.1 Suites et espaces métriques

Proposition 7.159 (Caractérisation séquentielle de la limite[1]).

Soient deux espaces métriques X et Y ainsi qu'une fonction $f: X \rightarrow Y$. Soit $a \in X$ et $\ell \in Y$. On a

$$\lim_{x \rightarrow a} f(x) = \ell, \quad (7.142)$$

si et seulement si, pour toute suite (x_k) telle que $x_k \rightarrow a$, on a

$$\lim f(x_k) = \ell. \quad (7.143)$$

Par ailleurs, l'une des deux limites existe si et seulement si l'autre existe.

Démonstration. Le sens direct est la proposition 7.84. Pour la réciproque, nous passons par la contraposée. C'est-à-dire que nous supposons que ℓ n'est pas une limite de f pour $x \rightarrow a$. Il existe un ϵ tel que pour tout δ , il existe un x vérifiant $d_X(x; a) < \delta$ et $d_Y(f(x); \ell) > \epsilon$.

Nous construisons à présent une suite de la manière suivante. Pour $\delta = \frac{1}{n}$ nous considérons x_n tel que $d_X(x_n; a) < \delta$ et $d_Y(f(x_n); \ell) > \epsilon$. Cette suite converge vers a , mais la suite $f(x_n)$ ne converge manifestement pas vers ℓ : elle ne rentre jamais dans la boule $B(\ell, \epsilon)$. $\square$

Une fonction continue est séquentiellement continue. Dans les espaces métriques la proposition suivante montre que la réciproque est également vraie et la continuité est équivalente à la continuité séquentielle. Cela n'est cependant pas vrai pour n'importe quel espace topologique.

Corolaire 7.160 (Caractérisation séquentielle de la continuité en un point[1]).

Si X et Y sont des espaces métriques, alors une fonction $f: X \rightarrow Y$ est continue en un point si et seulement si elle est séquentiellement continue en ce point.

Démonstration. Paraphrasons la preuve précédente. Nous supposons que X et Y sont métriques. Si f n'est pas continue en a , il existe $\epsilon > 0$ tel que pour tout $\delta > 0$, il existe x tel que $\|x - a\| \leq \delta$ et $\|f(x) - f(a)\| > \epsilon$. Nous considérons un tel ϵ et pour chaque $n \geq 1 \in \mathbb{N}$ nous considérons un x_n correspondant à $\delta = \frac{1}{n}$. Cela nous donne une suite $x_n \rightarrow a$ dans X mais $\|f(x_n) - f(a)\|$ reste plus grand que ϵ . Cela montre que f n'est pas non plus séquentiellement continue. $\square$

Les espaces métriques ont une propriété importante que la **fermeture séquentielle** est équivalente à la fermeture.

Proposition 7.161 (Caractérisation séquentielle d'un fermé).

Soient X un espace métrique et $F \subset X$. L'ensemble F est fermé si et seulement si toute suite contenue dans F et convergeant dans X converge vers un élément de F .

Démonstration. Une suite contenue dans un fermé ne peut converger que vers un élément de ce fermé : c'était la proposition 7.32. Le point le plus important est donc l'autre sens : si toute suite d'éléments de F converge dans F alors F est fermé.

Par contraposée, supposons que $X \setminus F$ ne soit pas ouvert. Alors il existe $x \in X \setminus F$ pour lequel tout voisinage intersecte F . En prenant $x_k \in B(x, \frac{1}{k})$, nous construisons une suite contenue dans F , convergeant vers x qui n'est pas dans F . $\square$

Lemme 7.162.

Soit X un espace métrique, et soit (x_n) une suite convergente contenue dans un ensemble $A \subset X$. Alors la limite x_n appartient à $\bar{A}$.

Ce lemme est précisément la version « espace métrique » du corolaire 7.33 ; mais, donnons-en une preuve tout de même.

Démonstration. Supposons que nous ayons une partie A de X , et une suite (x_n) dont la limite ℓ se trouve hors de $\bar{A}$. Dans ce cas, il existe un $r > 0$ tel que $^{48} B(\ell, r) \cap A = \emptyset$. Si tous les éléments x_n de la suite sont dans A , il n'y en a donc aucun tel que $d(x_n, \ell) < r$. Cela contredit la notion de convergence $x_n \rightarrow \ell$. $\square$

Corolaire 7.163.

Soit X un espace métrique, $A \subset X$ et $a \in \bar{A}$. Alors il existe une suite d'éléments dans A qui converge vers a .

Démonstration. Si $a \in A$, alors nous pouvons prendre la suite constante $x_n = a$. Si a n'est pas dans A , alors a est dans ∂A , et pour tout n , il existe un point de A dans la boule $B(a, \frac{1}{n})$. Si nous nommons x_n ce point, la suite ainsi construite est une suite contenue dans A et qui converge vers a (ce dernier point est laissé à la sagacité du lecteur.). $\square$

En termes savants, ce corolaire signifie que la fermeture $\bar{A}$ est composé de A plus de toutes les limites de toutes les suites contenues dans A .

Proposition 7.164 (Caractérisation séquentielle de la continuité^[1]).

Soient X et Y deux espaces métriques. Une application $f: X \rightarrow Y$ est continue sur X si et seulement si elle est séquentiellement continue sur X .

Démonstration. Le sens direct est déjà prouvé dans la proposition 7.84. Nous nous concentrons donc sur la réciproque.

Soit $\mathcal{O}$ un ouvert de Y ; nous allons voir que le complémentaire de $f^{-1}(\mathcal{O})$ est fermé dans E . Pour cela nous considérons une suite convergente $x_k \xrightarrow{E} x$ avec $x_k \in \mathbb{C}f^{-1}(\mathcal{O})$ pour tout k . Nous allons montrer que $x \in \mathbb{C}f^{-1}(\mathcal{O})$ et la caractérisation séquentielle⁴⁹ de la fermeture conclura que $\mathbb{C}f^{-1}(\mathcal{O})$ est fermé.

Pour tout k , nous avons $f(x_k) \in \mathbb{C}\mathcal{O}$, mais $\mathcal{O}$ est ouvert et $f(x_k) \xrightarrow{Y} f(x)$ parce que f est séquentiellement continue. Par conséquent $f(x) \in \mathbb{C}\mathcal{O}$ et $x \in \mathbb{C}f^{-1}(\mathcal{O})$. $\square$

Proposition 7.165.

Si X et Y sont deux espaces métriques et $f, g: X \rightarrow Y$ sont deux fonctions continues égales sur une partie dense de X alors $f = g$.

48. Une autre manière de dire la même chose : si $\ell \notin \bar{A}$, alors $d(\ell, A) > 0$.

49. Proposition 7.161.

Démonstration. Les fonctions f et g sont séquentiellement continues (proposition 7.85, ou proposition 7.160). Soient A un ensemble dense dans X sur lequel f et g sont égales, et $x \notin A$. Vu que A est dense, il existe une suite a_n dans A telle que $a_n \rightarrow x$. La séquentielle continuité de f et g donnent

$$f(a_n) \rightarrow f(x) \quad (7.144a)$$

$$g(a_n) \rightarrow g(x), \quad (7.144b)$$

mais pour tout n , $f(a_n) = g(a_n)$. Par unicité de la limite⁵⁰ dans Y , $f(x) = g(x)$. $\square$

7.9.2 Espace métrisable

Définition 7.166 (Espace vectoriel topologique métrisable[169]).

Un espace topologique est **métrisable** si il existe une distance compatible avec la topologie.

Proposition 7.167 ([170]).

Soit un espace topologique métrisable X .

- (1) Tout fermé de X est une intersection dénombrable d'ouverts.
- (2) Tout ouvert de X est une union dénombrable de fermés.

Démonstration. Soit une métrique d compatible avec la topologie de X et un fermé A . Nous posons

$$V_n = \{x \in X \text{ tel que } d(x, A) < \frac{1}{n}\}. \quad (7.145)$$

Et juste pour faire simple nous notons $V_0 = X$.

Les parties V_n sont ouvertes Soit $x \in V_n$. Trouvons un voisinage de x contenu dans V_n afin de pouvoir encore invoquer le théorème 7.7. D'abord, vu que $x \in V_n$, il existe $a \in A$ tel que $d(x, a) < \frac{1}{n}$ (ici les inégalités strictes sont importantes).

Soient $\epsilon > 0$ que nous fixerons plus bas, et $y \in B(x, \epsilon)$. L'inégalité triangulaire donne

$$d(y, a) \leq d(y, x) + d(x, a) < \epsilon + \frac{1}{n}. \quad (7.146)$$

Nous pouvons donc choisir ϵ de telle sorte que $d(y, a) < 1/n$. Avec ce ϵ , nous avons, pour tout $y \in B(x, \epsilon)$:

$$d(y, A) \leq d(y, a) < \frac{1}{n} \quad (7.147)$$

et donc $y \in V_n$.

A est l'intersection des V_n Nous avons évidemment $A \subset V_n$ pour tout n . Et d'autre part, si $a \in \bigcap_{n \in \mathbb{N}} V_n$ alors $d(a, A) < \frac{1}{n}$ pour tout n . Cela implique $d(a, A) = 0$, et donc $a \in A$ par le lemme 7.113.

Ceci démontre le point (1).

En ce qui concerne la seconde partie, nous appliquons la première partie au complémentaire. Si $\mathcal{O}$ est ouvert, $\mathcal{O}^c$ est fermé et

$$\mathcal{O}^c = \bigcap_{n \in \mathbb{N}} V_n, \quad (7.148)$$

ce qui donne immédiatement

$$\mathcal{O} = \bigcup_{n \in \mathbb{N}} V_n^c \quad (7.149)$$

où les V_n^c sont fermés. $\square$

Corolaire 7.168.

Si X est un espace topologique métrisable, alors X accepte une base dénombrable de topologie autour de chaque point.

50. Proposition 7.73.

Démonstration. Il s'agit seulement de remarquer que les singletons sont fermés et d'appliquer la proposition 7.167. $\square$

7.10 Suites de Cauchy, métrique et espaces complets

7.10.1 Généralités

Définition 7.169 (Suite de τ -Cauchy, espace vectoriel topologique[171, 172]).

Soit E un espace vectoriel topologique. Une suite (x_k) dans E est une **suite τ -Cauchy** si pour tout voisinage $\mathcal{U}$ de 0 il existe $N \in \mathbb{N}$ tel que $x_k - x_l \in \mathcal{U}$ pour tout $k, l \geq N$.

Définition 7.170 (Espace τ -complet).

Nous disons qu'une partie A d'un espace vectoriel topologique est **τ -complet** si toute suite τ -Cauchy d'éléments de A converge⁵¹ vers un élément de A .

Définition 7.171 (Suite de Cauchy, espace métrique).

Une suite (a_k) dans un espace métrique (V, d) est **de Cauchy** si pour tout $\epsilon \in \mathbb{R}$, il existe N tel que si $n, m \geq N$ alors $d(a_n, a_m) < \epsilon$.

Notons qu'ici, même si l'espace V n'a rien à voir avec $\mathbb{R}$, nous prenons ϵ dans $\mathbb{R}$ et la distance à valeurs dans $\mathbb{R}$. Cela semble une évidence, mais il faut se rendre compte que $\mathbb{R}$ commence à prendre une place centrale dans nos constructions. Ce n'était pas le cas du temps où nous parlions de suites de Cauchy et de complétude dans des corps totalement ordonnés (définitions 1.253). Dans ce contexte, le ϵ était pris dans le corps lui-même.

Définition 7.172 (Métrique complète).

Soit (E, d) un espace métrique. Nous disons que la métrique d est **complète** si toute suite de Cauchy dans (E, d) converge dans E .

7.173.

Ces définitions méritent quelques remarques.

- (1) Dans le cas des espaces vectoriels topologiques, nous définissons les notions de suite τ -Cauchy et d'espace topologique τ -complet. Nous ajoutons le préfixe τ pour indiquer que ce sont des notions topologiques.
- (2) Dans le cas des espaces métriques, nous définissons la notion de *métrique* complète. C'est bien la métrique qui est complète, et non l'espace. En effet nous allons voir dans l'exemple 7.175 que le même espace topologique peut accepter plusieurs distances différentes (donnant la même topologie) donnant lieu à des suites de Cauchy différentes.
- (3) Si un espace vectoriel a une topologie issue d'une distance, rien ne dit que ses suites τ -Cauchy et ses suites de Cauchy sont les mêmes. Ce sont deux notions a priori séparées. Si V est un espace vectoriel topologique que l'on peut munir de deux distances d_1, d_2 donnant toutes deux la topologie, dire que V est τ -complet, dire que d_1 est complète et dire que d_2 est complète sont trois choses différentes. Même si les trois topologies sont identiques.
- (4) Nous allons bien entendu voir que dans de larges gammes d'exemples, les notions de suite de Cauchy et τ -Cauchy coïncident.

Définition 7.174 (espace de Banach, algèbre de Banach[173]).

Un **espace de Banach** est un espace vectoriel normé complet⁵² pour la topologie de la norme.

Une **algèbre de Banach** est une algèbre commutative et associative qui est un espace vectoriel normé complet.

⁵¹. Définition 7.13.

⁵². Définition 7.172.

Exemple 7.175 (La complétude n'est pas une propriété topologique[174]).

Le fait pour un espace d'être complet n'est pas une propriété topologique, mais une propriété métrique. Plus exactement, il existe des espaces topologiques isomorphes, mais dont l'un est complet et l'autre non.

Nous considérons la distance suivante sur $\mathbb{N}$:

$$d_1(x, y) = \left| \frac{1}{x} - \frac{1}{y} \right|. \quad (7.150)$$

Pour vérifier que cette formule définit bien une distance (définition 7.98), le seul point non immédiat est l'inégalité triangulaire :

$$d_1(x, y) = \left| \frac{1}{x} - \frac{1}{y} \right| \leq \left| \frac{1}{x} - \frac{1}{z} \right| + \left| \frac{1}{z} - \frac{1}{y} \right| = d_1(x, z) + d_1(z, y). \quad (7.151)$$

Au niveau de la topologie induite par cette distance, c'est la topologie discrète. En effet, soit $x \in \mathbb{N}$ et $\epsilon > 0$; nous voulons déterminer la boule $B(x, \epsilon)$ en résolvant l'équation

$$\left| \frac{1}{x} - \frac{1}{y} \right| < \epsilon \quad (7.152)$$

pour $y \in \mathbb{N}$. Nous trouvons que $\frac{1}{y} > \frac{1}{x} - \epsilon$ et $\frac{1}{y} < \frac{1}{x} + \epsilon$, soit

$$\left\{ \begin{array}{l} y > \frac{1}{\frac{1}{x} - \epsilon} \\ y < \frac{1}{\frac{1}{x} + \epsilon} \end{array} \right. \quad (7.153a)$$

$$\left\{ \begin{array}{l} y > \frac{1}{\frac{1}{x} - \epsilon} \\ y < \frac{1}{\frac{1}{x} + \epsilon} \end{array} \right. \quad (7.153b)$$

Si ϵ est assez petit, la seule solution entière est $y = x$. Les ouverts sont donc toutes les parties parce que tous les singletons sont ouverts.

L'espace topologique associé à $(\mathbb{N}, d_1)$ est donc la topologie discrète⁵³.

Si nous considérons par contre la distance usuelle sur $\mathbb{N}$, à savoir $d(x, y) = |x - y|$, nous obtenons encore la topologie discrète. Nous avons donc un isomorphisme d'espaces topologiques

$$(\mathbb{N}, d) \simeq (\mathbb{N}, d_1). \quad (7.154)$$

Nous pouvons même donner un isomorphisme explicite : $f(n) = n$.

La suite $(x_n) = n$ est une suite de Cauchy dans $(\mathbb{N}, d_1)$ parce que si $\epsilon > 0$ est donné, il suffit de prendre N assez grand pour avoir $\frac{1}{N} < \epsilon$ (possible par le lemme 1.307) nous avons, pour $n, m > N$:

$$\left| \frac{1}{n} - \frac{1}{m} \right| < \frac{1}{n} < \frac{1}{N} < \epsilon. \quad (7.155)$$

Or cette suite ne converge pas. Soit en effet un candidat limite k . Calculons

$$d_1(x_n, k) = \left| \frac{1}{n} - \frac{1}{k} \right| \rightarrow \frac{1}{k} \neq 0. \quad (7.156)$$

L'espace $(\mathbb{N}, d_1)$ n'est pas complet.

Notons que cette suite n'est pas de Cauchy dans $(\mathbb{N}, d)$.

En résumé :

- (1) Les espaces topologiques $(\mathbb{N}, d)$ et $(\mathbb{N}, d_1)$ sont isomorphes.
- (2) Ils ont les mêmes notions de suites convergentes : une suite convergente pour l'un est convergente pour l'autre.
- (3) Ils n'ont pas les mêmes notions de suites de Cauchy.
- (4) Dans $(\mathbb{N}, d_1)$, il existe des suites de Cauchy qui ne convergent pas (pas complet).
- (5) L'espace $(\mathbb{N}, d)$ est complet, mais $(\mathbb{N}, d_1)$ n'est pas complet.
- (6) Le fait pour un espace topologique métrique d'être complet n'est pas intrinsèque à sa topologie : la complétude est une propriété de la distance. La complétude est une propriété de la métrique, et non de la topologie qui s'en suit.

△

53. Celle dont toutes les parties sont des ouverts.

7.10.2 Espace topologique métrique

Dans les espaces vectoriels topologiques métriques, il n'y a pas d'ambiguïté.

Proposition 7.176 (Caractérisations avec la distance d).

Soit (E, d) un espace vectoriel topologique métrique.

- (1) Une suite (x_n) dans E est convergente⁵⁴ vers x si et seulement si pour tout $\epsilon \in \mathbb{R}$ il existe N_ϵ tel que pour tout $n \geq N_\epsilon$ nous avons $d(x_n, x) \leq \epsilon$.
- (2) Une suite (x_n) dans E est de Cauchy⁵⁵ si pour tout $\epsilon \in \mathbb{R}$, il existe un N_ϵ tel que si $p, q \geq N_\epsilon$, nous avons $d(x_p, x_q) \leq \epsilon$.

Démonstration. En ce qui concerne la convergence :

Sens direct Nous supposons que $x_k \rightarrow x$ dans E . Soit $\epsilon > 0$; vu que $B(x, \epsilon)$ est un ouvert contenant x , il existe un $N_\epsilon > 0$ tel que $k > N_\epsilon$ implique $x_k \in B(x, \epsilon)$. Cela signifie $d(x, x_k) \leq \epsilon$.

Réciproque Nous supposons que pour tout $\epsilon > 0$, il existe $N_\epsilon > 0$ tel que si $k > N_\epsilon$ alors $x_k \in B(x, \epsilon)$. Soit un ouvert $\mathcal{O}$ autour de x . Nous sommes dans un espace métrique; ergo la topologie est donné par le théorème 7.99 et en particulier la liste des ouverts est donnée par (7.88). Il existe donc une boule $B(x, \epsilon)$ incluse à $\mathcal{O}$. Pour tout $k > N_\epsilon$ nous avons alors $x_k \in B(x, \epsilon) \subset \mathcal{O}$.

En ce qui concerne les suites de Cauchy :

Sens direct Si (x_n) est une suite de Cauchy et si $\epsilon > 0$ est donné, alors $B(0, \epsilon)$ est un voisinage de 0 et il existe N_ϵ tel que si $p, q \geq N_\epsilon$ alors $x_p - x_q \in B(0, \epsilon)$. Posons $u = x_p - x_q$; en utilisant l'invariance par translation (lemme 7.122(1)) nous avons

$$d(u, 0) = d(x_p - x_q, 0) = d(x_p, x_q). \quad (7.157)$$

Par conséquent $d(x_p, x_q) \leq \epsilon$.

Réciproque Soit $\mathcal{O}$ un voisinage de 0. Il existe ϵ tel que $B(0, \epsilon) \subset \mathcal{O}$. Par hypothèse il existe N_ϵ tel que $d(x_p, x_q) \leq \epsilon$ dès que $p, q \geq N_\epsilon$. En utilisant encore l'invariance par translation nous avons

$$d(x_p, x_q) = d(x_p - x_q, 0), \quad (7.158)$$

et comme cela est plus petit que ϵ , nous avons $x_p - x_q \in B(0, \epsilon) \subset \mathcal{O}$.

□

Proposition 7.177 ([175]).

Toute suite convergente dans un espace métrique est de Cauchy.

Démonstration. Nous utilisons les caractérisations de la proposition 7.176 des suites convergentes et de Cauchy.

Soit un espace métrique (X, d) et $x_n \rightarrow \ell$ une suite convergente. Si $\epsilon > 0$, la proposition 7.176(1), dit qu'il existe N tel que pour tout $n > N$ nous ayons $d(x_n, \ell) < \epsilon$. Par conséquent si $n, m > N$ alors

$$d(x_n, x_m) \leq d(x_n, \ell) + d(\ell, x_m) \leq 2\epsilon. \quad (7.159)$$

Cela prouve que (x_n) est une suite de Cauchy.

□

54. Définition 7.13.

55. Définition 7.169.

7.11 Espaces vectoriels topologiques

Définition 7.178.

Un espace vectoriel V sur le corps $\mathbb{K}$ muni d'une topologie est un **espace vectoriel topologique** si

- (1) la somme de deux vecteurs est une application continue $V \times V \rightarrow V$; et
- (2) la multiplication par un scalaire est une application continue $\mathbb{K} \times V \rightarrow V$.

Ici, sur $V \times V$ et sur $\mathbb{K} \times V$ nous avons la topologie produit.

Dans toute la suite, nous supposons que $\mathbb{K}$ est un corps avec une topologie métrique.

On le redit quand même : le corps⁵⁶ lui-même doit avoir sa topologie. Dans la grande majorité des cas, ce corps est $\mathbb{R}$ ou $\mathbb{C}$ muni de la topologie usuelle.

Mine de rien, le fait que les deux opérations usuelles soient continues a de belles conséquences sur la topologie de l'espace...

Proposition 7.179 ([172]).

Pour $x \in V$ et $\lambda \in \mathbb{K}$, $\lambda \neq 0$ fixés, les fonctions T_x et M_λ définies par :

$$T_x : V \rightarrow V \quad \text{et} \quad M_\lambda : V \rightarrow V \quad (7.160)$$

$$y \mapsto x + y \quad y \mapsto \lambda y \quad (7.161)$$

sont des homéomorphismes de V dans V .

Démonstration. Ce sont des bijections continues, dont les inverses sont respectivement T_{-x} et $M_{1/\lambda}$. $\square$

Corolaire 7.180 (Invariance de la topologie [172]).

Toute base de voisinage de 0 se transporte en tout point de l'espace vectoriel topologique.

Plus précisément, si $\{A_i\}_{i \in I}$ est une base de voisinage de 0, alors $\{A_i + a\}_{i \in I}$ est une base de voisinage de a .

Définition 7.181 (Partie symétrique[172]).

Une partie U d'un espace vectoriel topologique est **symétrique** si $x \in U$ implique $-x \in U$.

Définition 7.182 (Partie équilibrée[172]).

Une partie E d'un espace vectoriel topologique V est **équilibrée** si pour tout $|\alpha| < 1$ dans $\mathbb{K}$, $\alpha E \subset E$.

Lemme 7.183 ([172, 1]).

Soit un espace vectoriel topologique.

- (1) Soit un ouvert A autour de 0 dans l'espace vectoriel topologique V . Il existe $\delta > 0$ dans le corps $\mathbb{K}$ et un voisinage ouvert W de 0 tel que $\lambda W \subset A$ pour tout $|\lambda| < \delta$.
- (2) Tout voisinage de 0 contient un ouvert équilibré.
- (3) Tout voisinage de 0 contient un ouvert équilibré et symétrique.

Démonstration. En plusieurs parties.

Pour (1) Nous savons que $0 \cdot 0 = 0$ et que l'application

$$f : \mathbb{K} \times V \rightarrow V$$

$$\lambda, x \mapsto \lambda x \quad (7.162)$$

est continue. La partie $f^{-1}(A)$ contient $(0, 0)$. Il existe donc un voisinage ouvert S de 0 dans $\mathbb{K}$ et un voisinage ouvert W de 0 dans V tel que $S \times W \subset f^{-1}(A)$.

56. Définition 1.190

Vu que $\mathbb{K}$ est un corps dont la topologie est métrique⁵⁷, il existe une boule $S' = B(0, \delta) \subset S$. Nous avons $f(S' \times W) \subset A$. Donc pour tout $|\lambda| < \delta$ nous avons $\lambda W \subset A$.

Pour (2) Soit un voisinage ouvert $\mathcal{O}$ de 0 dans V . Par le point (1), nous considérons un voisinage W de 0 et un $\delta > 0$ tel que $\lambda W \subset \mathcal{O}$ pour tout $|\lambda| < \delta$.

Nous posons

$$U = \{\lambda w \mid \text{tel que } |\lambda| < \delta, w \in W\}. \quad (7.163)$$

Nous avons $U \subset A$ par définition de W . De plus U est équilibré parce que si $|\mu| < 1$, et si $x \in U$, il existe $|\lambda| < \delta$ et $w \in W$ tels que $x = \lambda w$. Alors $\mu x = \mu \lambda w$. Nous avons $|\mu \lambda| < \delta$ et donc $\mu \lambda w \in U$.

Pour (3) Nous considérons U équilibré comme dans (2). Ensuite nous posons $U' = U \cap (-U)$. La partie U' est symétrique, elle est ouverte (intersection d'ouverts). Et elle est équilibrée parce que si $x \in U'$ et $|\lambda| < 1$ alors :

- $x \in U$ et U est équilibré, donc $\lambda x \in U$.
- $x \in -U$ et U est équilibré, donc il existe $y \in U$ tel que $x = -y$. Pour ce y nous avons $\lambda y \in U$ et donc $\lambda x = -\lambda y \in -U$. Donc $\lambda x \in -U$.
- Au final, $\lambda x \in U \cap (-U) = U'$ et U' est équilibré.

□

Lemme 7.184 ([176]).

Soit un espace vectoriel topologique V ainsi qu'un voisinage ouvert $\mathcal{O}$ de 0 dans V . Il existe des voisinages ouverts U_1 et U_2 de 0 dans V tels que

$$U_1 + U_2 \subset \mathcal{O}. \quad (7.164)$$

Démonstration. Par définition d'un espace vectoriel topologique, l'application

$$\begin{aligned} f: V \times V &\rightarrow V \\ x, y &\mapsto x + y \end{aligned} \quad (7.165)$$

est continue. Donc la partie $f^{-1}(\mathcal{O})$ est un ouvert de $V \times V$ (c'est la définition 7.75(2) de la continuité). La définition 7.15 de la topologie produit, appliquée au point $(0, 0) \in V \times V$ implique qu'il existe des voisinages U_1 et U_2 de 0 dans V tels que

$$U_1 \times U_2 \subset f^{-1}(\mathcal{O}). \quad (7.166)$$

Donc $f(U_1 \times U_2) \subset \mathcal{O}$ et en particulier $U_1 + U_2 \subset \mathcal{O}$. □

Proposition 7.185 ([172, 1]).

Soit V un espace vectoriel topologique, et $\mathcal{O}$ un voisinage ouvert de 0. Il existe un voisinage ouvert U de 0 tel que

- (1) U est symétrique,
- (2) U est équilibré
- (3) U vérifie $U + U \subset \mathcal{O}$.
- (4) U vérifie $U + U + U + U \subset \mathcal{O}$.

Démonstration. En plusieurs petits pas.

Le point de départ Le lemme 7.184 donne des voisinages ouverts U_1 et U_2 de 0 dans V tels que $U_1 + U_2 \subset \mathcal{O}$.

Symétrique En posant $U' = U_1 \cap U_2 \cap (-U_1) \cap (-U_2)$, on a un sous-ensemble symétrique de U_1 et U_2 qui vérifie $U' + U' \subset W$. De plus U' est encore un voisinage ouvert de 0 dans V .

57. Pour rappel, nous supposons toujours ça.

équilibré C'est le moment d'utiliser le lemme 7.183. La partie U' contient un voisinage ouvert U'' de 0 qui est symétrique et équilibré. Ce U'' vérifie encore $U'' + U'' \subset \mathcal{O}$.

En 4 parties Maintenant nous posons ré-appliquons tout ce que nous venons de faire à U'' pour obtenir un voisinage symétrique et équilibré de 0 tel que $U + U \subset U'$. Nous avons alors $U + U + U + U \subset \mathcal{O}$.

Notons que ce U vérifie à fortiori $U + U \subset \mathcal{O}$.

□

Proposition 7.186 (Séparation [172, 177]).

Soit V , un espace vectoriel topologique. Soient des parties K et F de V telles que :

- (1) K est compact,
- (2) F est fermé,
- (3) $K \cap F = \emptyset$.

Alors il existe un voisinage U de 0 tel que

$$(K + U) \cap (F + U) = \emptyset. \quad (7.167)$$

Autrement dit, la topologie d'un espace vectoriel topologique sépare les fermés des compacts.

Démonstration. Soit un élément $x \in K$. La partie F^c est un ouvert qui contient x ; donc $F^c - x$ est un voisinage ouvert de 0.

Quelque chose sans intersection avec F La proposition 7.185, il existe un ouvert symétrique U_x autour de 0 tel que

$$U_x + U_x + U_x + U_x \subset F^c + x. \quad (7.168)$$

En enlevant un des éléments de la somme, nous gardons la même inclusion :

$$U_x + U_x + U_x \subset F^c + x. \quad (7.169)$$

Et en passant le x de l'autre côté :

$$x + U_x + U_x + U_x \subset F^c. \quad (7.170)$$

Cela pour dire que nous avons, pour chaque $x \in K$ un voisinage ouvert U_x de 0 tel que

$$(x + U_x + U_x + U_x) \cap F = \emptyset. \quad (7.171)$$

$(x + U_x + U_x) \cap (U_x + F) = \emptyset$ Supposons $z \in (x + U_x + U_x) \cap (U_x + F)$, et déduisons une contradiction. En particulier $z \in U_x + F$ et donc il existe $u \in U_x$, $f \in F$ tel que $z = u + f$. Nous avons alors (nous utilisons le fait que U_x soit symétrique)

$$f = z - u \in z + U_x \quad (7.172)$$

Mais z est aussi dans $x + U_x + U_x$. Donc

$$f \in z + U_x \subset x + U_x + U_x + U_x. \quad (7.173)$$

Cela prouve que $x + U_x + U_x + U_x \cap F \neq \emptyset$, en contradiction avec (7.171). Nous en concluons que

$$(x + U_x + U_x) \cap (U_x + F) = \emptyset. \quad (7.174)$$

Un sous-recouvrement fini Fini de rigoler. Si nous avons un compact dans les hypothèses, il fallait que ça arrive. Pour chaque $x \in K$ nous avons un voisinage ouvert U_x de 0 et donc un voisinage ouvert $x + U_x$ de x . Du coup $\{U_x + x\}_{x \in K}$ forme un recouvrement de K par des

ouverts. Et hop, sous-recouvrement fini (c'est la définition 7.50 d'un compact) : nous avons $\{x_i\}_{i=1,\dots,n}$ tels que

$$K \subset \bigcup_{i=1}^n (x_i + U_{x_i}). \quad (7.175)$$

Nous posons $U = \bigcap_{i=1}^n U_{x_i}$. Même si c'est évident, remarquez que U est un ouvert autour de 0 et que U est plus petit que chacun des U_{x_i} . Récrivons (7.174) pour chacun des x_i :

$$(x + U_{x_i} + U_{x_i}) \cap (F + U_{x_i}) = \emptyset. \quad (7.176)$$

Lorsqu'on enlève des éléments dans une intersection vide, l'intersection reste vide. Donc en remplaçant des U_{x_i} par des U dans (7.176), nous conservons une intersection vide :

$$(x + U_{x_i} + U) \cap (F + U) = \emptyset. \quad (7.177)$$

Conclusion Aucun ensemble de la forme $x + U_{x_i} + U$ n'intersecte $F + U$. L'union ne l'intersecte pas non plus :

$$\bigcup_{i=1}^n (x + U_{x_i} + U) \cap (F + U) = \emptyset. \quad (7.178)$$

Et donc

$$(K + U) \cap (F + U) = \emptyset, \quad (7.179)$$

comme nous le voulions.

□

Définition 7.187.

Une distance d sur un espace vectoriel topologique V est dite **compatible** avec la topologie si la topologie induite⁵⁸ de d est celle de V .

Définition 7.188.

Une distance d sur un espace vectoriel V est dite **invariante** si pour tout $x, y, a \in V$ nous avons

$$d(x + a, y + a) = d(x, y). \quad (7.180)$$

Notons que lorsque nous parlons d'une distance compatible avec un espace vectoriel topologique, nous parlons de compatibilité avec la topologie, pas avec la structure vectorielle.

Lemme 7.189 ([1]).

Soit un espace vectoriel muni d'une distance invariante. Alors

$$B(a, r) + x = B(a + x, r). \quad (7.181)$$

Démonstration. Un élément de $B(a, r) + x$ est de la forme $y + x$ avec $d(a, y) < r$. Nous avons alors $d(y + x, a + x) = d(y, a) < r$, de telle sorte que $y + x \in B(a + x, r)$.

Dans le sens inverse, si $y \in V$ vérifie $d(a + x, y) < r$, alors je prétend que $y - x \in B(a, r)$. En effet $d(y - x, a) = d(y - x + x, a + x) = d(y, a + x) < r$. □

<+ +>

Une version plus complète du lemme suivant sera dans la proposition 11.136 et ce qui suit.

Lemme 7.190.

Nous introduisons l'ensemble $\mathbb{D}_2$ des suites finies dans $\{0, 1\}$ ⁵⁹.

58. Définition 7.99.

59. C'est en gros ce qui se fera dans 11.134 pour les développements de nombres dans une base donnée, sauf qu'ici nous n'avons pas besoin de subtilités sur les queues de suites.

L'application

$$\begin{aligned}\varphi: \mathbb{D}_2 &\rightarrow [0, 1[\\ x &\mapsto \sum_{i=1}^{l(x)} \frac{x_i}{2^i}.\end{aligned}\tag{7.182}$$

où $l(x)$ est la longueur de la suite finie x est injective.

Démonstration. Le lemme 1.345 donne la somme partielle de la série géométrique. Dans notre cas, $q = 1/2$. Si $x \in D_n$, alors en majorant chacun des c_i par 1,

$$x \leq \sum_{i=1}^n \left(\frac{1}{2}\right)^i = \frac{1 - (1/2)^{n+1}}{1/2} - 1 = 1 - (1/2)^{n+1} < 1.\tag{7.183}$$

Donc c'est bon pour dire que φ prend ses valeurs dans $[0, 1[$.

Il reste à voir l'injectivité. Nous supposons que $\varphi(x) = \varphi(y)$. Quitte à allonger x ou y par des zéros, nous supposons qu'elles ont même longueur N . Enfin nous définissons n_0 le plus petit indice pour lequel $x_i \neq y_i$. Nous avons :

$$0 = \frac{1}{2^{n_0}} + \sum_{i=n_0+1}^N \frac{x_i - y_i}{2^i}.\tag{7.184}$$

Le deuxième terme est majoré de la façon suivante :

$$\left| \sum_{i=n_0+1}^N \frac{x_i - y_i}{2^i} \right| \leq \sum_{i=n_0+1}^N \frac{|x_i - y_i|}{2^i}\tag{7.185a}$$

$$\leq \sum_{i=n_0+1}^N \frac{1}{2^i}\tag{7.185b}$$

$$= \sum_{i=1}^N \left(\frac{1}{2}\right)^i - \sum_{i=1}^{n_0} \left(\frac{1}{2}\right)^i\tag{7.185c}$$

$$= \frac{1 - (1/2)^{N+1}}{1/2} - \frac{1 - (1/2)^{n_0+1}}{1/2}\tag{7.185d}$$

$$= \frac{1}{2^{n_0}} - \frac{1}{2^N}\tag{7.185e}$$

$$< \frac{1}{2^{n_0}}.\tag{7.185f}$$

L'égalité (7.184) n'est donc pas possible. Nous déduisons que n_0 n'existe en fait pas et que $x = y$. D'où l'injectivité de φ . $\square$

Toujours avec l'application φ du lemme 7.190 nous avons ceci.

Lemme 7.191.

Soient $r, s \in \varphi(\mathbb{D}_2)$ tels que $r + s < 1$. Alors $r + s \in \varphi(\mathbb{D}_2)$.

Lemme 7.192.

Soient $r, s \in \varphi(\mathbb{D}_2)$ tels que $r + s < 1$. Nous posons $u = \varphi^{-1}(r)$, $v = \varphi^{-1}(s)$ et $w = \varphi^{-1}(r + s)$. Si k est le plus petit entier tel que $w_k \neq u_k + v_k$, alors $u_k = v_k = 0$ et $w_k = 1$.

Théorème 7.193 (Espace topologique métrisable[172, 1]).

Si V est un espace vectoriel topologique. Nous supposons :

(1) Tout point admet une base dénombrable de topologie⁶⁰.

60. Définition 7.2.

(2) Le singleton $\{0\}$ est fermé⁶¹.

Alors il existe une distance d sur V telle que

- (1) d est compatible avec la topologie de V ,
- (2) d est invariante par translation.

Démonstration. Vu que V admet une base dénombrable de topologie, nous en considérons une autour de 0 dans $V : \{A_i\}_{i \in \mathbb{N}}$.

Nouvelle base de topologie Nous construisons une nouvelle base de topologie $\{U_i\}_{i \in \mathbb{N}}$ autour de 0 de la façon suivante. La proposition 7.185 donne un ouvert symétrique équilibré dans A_0 . Nous le nommons U_0 :

$$U_0 \subset A_0. \quad (7.186)$$

Pour les suivants, U_{k+1} est un ouvert symétrique équilibré dans $U_k \cap A_k$ vérifiant

$$U_{k+1} + U_{k+1} + U_{k+1} + U_{k+1} \subset A_k \cap U_k. \quad (7.187)$$

Le fait est que $A_k \cap U_k$ est un ouvert autour de 0 ; donc la proposition 7.185 permet de construire un ouvert symétrique et équilibré U_{k+1} autour de 0 ayant la propriété demandée.

C'est bien une base Notons d'abord que $U_k \subset A_k$. Si $\mathcal{O}$ est un ouvert autour de 0, il existe k tel que $A_k \subset \mathcal{O}$: c'est la définition 7.2 d'une base de topologie. Nous avons donc $U_k \subset A_k \subset \mathcal{O}$, et les $\{U_k\}$ forment une base dénombrable de la topologie autour de 0.

Quelques inclusions Notons au passage quelques inclusions. Pour tout $n \in \mathbb{N}$ nous avons

$$U_{n+1} + U_{n+1} + U_{n+1} + U_{n+1} \subset U_n. \quad (7.188)$$

À fortiori nous avons

$$U_{n+1} \subset U_n \quad (7.189)$$

et pour tout $n, k \in \mathbb{N}$, nous obtenons alors

$$U_{n+1} + U_{n+2} + \cdots + U_{n+(k-1)} + U_{n+k} \subset U_{n+1} + U_{n+1} \subset U_n. \quad (7.190)$$

L'ensemble D Nous considérons l'ensemble $\mathbb{D}_2$ et l'application φ du lemme 7.190. Nous notons $D = \varphi(\mathbb{D}_2) \subset [0, 1[$. L'application $\varphi : \mathbb{D}_2 \rightarrow D$ est injective, et nous pouvons donc parler de $\varphi^{-1}(r)$ pour tout $r \in D$.

La fonction ϕ Nous définissons maintenant une fonction à valeurs dans la topologie τ_V de V :

$$\begin{aligned} \phi : D \cup [1, +\infty[&\rightarrow \tau_V \\ r &\mapsto \begin{cases} V & \text{si } r \geq 1; \\ \sum_i \varphi^{-1}(r)_i U_i & \text{si } r \in D. \end{cases} \end{aligned} \quad (7.191)$$

La dernière somme est toujours une somme finie et est un ouvert parce que la multiplication par un scalaire et l'addition sont des ouverts.

Notez aussi que plus r est petit, plus ce sont les grands i qui tendront à avoir $\varphi^{-1}(r) \neq 0$. En effet, pour $r = 1/8$, nous avons $\varphi^{-1}(1/8) = (0, 0, 0, 1)$, et plus généralement pour $r < 1/2^N$, les N premiers termes de $\varphi^{-1}(r)$ seront nuls.

Quelques remarques sur cette fonction.

Une égalité facile Si je ne me trompe pas d'un off-by-one, nous avons

$$\phi(1/2^N) = U_N. \quad (7.192)$$

$0 \in \phi(r)$ pour tout r En effet, $\phi(r)$ n'est jamais vide, c'est toujours un voisinage de 0.

61. Attention : dans [172], cela fait partie de la définition d'un espace vectoriel topologique et n'est donc pas listé dans les hypothèses de ce théorème.

$\phi(r) + \phi(s) \subset \phi(r+s)$ Si $r+s \geq 1$, c'est clair. Sinon, nous posons $u = \varphi^{-1}(r)$, $v = \varphi^{-1}(s)$ et $w = \varphi^{-1}(r+s)$. Dans la suite, nous prolongeons u et v pour qu'elles aient le même nombre d'éléments que nous notons N .

Deux cas se produisent : soit $w_i = u_i + v_i$ pour tout i soit non.

Premier cas Si $w_i = u_i + v_i$ pour tout i , alors en particulier les u_i et v_i ne peuvent pas être 1 en même temps et nous pouvons séparer clairement les termes de la somme :

$$\phi(r+s) = \sum_i w_i U_i = \sum_i u_i U_i + \sum_i v_i U_i = \phi(r) + \phi(s); \quad (7.193)$$

Second cas Sinon, posons k le plus petit entier tel que $w_k \neq u_k + v_k$. Alors le lemme 7.192 dit que $u_k = v_k = 0$ et $w_k = 1$. Nous avons d'abord

$$\phi(r) = \sum_{i=1}^{k-1} u_i U_i + \sum_{i=k+1}^n u_i U_i \subset \sum_{i=1}^{k-1} u_i U_i + U_{k+1} + U_{k+1} \quad (7.194)$$

où nous avons utilisé (7.189) pour tous les derniers termes. De même nous avons :

$$\phi(s) = \sum_{i=1}^{k-1} v_i U_i + \sum_{i=k+1}^n v_i U_i \subset \sum_{i=1}^{k-1} v_i U_i + U_{k+1} + U_{k+1}. \quad (7.195)$$

En combinant, et en utilisant (7.188),

$$\phi(r) + \phi(s) = \sum_{i=1}^{k-1} u_i U_i + \sum_{i=1}^{k-1} v_i U_i + \underbrace{U_{k+1} + U_{k+1} + U_{k+1} + U_{k+1}}_{\subset U_k} \quad (7.196a)$$

$$\subset \sum_{i=1}^{k-1} w_i U_i + U_k \quad (7.196b)$$

$$= \sum_{i=1}^k w_i U_i \quad (7.196c)$$

$$\subset \phi(r+s). \quad (7.196d)$$

Pour (7.196c) nous avons utilisé le fait que $w_k = 1$. Au final nous avons bien $\phi(r) + \phi(s) \subset \phi(r+s)$.

ϕ est croissante Dans notre contexte « croissante » signifie que si $r < s$ alors $\phi(r) \subset \phi(s)$. Il suffit d'écrire

$$\phi(r) \subset \phi(r) + \phi(s-r) \subset \phi(s). \quad (7.197)$$

Définition de la distance (enfin !) Nous définissons l'application

$$\begin{aligned} f: V &\rightarrow \mathbb{R} \\ x &\mapsto \inf\{r \text{ tel que } x \in \phi(r)\}, \end{aligned} \quad (7.198)$$

et ensuite ce qui va être notre distance :

$$d(x, y) = f(y - x). \quad (7.199)$$

Notons que cet infimum est un réel, et qu'il n'est pas spécialement dans $\varphi(\mathbb{D}_2)$. Nous devons prouver que ce d est une distance invariante par translation et compatible avec la topologie.

d est invariante par translation Il s'agit seulement d'écrire $d(x+a, y+a)$ et de remarquer que $(y+a) - (x+a) = y-x$.

$d(x, x) = 0$ Oui, car 0 est dans $\phi(r)$, pour tout r , puisque les U_i sont des voisinages de 0.

$d(x, y) = 0$ implique $x = y$ Nous montrons que $f(x) \neq 0$ dès que $x \neq 0$. Rappeliez-vous que nous avons posé l'hypothèse que $\{0\}$ est un fermé dans V . Vu que $\{x\}$ est un compact⁶², la proposition 7.186 nous indique qu'il existe un voisinage A de 0 qui ne contient pas x . Vu que les $\{U_k\}_{k \in \mathbb{N}}$ forment une base de la topologie autour de 0, il existe un n_0 tel que $x \notin U_{n_0}$. Et comme $U_{k+1} \subset U_k$ nous avons

$$x \notin U_k \quad (7.200)$$

pour tout $k \geq n_0$. Nous savons aussi que ϕ est croissante et que $\phi(1/2^N) = U_N$. Donc pour tout $\epsilon < \frac{1}{2^k}$, nous avons

$$\phi(\epsilon) \subset U_k \quad (7.201)$$

et donc $x \notin \phi(\epsilon)$. Donc

$$f(x) \geq \frac{1}{2^k} > 0 \quad (7.202)$$

la dernière inégalité est stricte et c'est important.

En ce qui concerne la distance, si $d(x, y) = 0$, alors $f(y - x) = 0$. Cela signifie que $y - x = 0$ et donc que $x = y$. Ok.

$d(x, y) = d(y, x)$ Oui, car tous les voisinages considérés sont symétriques. Donc $x - y \in \phi(r)$ si et seulement si $y - x \in \phi(r)$.

$d(x, z) \leq d(x, y) + d(y, z)$ Nous supposons que x, y et z sont trois points distincts, de telle sorte que les trois distances soient strictement positives.

Soit $\epsilon > 0$. Par définition des distances comme infimums, et grâce au corolaire 1.311, il existe r et s dans $\varphi(\mathbb{D}_2)$ tels que :

$$d(x, y) < r < d(x, y) + \frac{\epsilon}{2} \quad \text{et} \quad d(y, z) < s < d(y, z) + \frac{\epsilon}{2}. \quad (7.203)$$

En sommant :

$$d(x, y) + d(y, z) < r + s < d(x, y) + d(y, z) + \epsilon. \quad (7.204)$$

Vu que ϕ est croissante, on a $y - x \in \phi(r)$ et $z - y \in \phi(s)$; donc

$$z - x = (y - x) + (z - y) \in \phi(r) + \phi(s) \subset \phi(r + s) \quad (7.205)$$

Ainsi, pour tout $\epsilon > 0$, on a

$$d(x, z) \leq r + s < d(x, y) + d(y, z) + \epsilon. \quad (7.206)$$

Compatibilité avec la topologie Nous devons montrer que les d -ouverts sont les mêmes que les ouverts de la topologie de V . Nous allons utiliser la proposition 7.2.

Les ouverts sont des d -ouverts Soit un ouvert $\mathcal{O}$ contenant $x \in V$. Alors $\mathcal{O} - x$ est un ouvert contenant 0, et il existe un n tel que

$$U_n \subset \mathcal{O} - x. \quad (7.207)$$

Nous avons alors

$$B(0, \frac{1}{2^n}) \subset U_n \subset \mathcal{O} - x. \quad (7.208)$$

Nous utilisant le lemme 7.189 pour additionner x dans toutes les inclusions :

$$B(x, \frac{1}{2^n}) = B(0, \frac{1}{2^n}) + x \subset \mathcal{O}. \quad (7.209)$$

Les boules forment donc une base de la topologie de V . Donc tous les ouverts de V sont des unions de boules et sont donc des d -ouverts.

62. Les singletons sont toujours des compacts dans les espaces topologiques.

Les d -ouverts sont des ouverts Considérons une boule $B(0, r)$. Il existe un n tel que $B(0, 1/2^n) \subset B(0, r)$ et donc tel que

$$U_n \subset B(0, r). \quad (7.210)$$

En procédant par translations et tout ça, on en déduit que les $\{U_n + x\}_{n \in \mathbb{N}, x \in V}$ forment une base de la d -topologie. Donc les d -ouverts sont des ouverts.

□

7.11.1 Équivalence entre Cauchy et τ -Cauchy

Lemme 7.194.

Soit un espace vectoriel topologique⁶³ V et une distance $d: V \times V \rightarrow \mathbb{R}^+$ compatible⁶⁴ avec la topologie de V . Si d est invariante⁶⁵, alors les suites de Cauchy pour d et les suites τ -Cauchy sont les mêmes.

Démonstration. Nous avons deux implications à prouver.

Cauchy pour d implique τ -Cauchy Soit (x_n) , une suite de Cauchy dans V pour d , et un voisinage U de 0. Vu que d est compatible avec la topologie de V , il existe une boule ouverte $B(0, \epsilon)$ incluse à U . Soit $N > 0$ tel que $m, n > N$ implique $d(x_n, x_m) < \epsilon$. Par invariance de la métrique, nous avons aussi

$$d(0, x_m - x_n) < \epsilon, \quad (7.211)$$

c'est-à-dire $x_m - x_n \in B(0, \epsilon) \subset U$. La suite (x_n) est donc τ -Cauchy.

τ -Cauchy implique Cauchy pour d Soit (x_n) , une suite τ -Cauchy dans V et $\epsilon > 0$. Vu que $B(0, \epsilon)$ est un voisinage de 0 dans V , il existe N tel que $m, n > N$ implique $x_n - x_m \in B(0, \epsilon)$. Cela signifie que $d(0, x_n - x_m) < \epsilon$ et toujours par invariance, que $d(x_n, x_m) < \epsilon$.

□

Tout ceci nous mène à donner une large classe d'espaces vectoriels topologiques sur lesquelles les notions de suites de Cauchy pour une distance et τ -Cauchy coïncident.

Théorème-Définition 7.195.

Soit V un espace vectoriel topologique métrisable⁶⁶, alors il admet une métrique d compatible avec la topologie telle que une suite dans V est de Cauchy pour d si et seulement si elle est τ -Cauchy.

Une **suite de Cauchy** dans un espace vectoriel métrique (E, d) est une suite τ -Cauchy ou de Cauchy pour d .

Démonstration. Soit d une métrique sur V satisfaisant au théorème 7.193. Vu qu'elle est invariante par translation, les suites d -Cauchy sont exactement les suites τ -Cauchy par le lemme 7.194. □

Remarque 7.196.

Même si V est métrisable, si on choisit la métrique n'importe comment, on ne peut rien espérer.

7.197.

Sur les espaces vectoriels topologiques métrisables, nous pouvons donc parler de suite de Cauchy sans préciser si nous parlons de τ -Cauchy ou de d -Cauchy, parce que nous sous-entendons avoir choisi une métrique non seulement compatible avec la topologie, mais également invariante par translation.

Il reste cependant à traiter le cas d'un espace vectoriel topologique non métrisable. Dans ce cas, il n'y a pas de métrique, et la question de l'équivalence des définitions ne se pose pas.

63. Définition 7.178.

64. Définition 7.187.

65. Définition 7.188.

66. Voir la proposition 7.193 pour une condition suffisante.

Le théorème suivant donne la complétude de $\mathbb{R}$ et le critère de Cauchy pour les définitions métriques et topologiques usuelles. Lorsqu'on dit que $\mathbb{R}$ est complet, le plus souvent nous parlons de ce théorème, et non de 1.319 qui en est un lemme indispensable mais qui parle de notions différentes, bien que très liées.

Théorème 7.198 (Complétude de $\mathbb{R}$, critère de Cauchy[12]).

Nous avons :

- (1) L'espace métrique $(\mathbb{R}, d)$ est complet (définition 7.172).
- (2) Une suite dans $\mathbb{R}$ est convergente (définition 7.13) si et seulement si elle est de Cauchy (définition 7.195).

Démonstration. Tout ce théorème se base sur le fait que la définition de suite de Cauchy dans $(\mathbb{R}, d)$ et de suite convergente dans $(\mathbb{R}, d)$ coïncident avec les définitions correspondantes dans $\mathbb{R}$ vu comme simple corps ordonné (définitions 1.253).

Donc si (x_n) est de Cauchy dans $(\mathbb{R}, d)$, elle est de Cauchy dans le corps ordonné $(\mathbb{R}, \leq)$. Donc le théorème 1.319 nous dit que (x_n) est convergente dans $(\mathbb{R}, \leq)$. Et donc convergente dans $(\mathbb{R}, d)$.

Toutes les autres affirmations se prouvent de la même manière. $\square$

Si vous n'êtes pas sûr ou si vous ne voulez pas étudier les notations de convergence et de suites de Cauchy dans les corps, vous pouvez simplement recopier la démonstration du théorème 1.319 en remplaçant partout $\mathbb{Q}$ par $\mathbb{R}$, et aussi en remplaçant les $|x - y|$ par $d(x, y)$.

7.199.

Nous pouvons également mettre une structure d'espace métrique sur $\mathbb{C}$ en posant

$$d(z, z') = |z - z'|. \quad (7.212)$$

Proposition 7.200.

L'espace métrique $(\mathbb{C}, d)$ est complet.

Démonstration. Commençons par nous rendre compte que pour tout $z \in \mathbb{C}$ nous avons $|\operatorname{Re}(z)| \leq |z|$. C'est bon ? Vous vous en êtes rendu compte ? Ok. Continuons.

Soit une suite de Cauchy (z_k) dans $\mathbb{C}$ et $\epsilon > 0$. Si $x_k = \operatorname{Re}(z_k)$, nous avons

$$|x_k - x_l| = |\operatorname{Re}(z_k - z_l)| \leq |z_k - z_l|. \quad (7.213)$$

Vu que (z_k) est de Cauchy, il existe un N tel que si $k, l \geq N$,

$$|x_k - x_l| \leq |z_k - z_l| \leq \epsilon. \quad (7.214)$$

Donc la suite des parties réelles converge par la complétude de $(\mathbb{R}, d)$ du théorème 7.198. Notez que le d ici n'est pas tout à fait le même, et que la démonstration fonctionne parce que la distance prise sur $\mathbb{R}$ est la restriction à $\mathbb{R}$ de la distance prise sur $\mathbb{C}$. Notons x la limite de (x_k) .

De la même manière la suite des parties imaginaires $y_k = \operatorname{Im}(z_k)$ converge vers un réel que nous notons y . Avec tout cela, la suite z_k converge dans $\mathbb{C}$ vers $x + iy$. En effet pour ϵ donné et pour un k suffisamment grand,

$$|z_k - (x + iy)| = |\operatorname{Re}(z_k) - x + i(\operatorname{Im}(z_k) - y)| \leq |x_k - x| + |y_k - y| \leq \epsilon. \quad (7.215)$$

$\square$

7.12 Norme, espace vectoriel normé

La valeur absolue est essentielle pour introduire les notions de limite et de continuité pour les fonctions d'une variable. Par exemple nous verrons dans la proposition 10.71 que la fonction $f: \mathbb{R} \rightarrow \mathbb{R}$ est continue en a si et seulement si pour tout $\epsilon > 0$, il existe un $\delta > 0$ tel que

$$|x - a| \leq \delta \Rightarrow |f(x) - f(a)| \leq \epsilon. \quad (7.216)$$

La quantité $|x - a|$ donne la « distance » entre x et a ; la définition de la continuité signifie que pour tout ε , il existe un δ tel que si a et x sont au plus à la distance δ l'un de l'autre, alors $f(x)$ et $f(a)$ ne seront éloignés au plus d'une distance ε .

La valeur absolue, dans $\mathbb{R}$, nous sert donc à mesurer des distances entre les nombres. Les principales propriétés de la valeur absolue sont :

- (1) $|x| = 0$ implique $x = 0$,
- (2) $|\lambda x| = |\lambda||x|$,
- (3) $|x + y| \leq |x| + |y|$

pour tout $x, y \in \mathbb{R}$ et $\lambda \in \mathbb{R}$.

Afin de donner une notion de limite pour les fonctions de plusieurs variables, nous devons trouver un moyen de définir les notions de « taille » d'un vecteur et de distance entre deux points de $\mathbb{R}^n$, avec $n > 1$. La notion de « taille » doit satisfaire propriétés analogues à celles de la valeur absolue.

La première notion de « taille » pour un vecteur de $\mathbb{R}^2$ que nous vient à l'esprit est la longueur du segment entre l'origine et l'extrémité libre du vecteur. Cela peut être calculée à l'aide du théorème de Pythagore :

$$\text{taille de } (a, b) = \sqrt{a^2 + b^2}. \quad (7.217)$$

Nous pouvons introduire une notion de distance entre les éléments de $\mathbb{R}^2$ de façon similaire :

$$d((a_x, a_y), (b_x, b_y)) = \sqrt{(a_x - b_x)^2 + (a_y - b_y)^2}. \quad (7.218)$$

Cette définition a l'air raisonnable ; est-elle mathématiquement correcte ? Peut-elle jouer le rôle de la valeur absolue dans $\mathbb{R}^2$? Est-elle la seule définition possibles de « taille » et distance en $\mathbb{R}^2$?

Nous voulons formaliser les notions de « taille » et de distance dans $\mathbb{R}^n$, et plus généralement dans un espace vectoriel V de dimension finie. Pour cela nous nous inspirons des propriétés de la valeur absolue.

7.12.0.1 Critère de Cauchy

Théorème 7.201 (Bolzano-Weierstrass, thème 12).

Toute suite contenue dans un compact admet une sous-suite convergente.

Démonstration. Nous faisons la preuve par l'absurde en supposant que (x_k) n'admette pas de sous-suite convergente. Soit $a \in K$; aucune sous-suite de (x_k) ne converge vers a . En particulier, il existe un voisinage ouvert $\mathcal{O}_a$ de a et une partie finie I_a de $\mathbb{N}$ tel que $x_k \in \mathcal{O}_a$ seulement pour $k \in I_a$.

Les ouverts $\mathcal{O}_a$ recouvrent K ; nous pouvons en extraire un sous-recouvrement fini (c'est la définition 7.50 de la compacité). Nous avons donc des points $a_1, \dots, a_n$ tels que

$$K \subset \bigcup_{i=1}^n \mathcal{O}_{a_i} \quad (7.219)$$

et tels que pour chaque $\mathcal{O}_{a_i}$, nous avons $x_k \in \mathcal{O}_{a_i}$ seulement pour $k \in I_{a_i}$. Bien entendu, toute la suite est dans K et donc dans l'union.

En conclusion, nous avons $\mathbb{N} = \bigcup_{i=1}^n I_{a_i}$, ce qui prouve que $\mathbb{N}$ est un ensemble fini. Contradiction avec la proposition 1.99 qui dit que $\mathbb{N}$ est infini. $\square$

Lemme 7.202.

Une suite de Cauchy⁶⁷ dans un espace vectoriel normé admettant une sous-suite convergente est elle-même convergente vers la même limite.

67. Définition 7.171.

Démonstration. Soit (a_n) une suite de Cauchy dans un espace vectoriel normé E et ℓ la limite d'une sous-suite de (a_n) . Soit $\epsilon > 0$ et $N \in \mathbb{N}$ tel que $\|a_m - a_p\| < \epsilon$ dès que $m, p \geq N$. Nous allons montrer que si $k > N$ alors $\|a_k - \ell\| < 2\epsilon$. Pour cela nous considérons un $n > N$ tel que $\|a_n - \ell\| \leq \epsilon$ et nous calculons

$$\|a_k - \ell\| \leq \|a_k - a_n\| + \|a_n - \ell\| \leq 2\epsilon. \quad (7.220)$$

□

Dans le cas des espaces de dimension finie, le fait d'être complet est automatique, comme le montre la proposition suivante.

Proposition 7.203.

Soit $(E, \|\cdot\|)$ un espace vectoriel normé de dimension finie sur un corps $\mathbb{K}$ qui est complet⁶⁸. Alors E est complet⁶⁹.

Pour rappel, la complétude de l'espace métrique $\mathbb{R}$ est la proposition 1.275.

Démonstration. Nous considérons une suite de Cauchy (f_n) dans E et si $\{e_\alpha\}$ est une base orthonormée de E nous définissons les coefficients $f_n = \sum_\alpha a_{n\alpha} e_\alpha$. La somme sur α est finie par hypothèse sur la dimension de E .

Nous avons

$$\|f_n - f_m\| = \left\| \sum_\alpha (a_{n\alpha} - a_{m\alpha}) e_\alpha \right\| = \sum_\alpha |a_{n\alpha} - a_{m\alpha}|^2. \quad (7.221)$$

Pour tout ϵ , il existe N tel que si $m, n > N$ alors $|a_{n\alpha} - a_{m\alpha}| < \sqrt{\epsilon}$. Autrement dit, pour chaque α , la suite $(a_{n\alpha})_{n \in \mathbb{N}}$ est de Cauchy dans $\mathbb{K}$ et converge donc dans $\mathbb{K}$. Soit a_α la limite et définissons $f = \sum_\alpha a_\alpha e_\alpha$. Nous avons alors

$$\|f_n - f\| = \left\| \sum_\alpha (a_{n\alpha} - a_\alpha) e_\alpha \right\|, \quad (7.222)$$

dont la limite $n \rightarrow \infty$ est bien zéro. Donc la suite (f_n) converge vers $f \in E$. L'espace E est alors complet. □

Proposition 7.204.

Soient V et W deux espaces vectoriels normés. Soient K une partie compacte de V et $f: K \rightarrow W$ une fonction continue. Alors l'image $f(K)$ est compacte dans W .

Ce résultat est démontré dans un cadre plus général par le théorème 7.97.

Démonstration. Nous allons prouver que $f(K)$ est fermée et bornée.

$f(K)$ est fermé Nous allons prouver que si (y_n) est une suite convergente contenue dans $f(K)$, alors la limite est également contenue dans $f(K)$. Dans ce cas, nous aurons que l'adhérence de $f(K)$ est contenue dans $f(K)$ et donc que $f(K)$ est fermé. Pour chaque $n \in \mathbb{N}$, le vecteur y_n appartient à $f(K)$ et donc il existe un $x_n \in K$ tel que $f(x_n) = y_n$. La suite (x_n) ainsi construite est une suite dans le fermé K et possède donc une sous-suite convergente (proposition 7.201). Notons (x'_n) cette sous-suite convergente, et a sa limite : $\lim(x'_n) = a \in K$. Le fait que la limite soit dans K provient du fait que K est fermé.

Nous pouvons considérer la suite $f(x'_n)$ dans W . Cela est une sous-suite de la suite (y_n) , et nous avons $\lim f(x'_n) = a$ parce que f est continue. Par conséquent nous avons

$$f(a) = \lim f(x'_n) = \lim y_n. \quad (7.223)$$

Cela prouve que la limite de (y_n) est dans $f(K)$ et par conséquent que $f(K)$ est fermé.

68. La définition est 1.253, mais si vous n'avez pas envie de vous embarquer trop loin, dites juste « toutes les suites de Cauchy convergent ». Typiquement c'est $\mathbb{R}$ ou $\mathbb{C}$.

69. Définition 7.172.

$f(K)$ est borné Si $f(K)$ n'est pas borné, nous pouvons trouver une suite (x_n) dans K telle que

$$\|f(x_n)\|_W > n \quad (7.224)$$

Mais par ailleurs, l'ensemble K étant compact (et donc fermé), nous avons une sous-suite (x'_n) qui converge dans K . Disons $\lim(x'_n) = a \in K$.

Par la continuité de f nous avons alors $f(a) = \lim f(x'_n)$, et donc

$$|f(a)| = \lim |f(x'_n)|. \quad (7.225)$$

La suite $f(x'_n)$ est alors une suite bornée, ce qui n'est pas possible au vu de la condition (7.224) imposée à la suite de départ (x_n) .

□

Corolaire 7.205.

Si $f: K \rightarrow \mathbb{R}$ est une application continue où K est une partie compacte d'un espace vectoriel normé, alors $f(K)$ est borné.

Démonstration. En effet, la proposition 7.204 montre que $f(K)$ est compact et donc borné. □

7.13 Espaces métriques

7.13.1 Espaces métrisables

Définition 7.206.

Un espace topologique est **métrisable** s'il est homéomorphe à un espace métrique.

Proposition 7.207.

Une fonction séquentiellement continue sur un espace métrisable et à valeurs dans un espace métrique est continue.

Démonstration. Soient E un espace métrique et $\phi: X \rightarrow (E, d)$ un homéomorphisme. Nous supposons que $f: X \rightarrow Y$ est séquentiellement continue. Nous considérons l'application $\tilde{f} = f \circ \phi^{-1}$, c'est-à-dire

$$\begin{aligned} \tilde{f}: E &\rightarrow Y \\ a &\mapsto f(\phi^{-1}(a)). \end{aligned} \quad (7.226)$$

L'application ϕ^{-1} est continue et donc séquentiellement continue. De plus $\tilde{f}$ est séquentiellement continue. En effet si $a_k \xrightarrow{E} a$, alors

$$\tilde{f}(a_k) = f(\phi^{-1}(a_k)), \quad (7.227)$$

mais ϕ^{-1} est séquentiellement continue, donc $\phi^{-1}(a_k) \xrightarrow{X} \phi^{-1}(a)$, ce qui signifie que $\phi^{-1}(a_k)$ est une suite convergente dans X et donc

$$\lim_{k \rightarrow \infty} \tilde{f}(a_k) = \lim_{k \rightarrow \infty} f(\phi^{-1}(a_k)) = f(\phi^{-1}(a)) = \tilde{f}(a). \quad (7.228)$$

L'application $\tilde{f}$ est donc séquentiellement continue. Mais étant donné que $\tilde{f}$ est définie sur un espace métrique (E) et à valeurs dans un métrique, elle est continue par la proposition 7.164. L'application $f = \tilde{f} \circ \phi$ est donc continue en tant que composée d'applications continues. □

7.13.2 Fonctions continues

La propriété suivante donne des caractérisations importantes de la continuité dans le cas des espaces métriques.

Proposition 7.208 (Continuité, ouverts et voisinages et limite[178]).

Soient $f: E \rightarrow F$ une application entre espaces métriques et $a \in E$. Alors nous avons équivalence entre les choses suivantes :

- (1) f est continue en a ,
- (2) Pour tout voisinage ouvert W de $f(a)$, il existe un voisinage ouvert V de a tel que $f(V) \subset W$.
- (3) Pour toute boule $W' = B(f(a), \epsilon)$, il existe une boule $V' = B(a, \delta)$ telle que $f(V) \subset W$.
- (4) $\forall \epsilon > 0, \exists \delta > 0$ tel que $f(B(a, \delta)) \subset B(f(a), \epsilon)$.
- (5) $\lim_{x \rightarrow a} f(x) = f(a)$ où la limite est donnée par la définition 7.70,
- (6) Pour tout $\epsilon > 0$, il existe $\delta > 0$ tel que $\|x - a\| < \delta$ implique $\|f(x) - f(a)\| < \epsilon$.

La proposition 7.237 nous montrera que ces équivalences tiennent encore lorsque l'espace a une topologie de seminormes.

Démonstration. L'équivalence (1) $\Leftrightarrow$ (2) est la définition 7.75. L'équivalence (3) $\Leftrightarrow$ (4) est une simple paraphrase.

Montrons (2) $\Rightarrow$ (3). Si $W' = B(f(a), \delta)$, nous avons un voisinage V de a tel que $f(V) \subset W$. L'ensemble V contenant une boule autour de chacun de ses points⁷⁰, il en contient un autour de a : $V' = B(a, \delta) \subset V$. A fortiori nous avons $f(V') \subset W$.

Montrons (3) $\Rightarrow$ (2). Si W est un ouvert autour de $f(a)$, il contient une boule autour de $f(a)$: $B(f(a), \epsilon) \subset W$. Il existe donc une boule $V' = B(a, \delta)$ telle que $f(V') \subset B(f(a), \epsilon) \subset W$.

L'équivalence (1) $\Leftrightarrow$ (5) est la définition 7.75 de la continuité en un point couplée à l'unicité de la limite due à la proposition 7.73 parce qu'un espace métrique est séparé.

Prouvons (5) $\Rightarrow$ (6). Soient $\epsilon > 0$ et $V = B(f(a), \epsilon)$. Étant donné que $f(a)$ est une limite de f pour $x \rightarrow a$, il existe un voisinage W de a tel que $f(W) \subset V$. Soit $\delta > 0$ tel que $B(a, \delta) \subset W$; alors si $\|x - a\| < \delta$ nous avons $x \in B(a, \delta) \subset W$ et donc $f(x) \in B(f(a), \epsilon)$, c'est-à-dire $\|f(a) - f(x)\| < \epsilon$.

Enfin l'implication (2) $\Rightarrow$ (5) est une réécriture de la définition de la limite en un point. $\square$

Voici un théorème qui parle de fermés emboîtés dans un espace métrique. Le corolaire 7.60 parle du cas $\cap_i A_i = \emptyset$ dans un compact.

Théorème 7.209 (Théorème des fermés emboîtés[179]).

Soit (E, d) un espace métrique. Il est complet si et seulement si toute suite décroissante de fermés non vides dont le diamètre tend vers zéro a une intersection qui se réduit à un seul point.

Démonstration. En deux parties.

Condition suffisante Soit $\{F_n\}_{n \in \mathbb{N}}$ une telle suite de fermés emboîtés. Si nous choisissons des points $x_n \in F_n$, nous obtenons une suite (x_n) de Cauchy et qui est par conséquent convergente vu que l'espace est par hypothèse complet. De plus, pour chaque $N \geq n$, la queue de suite $(x_n)_{n \geq N}$ est contenue dans F_N et donc converge vers un élément de F_N (parce que ce dernier est fermé). Donc la limite de (x_n) est dans $\bigcap_{n \in \mathbb{N}} F_n$.

De plus cette intersection a diamètre nul parce que le diamètre de $\bigcap_{n \in \mathbb{N}} F_n$ est majoré par tous les diamètres des F_n , lesquels sont arbitrairement petits par hypothèse. Donc l'intersection est réduite à un point.

Condition nécessaire Soit (x_n) un suite de Cauchy. Nous considérons les ensembles

$$F_n = \overline{\{x_i \text{ tel que } i \geq n\}}. \quad (7.229)$$

Le fait que la suite soit de Cauchy implique que $\text{diam}(F_n) \rightarrow 0$. Par hypothèse, nous avons alors

$$\bigcap_{n \in \mathbb{N}} F_n = \{a\}. \quad (7.230)$$

⁷⁰. Cela est le théorème-définition 7.99 des ouverts dans un espace métrique, à ne pas confondre avec le théorème 7.7.

Pour s'assurer que a est bien la limite de (x_n) , il suffit de remarquer que

$$d(x_n, a) \leq \text{diam } F_n \rightarrow 0. \quad (7.231)$$

□

Proposition 7.210.

Soient (X, d) un espace topologique métrique et F un fermé de X . Nous avons $d(x, F) = 0$ si et seulement si $x \in F$.

Démonstration. Si $x \in F$ alors $d(x, F) = 0$ parce que $d(x, x)$ fait partie de l'ensemble sur lequel nous prenons l'infimum.

Si réciproquement $d(x, F) = 0$, cela signifie que pour tout ϵ , il existe $x_\epsilon \in F$ tel que $d(x_\epsilon, x) \leq \psi$. En prenant $\epsilon = 1/k$ nous construisons une suite (x_k) d'éléments dans F vérifiant $d(x_k, x) = \frac{1}{k}$. Cela signifie que $\lim_{k \rightarrow \infty} x_k = x$ par la proposition 7.176(1).

Par la caractérisation séquentielle des fermés (un fermé contient les limites de toutes ses suites, proposition 7.161), la suite (x_k) étant dans F , la limite est dans F . Donc $x \in F$. □

Lemme 7.211.

Soit A_n une suite décroissante de fermés dans un espace métrique⁷¹ compact K . Alors

$$C = \bigcap_{n \in \mathbb{N}} A_n \quad (7.232)$$

est non vide.

Démonstration. Soit (x_n) une suite dans K telle que $x_n \in A_n$. La suite étant contenue dans A_1 , et A_1 étant compact (lemme 7.63), elle possède une sous-suite $(y_n = x_{\sigma_1(n)})$ convergente dont la limite est dans A_1 par le théorème de Bolzano-Weierstrass 7.108. Une queue de la suite y_n est dans A_2 et nous considérons donc une sous-suite convergente dans A_2 donnée par

$$z_n = y_{\sigma_2(n)} = x_{\sigma_1 \sigma_2(n)}. \quad (7.233)$$

En continuant ainsi nous construisons une suite convergente dans A_k . Nous considérons enfin la suite

$$y_n = x_{\sigma_1 \dots \sigma_n(n)}. \quad (7.234)$$

Pour tout k , une queue de cette suite est une sous-suite de $x_{\sigma_1 \dots \sigma_k(n)}$ et par conséquent cette suite converge dans A_k . La limite de cette suite est donc dans l'intersection demandée. □

Remarque 7.212.

Cette propriété est fautive pour les ouverts. Par exemple

$$\bigcap_{n > 1}]0, \frac{1}{n}[= \emptyset. \quad (7.235)$$

Lemme 7.213.

Si K est un compact dans un espace métrique et F un fermé disjoint de K , alors $d(K, F) > 0$.

Démonstration. La fonction

$$\begin{aligned} K &\rightarrow \mathbb{R} \\ x &\mapsto d(x, F) \end{aligned} \quad (7.236)$$

est une fonction continue sur K , et donc atteint son minimum par le théorème de Weierstrass 7.110. Soit $x_0 \in K$ un point de K qui réalise ce minimum. Si $d(x_0, F) = 0$, alors on aurait une suite (x_n) dans F qui convergerait vers x_0 , mais F étant fermé cela signifierait que x_0 serait dans F , ce qui contredirait l'hypothèse que F et K sont disjoints. □

⁷¹ L'hypothèse métrique provient de l'utilisation de Bolzano-Weierstrass, lequel est vrai pour les espaces séquentiellement compacts, dont les espaces métriques.

Proposition 7.214 ([164]).

Une isométrie d'un espace métrique compact sur lui-même est une bijection.

Démonstration. Soient X un espace métrique compact et $f: X \rightarrow X$ une isométrie. Le fait que f soit injective est obligatoire (sinon il y a des images dont la distance est nulle). Il faut montrer que f est surjective.

Soit $x \in X$ hors de $f(X)$. Le lemme 7.213 appliqué au fermé $\{x\}$ et au compact $f(K)$ donne un $r > 0$ tel que

$$d(x, f(K)) > r. \quad (7.237)$$

Soit la suite $u_n = f^n(x)$; c'est une suite dans K et possède donc une sous-suite convergente (Bolzano-Weierstrass 7.108) que l'on nomme (y_n) . Vu que f est une isométrie,

$$d(y_n, y_{n+1}) = d(x, y_m) > r \quad (7.238)$$

pour un certain $m \leq n + 1$. Cela signifie que pour tout n , nous avons $d(y_n, y_{n+1}) > r$, ce qui contredit le fait que la suite (y_n) converge. $\square$

Proposition 7.215.

Soient (X, d) un espace métrique compact et (u_n) une suite de X telle que

$$\lim_{n \rightarrow \infty} d(u_n, u_{n+1}) = 0. \quad (7.239)$$

Alors l'ensemble des points d'accumulation ⁷² de (u_n) est connexe.

Démonstration. Nous notons Γ l'ensemble des points d'accumulation de la suite.

Γ est compact Nous notons $A_p = \{u_n \text{ tel que } n \geq p\}$ et nous avons

$$\Gamma = \bigcap_{p \in \mathbb{N}} \overline{A_p} \quad (7.240)$$

parce que si $x \in \Gamma$, alors pour tout n , il existe $m > n$ tel que $x_m \in B(x, \epsilon)$, et donc tel que $x \in B(x_m, \epsilon)$. Donc pour tout ϵ et pour tout p , l'intersection $B(x, \epsilon) \cap A_p$ est non vide.

En tant qu'intersection de fermés, Γ est fermé (lemme 7.6). En tant que fermé dans un compact, Γ est compact (lemme 7.63).

Recouvrement par deux compacts Supposons que Γ ne soit ⁷³ pas connexe. Nous pouvons alors considérer S et O , deux ouverts disjoints recouvrant Γ et intersectant tout deux Γ . Nous posons alors

$$A = S \cap \Gamma \quad (7.241a)$$

$$B = O \cap \Gamma, \quad (7.241b)$$

et nous avons évidemment $\Gamma = A \cup B$. Montrons que A est fermé (B le sera aussi par le même raisonnement). Soit une suite d'éléments de $S \cap \Gamma$ convergent dans X . Alors la limite est dans $\bar{\Gamma} = \Gamma$ et donc elle est donc O ou S , mais elle est certainement dans $\bar{S}$. Cependant $\bar{S}$ n'intersecte pas O . En effet si $x \in \bar{S} \cap O$, alors tout voisinage de x intersecterait S , mais il y a des voisinages de x étant inclus dans O parce que O est ouvert; cela donnerait une intersection entre O et S , ce qui est impossible. Donc la limite n'est pas dans O et donc elle est dans S . Au final la limite est dans $S \cap \Gamma$, ce qui prouve son caractère fermé.

Comme d'habitude, $\Gamma \cap S$ est compact parce que fermé dans un compact ⁷⁴.

72. Définition 7.29.

73. est-ce qu'il faut vraiment un subjonctif ici ?

74. Lemme 7.63.

Décomposition en trois morceaux Vu que A et B sont des compacts disjoints, nous avons $d(A, B) = \alpha > 0$ pour un certain α par le lemme 7.213. Nous notons

$$A' = \{x \in X \text{ tel que } d(x, A) < \frac{\alpha}{3}\} \quad (7.242a)$$

$$B' = \{x \in X \text{ tel que } d(x, B) < \frac{\alpha}{3}\} \quad (7.242b)$$

Nous avons $A' = \bigcup_{x \in A} B(x, \frac{\alpha}{3})$ et donc en tant qu'union d'ouverts, A' est ouvert (définition de la topologie). Même chose pour B' .

Enfin nous notons

$$K = X \setminus (A' \cup B') \quad (7.243)$$

qui est fermé en tant que complémentaire d'ouvert, et donc compact. Étant donné que $A \subset A'$ et $B \subset B'$, nous avons $K \cap \Gamma = \emptyset$.

L'idée est maintenant de montrer que K contient un point d'accumulation de (u_n) .

Sous-suites de (u_n) L'hypothèse sur la suite (u_n) nous indique qu'il existe un N_0 tel que $\forall n \geq N_0$,

$$d(u_n, u_{n+1}) < \frac{\alpha}{3}. \quad (7.244)$$

Soient $N > N_0$ et $x_0 \in A$. Étant donné que x_0 est point d'accumulation de la suite, il existe $n_1 > N$ tel que $d(x_0, u_{n_1}) < \frac{\alpha}{3}$. Même chose dans B : nous prenons $y_0 \in B$ et un naturel $n_2 > n_1$ tel que $d(y_0, u_{n_2}) < \frac{\alpha}{3}$. Nous avons $u_{n_1} \in A'$ et $u_{n_2} \in B'$.

Soit n_0 le plus petit naturel supérieur à n_1 tel que $u_{n_0} \notin A'$. Cela existe parce que $u_{n_2} \in B'$ et $B' \cap A' = \emptyset$, mais n_0 n'est pas n_2 lui-même parce que $d(A', B') \geq \frac{\alpha}{3}$ alors que nous considérons $n_0, n_1, n_2 > N_0$ et donc pour tous les i entre n_1 et n_2 (compris), $d(u_i, u_{i+1}) < \frac{\alpha}{3}$. Notons qu'ici le strict dans la condition (7.244) est important. Nous avons donc $N_0 < n_1 < n_0 < n_2$.

Nous allons maintenant montrer que u_{n_0} est dans K . C'est fait pour : il est loin en même temps de A' et de B' . En utilisant l'inégalité triangulaire à l'envers, nous avons

$$\begin{aligned} d(u_{n_0}, B) &\geq d(u_{n_0-1}, B) - d(u_{n_0-1}, u_{n_0}) \\ &\geq d(A, B) - d(u_{n_0-1}, A) - d(u_{n_0-1}, u_{n_0}) \\ &\geq \alpha - \frac{\alpha}{3} - \frac{\alpha}{3} \\ &= \frac{\alpha}{3}. \end{aligned} \quad (7.245)$$

Pour la dernière inégalité nous avons utilisé le fait que u_{n_0-1} n'est pas dans A' . Bref, nous avons montré que u_{n_0} n'est pas dans B' (dans la définition de ce dernier nous avons bien une inégalité stricte). Vu que par définition u_{n_0} n'est pas non plus dans A' , nous avons $u_{n_0} \in K$. Nous avons montré jusqu'à présent que pour tout $N \geq N_0$, il existe un $n_0 \geq N$ tel que $u_{n_0} \in K$. Cela nous construit donc une sous-suite (v_n) de (u_n) contenue dans K . En tant que suite dans le compact K , la suite (v_n) admet un point d'accumulation dans K . Ce point est également point d'accumulation de la suite (u_n) complète, ce qui donne un point d'accumulation de (u_n) dans K et donc une contradiction.

Nous concluons que Γ est connexe. □

Encore une petite conséquence sans ambition du théorème de Bolzano-Weierstrass.

Proposition 7.216.

Si (x_n) est une suite dans un compact telle que toute sous-suite convergente ait le même point x comme limite. Alors la suite entière converge vers x .

Démonstration. Supposons que ce ne soit pas le cas. Alors il existe un ϵ tel que pour tout $N > 0$, il existe $n > N$ avec $d(x_n, x) > \epsilon$. Cela nous donne une sous-suite de (x_n) composée d'éléments

tous à une distance de x supérieure à ϵ . Nous la nommons (y_n) ; c'est une suite dans un compact qui admet donc une sous-suite convergente (et une telle sous-suite est une sous-suite de (x_n)) dont la limite devrait être x , mais c'est impossible par construction. $\square$

Lemme-Définition 7.217.

Soi Ω un ouvert dans un espace métrique E . Il existe une suite (K_n) de compacts tels que

- (1) $K_n \subset \Omega$
- (2) $\bigcup_{n=0}^{\infty} K_n = \Omega$
- (3) $K_n \subset \text{Int}(K_{n+1})$.

Une telle suite de compacts vérifie alors

- (1) Il existe δ_n tel que pour tout $z \in K_n$, $B(z, \delta_n) \subset K_{n+1}$.
- (2) Tout compact de Ω est inclus dans $\text{Int}(K_n)$ pour un certain n .

Une telle suite de compacts est une **suite exhaustive** de compacts pour Ω .

Démonstration. Nous considérons les ensembles

$$V_n = \{z \in E \text{ tel que } |z| \} \cup \bigcup_{a \notin \Omega} B(a, \frac{1}{n}), \quad (7.246)$$

et nous définissons $K_n = \complement V_n$. Vérifions que ces ensembles vérifient tout ce qu'il faut.

- (1) Si $a \notin \Omega$ alors a est dans tous les V_n et donc dans aucun des K_n ; nous avons donc bien $K_n \subset \Omega$.
- (2) Si $z \in \Omega$ alors nous prenons $n_1 > |z|$ puis n_2 tel que $B(z, \frac{1}{n_2}) \subset \Omega$. Alors $z \in K_n$ avec $n > \max(n_1, n_2)$.
- (3) Une chose à comprendre est que si $z \in K_n$, alors $d(z, \complement \Omega) \geq \frac{1}{n}$. Du coup si nous prenons δ tel que

$$\frac{1}{n+1} < \delta < \frac{1}{n} \quad (7.247)$$

alors $B(z, \delta) \subset K_{n+1}$.

- (4) Enfin, les K_n sont tous compacts. En effet ils sont bornés parce que $K_n \subset B(0, n)$ et ensuite K_n est fermé en tant que complémentaire d'un ouvert (V_n est ouvert en tant qu'union d'ouverts).

Nous passons maintenant aux propriétés, qui sont indépendantes de la façon dont nous avons construit les K_n vérifiant les conditions.

- (1) Nous pouvons considérer la fonction $K_n \rightarrow \mathbb{R}$ donnée par $z \mapsto d(z, \complement K_{n+1})$. Vu que $K_n \subset \text{Int}(K_{n+1})$, c'est une fonction (continue sur le compact K_n) prenant des valeurs strictement positives. Elle a donc un minimum strictement positif. Si δ_n est plus petit que ce minimum nous avons $B(z, \delta_n) \subset K_{n+1}$ pour tout $z \in K_n$.
- (2) D'abord nous avons $\Omega = \bigcup_{n=0}^{\infty} \text{Int}(K_n)$. En effet nous avons

$$\Omega = \bigcup_{n=0}^{\infty} K_n \subset \bigcup_{n=0}^{\infty} \text{Int}(K_{n+1}) \subset \bigcup_{n=0}^{\infty} \text{Int}(K_n). \quad (7.248)$$

L'inclusion dans l'autre sens est facile.

Soit K compact dans Ω . Vu que Ω est l'union des $\text{Int}(K_n)$, nous avons

$$K \subset \bigcup_{n=0}^{\infty} \text{Int}(K_n). \quad (7.249)$$

Cela donne à K un recouvrement par des ouverts dont nous pouvons extraire un sous-recouvrement fini par compacité. Les K_n étant croissants, du recouvrement fini, il suffit de prendre le plus grand (disons K_m) et nous avons $K \subset \text{Int}(K_m)$.

□

Notons qu'avec la suite de K_n telle que construite, le dernier point est réglé en prenant

$$\frac{1}{n+1} < \delta_n < \frac{1}{n}. \quad (7.250)$$

Lemme 7.218 ([180]).

Soient un compact $K \subset \mathbb{R}^d$ ainsi que des ouverts $\{\Omega_i\}_{i=1,\dots,n}$ tels que $K \subset \bigcup_{i=1}^n \Omega_i$.

Il existe des compacts $\{K_i\}_{i=1,\dots,n}$ tels que

- $K_i \subset \Omega_i$,
- $K \subset \bigcup_{i=1}^n K_i$.

Démonstration. Soit $x \in K$. Vu que les Ω_i recouvrent K , il existe un $k(x) \in \{1, \dots, n\}$ tel que $x \in \Omega_{k(x)}$. De plus, vu que $\Omega_{k(x)}$ est ouvert, il existe un voisinage de x contenu dans $\Omega_{k(x)}$ (théorème 7.7). Autrement dit, il existe $r(x) > 0$ tel que

$$\overline{B(x, r(x))} \subset \Omega_{k(x)}. \quad (7.251)$$

Vu que l'ensemble $\{B(x, r(x))\}_{x \in K}$ est un recouvrement de K par des ouverts, nous pouvons en extraire un sous-recouvrement fini⁷⁵. Soient donc $x_1, \dots, x_m \in K$ tels que

$$K \subset \bigcup_{i=1}^m B(x_i, r(x_i)). \quad (7.252)$$

Pour chaque $j = 1, \dots, n$, nous posons

$$A_j = \{l \in \{1, \dots, m\} \text{ tel que } k(x_l) = j\}. \quad (7.253)$$

Et enfin nous définissons, pour $j = 1, \dots, n$ les parties

$$K_j = \bigcup_{l \in A_j} \overline{B(x_l, r(x_l))} \quad (7.254)$$

et il nous reste à prouver que ces ensembles répondent bien à la question.

$\bigcup_{j=1}^n A_j = \{1, \dots, m\}$ **est une union disjointe** Un élément l de $A_i \cap A_j$ devrait vérifier $i = k(x_l) = j$. Si $s \in \{1, \dots, m\}$, alors $s \in A_{k(x_s)}$. Donc oui, l'union des A_j est tout $\{1, \dots, m\}$.

$K_j \subset \Omega_j$ Nous avons

$$K_j = \bigcup_{l \in A_j} \overline{B(x_l, r(x_l))} \subset \bigcup_{l \in A_j} \Omega_{k(x_l)} = \bigcup_{l \in A_j} \Omega_j = \Omega_j. \quad (7.255)$$

$K \subset \bigcup_{i=1}^n K_i$. Par (7.252), et vu que $\{1, \dots, m\} = \bigcup_{j=1}^n A_j$,

$$K \subset \bigcup_{i=1}^m B(x_i, r(x_i)) \quad (7.256a)$$

$$= \bigcup_{j=1}^n \bigcup_{l \in A_j} B(x_l, r(x_l)) \quad (7.256b)$$

$$= \bigcup_{j=1}^n \underbrace{\bigcup_{l \in A_j} \overline{B(x_l, r(x_l))}}_{K_j} \quad (7.256c)$$

$$= \bigcup_{j=1}^n K_j. \quad (7.256d)$$

75. C'est la définition 7.50 d'un compact.

□

Théorème 7.219 (Tykhonov).

Un produit quelconque d'espaces métriques non vides est compact si et seulement si chacun de ses facteurs est compact.

Nous n'allons donner la preuve que dans le cas d'un produit fini dans le théorème 7.225.

7.13.3 Ensembles enchainés

Soit (X, d) un espace métrique.

Définition 7.220.

Une ϵ -**chaîne** joignant les points a et b de X est une suite finie $(u_0, \dots, u_n)$ dans X telle que $u_0 = a$, $u_n = b$ et pour tout $0 \leq i \leq n-1$ nous avons $d(u_i, u_{i+1}) \leq \epsilon$.

Une partie A de X est **bien enchainée** si pour tout $\epsilon > 0$ et pour tout $a, b \in A$, il existe une ϵ -chaîne joignant a et b dans A .

Lemme 7.221.

Les rationnels dans $\mathbb{R}$ sont bien enchainés.

Démonstration. Soient p et q des rationnels avec $p < q$, ainsi que $\epsilon > 0$. Le lemme 1.307 nous permet de considérer un rationnel δ vérifiant $0 < \delta < \epsilon$. Et nous définissons les rationnels

$$r_k = p + k\delta. \quad (7.257)$$

Vu que $\mathbb{Q}$ est archimédien⁷⁶, il existe K tel que $r_K > q$. D'autre part, $r_0 = p < q$. Donc il existe $N = \max\{k \in \mathbb{N} \text{ tel que } r_k < q\}$.

Nous considérons la chaîne $(r_0, \dots, r_N, q)$. Elle débute à $r_0 = p$ et termine à q ; pas de problèmes avec ça. À part pour le dernier pas, nous avons

$$|r_N - r_{N-1}| = \delta < \epsilon, \quad (7.258)$$

donc c'est bien une ϵ -chaîne. Il reste à voir $|q - r_N|$. Nous avons $r_N \leq q \leq r_{N+1}$, et donc

$$0 \leq q - r_N \leq r_{N+1} - r_N = \delta \leq \epsilon. \quad (7.259)$$

Donc ok aussi pour ce dernier pas. □

Proposition 7.222 ([181, 1]).

Un espace métrique connexe⁷⁷ est bien enchainé.

Démonstration. Soit un espace métrique X et $\epsilon > 0$. La relation $x \sim y$ si et seulement si x et y peuvent être reliés par une ϵ -chaîne est une relation d'équivalence.

Soit $x \in X$. Nous prouvons que la classe $[x]$ est ouverte. En effet soit $y \in [x]$, si $z \in B(y, \epsilon)$ nous avons $z \in [y]$, et donc $z \in [x]$. Nous en déduisons que $B(y, \epsilon) \subset [x]$, et donc que $[x]$ est ouvert par le théorème 7.7.

Donc les classes sont des ouverts.

Supposons que X n'est pas bien enchainé. Alors il existe ϵ pour lequel X possède plus qu'une classe d'équivalence. Soit $\{[x_k]\}_{k \in I}$ l'ensemble des classes d'équivalences.

Nous considérons un $i_0 \in I$ quelconque, et nous définissons les ouverts $A = [x_{i_0}]$ et

$$B = \bigcup_{k \in I \setminus \{i_0\}} [x_k]. \quad (7.260)$$

Ce sont deux ouverts disjoints qui recouvrent X qui n'est donc pas connexe. □

⁷⁶. Proposition 1.269.

⁷⁷. Définition 7.44.

Proposition 7.223.

La fermeture d'un ensemble bien enchainé dans un espace métrique compact (X, d) est connexe.

Démonstration. Soit $A \subset X$ un ensemble bien enchainé, et soient $a, b \in \bar{A}$. Nous construisons une suite (u_k) dans A de la façon suivante. Pour chaque $n > 0$ nous prenons $a' \in B(a, \frac{1}{n}) \cap A$ et $b' \in B(b, \frac{1}{n}) \cap A$. Ensuite nous considérons une $\frac{1}{n}$ -chaîne $\{v_i^{(n)}\}_{i \in I_n}$ dans A entre a' et b' . Ici l'ensemble I_n est fini. La suite (u_k) est simplement construite en mettant bout à bout les éléments $v_i^{(n)}$.

La suite ainsi construite est une suite dans A admettant a et b comme points d'accumulation (les autres points d'accumulation sont également dans $\bar{A}$) et telle que $\lim_{k \rightarrow \infty} d(u_k, u_{k+1}) = 0$. Par conséquent la proposition 7.215 nous dit que l'ensemble des points d'accumulation de (u_k) est connexe dans X . Nous le notons $C_{a,b}$.

Si nous fixons $a \in \bar{A}$, alors nous avons

$$\bigcup_{x \in \bar{A}} C_{a,x} = \bar{A}. \quad (7.261)$$

Vu que le membre de gauche est une union de connexes, c'est un connexe par la proposition 7.48. $\square$

Corolaire 7.224.

Un espace métrique compact est connexe si et seulement s'il est bien enchainé.

Démonstration. Dans le sens direct, c'est la proposition 7.222. Dans l'autre sens, si X est compact, alors X est fermé par le lemme 7.63(2). Et vu qu'il est fermé et bien enchainé, la proposition 7.223 implique qu'il est connexe. $\square$

7.13.4 Produit fini d'espaces métriques

Pour rappel, la distance sur un espace produit est donnée par la définition 7.127.

Théorème 7.225 ([1]).

Un produit fini d'espaces métriques non vides est compact si et seulement si chacun de ses facteurs est compact.

Démonstration. Soient $K_1, \dots, K_n$ des compacts et $K = K_1 \times \dots \times K_n$ le produit muni de sa métrique usuelle de la définition (7.127) (attention : chacun des K_i peut être de dimension infinie) :

$$d(\alpha, \beta) = \max\{d_i(\alpha_i, \beta_i)\} \quad (7.262)$$

où d_i est la distance sur K_i . Si (α_n) est une suite dans K alors la suite $(\alpha_n)_1$ est une suite dans le compact K_1 dont nous pouvons extraire une sous-suite convergente (Bolzano-Weierstrass 7.108). De la sous-suite de α correspondante nous extrayons la sous-suite pour la seconde composante, etc.

En fin de compte nous avons une sous-suite (que nous nommons α également) donc chacune des composantes est convergente. Nous nommons ℓ_k les limites correspondantes. Soit $\epsilon > 0$ pour chaque $k = 1, \dots, n$, il existe $N_k > 0$ tel que si $p > N_k$ alors

$$d((\alpha_p)_k - \ell_k) \leq \epsilon. \quad (7.263)$$

Ici $\alpha_p \in K$ est le p^{e} élément de la suite α et $(\alpha_p)_i \in K_i$ est la i^{e} composante de α_p . En prenant $N = \max_k N_k$ et $n > N$ nous avons

$$d(\alpha_n, (\ell_1, \dots, \ell_n)) \leq \epsilon. \quad (7.264)$$

Par conséquent de la suite (α) nous avons extrait une sous-suite convergente et la partie « réciproque » de Bolzano-Weierstrass nous assure alors que K est compact.

À l'inverse si un des facteurs n'est pas compact (mettons K_1) alors nous prenons un recouvrement $\{\mathcal{O}_i\}_{i \in I}$ de K_1 par des ouverts duquel il est impossible d'extraire un sous-recouvrement fini. Ensuite nous posons

$$\mathcal{P}_i = \mathcal{O}_i \times K_2 \times \dots \times K_n, \quad (7.265)$$

qui est un recouvrement de K par des ouverts (de K) d'où aucun sous-recouvrement fini ne peut être extrait. $\square$

Pour la culture générale, il y a bien entendu moyen de faire des produits dénombrables et pire d'espaces métriques.

Définition 7.226 ([182]).

Soient (E_n, d_n) des espaces métriques. Sur l'ensemble produit $E = \prod_{i=1}^{\infty} E_i$ nous définissons la métrique

$$d(x, y) = \sum_{k=1}^{\infty} \frac{1}{2^k} d'_k(x_i, y_i) \quad (7.266)$$

où $d'_i = \min(d_i, 1)$.

On peut montrer que ce d est bien une distance et que (E, d) devient un espace métrique.

Théorème 7.227 (Tykhonov dénombrable[182]).

Un produit dénombrable d'espaces métriques non vides est compact si et seulement si chacun de ses facteurs est compact.

Note : ce résultat est encore valable pour un produit quelconque, c'est le théorème de Tykhonov 7.219.

7.13.5 Équicontinuité

Définition 7.228 ([183]).

Soit une famille de fonctions $f_i: X \rightarrow E$ indexée par un ensemble I où X est un espace topologique et E un espace métrique. Cette famille est **équicontinue** en $x \in X$ si pour tout $\epsilon > 0$, il existe un voisinage V de x tel que

$$\|f_i(x) - f_i(y)\| < \epsilon \quad (7.267)$$

pour tout i dès que $x, y \in V$.

Nous disons qu'une famille est équicontinue sans préciser en quel point si elle est équicontinue en tout point.

La proposition suivante permet de montrer que certaines fonctions définies par une limite sont continues. Ce sera par exemple le cas de la fonction puissance, proposition 12.368.

Proposition 7.229 ([1, 183]).

Soit une suite équicontinue (f_i) de fonctions qui converge simplement vers f , alors f est continue.

Démonstration. Soit une suite équicontinue $f_i: X \rightarrow E$ convergeant simplement vers f . Soit $a \in X$. Nous prouvons que f est continue en a . Pour cela nous considérons $\epsilon > 0$ et, conformément à l'hypothèse équicontinuité un voisinage V de a tel que $|f_i(a) - f_i(x)| < \epsilon$ pour tout $x \in V$.

Nous avons la majoration

$$|f(x) - f(a)| \leq |f(x) - f_i(x)| + |f_i(x) - f_i(a)| + |f_i(a) - f(a)|. \quad (7.268a)$$

Plusieurs majorations.

- Vu que $f_i \rightarrow f$, il existe N_1 tel que $|f(x) - f_i(x)| < \epsilon$ pour tout $i > N_1$.
- De plus, par définition de V , nous avons aussi $|f_i(x) - f_i(a)| \leq \epsilon$.
- Vu que $f_i \rightarrow f$, il existe N_2 tel que $|f_i(a) - f(a)| < \epsilon$ pour tout $i > N_2$.

Donc en prenant $x \in V$ et $i > \max\{N_1, N_2\}$ nous avons

$$|f(x) - f(a)| \leq 3\epsilon. \quad (7.269)$$

□

7.13.6 Continuité uniforme

Définition 7.230 ([184]).

Soient deux espaces métriques (E, d) et (E', d') . Une application $f: E \rightarrow E'$ est **uniformément continue** si pour tout $\epsilon > 0$, il existe $\delta > 0$ tel que $d(x, y) \leq \delta$ implique $d'(f(x), f(y)) \leq \epsilon$.

Dans l'uniforme continuité, le α qui fait fonctionner ϵ doit le faire fonctionner pour tous les $x, y \in E$. C'est la différence avec la continuité simple dans laquelle nous pouvons choisir, pour un même ϵ , un δ différent en chaque point.

7.14 Ensembles nulle part denses

Nous allons nous limiter au cas de $\mathbb{R}$, mais je crois que ça se généralise sans trop de peine aux espaces métriques, voire plus. Voir aussi la section 7.16 sur les espaces de Baire.

Définition 7.231.

Un ensemble est dit **nulle part dense** s'il n'est dense dans aucun intervalle.

Un ensemble dans $\mathbb{R}$ est de **première catégorie** ou **maigre** s'il est une union dénombrable d'ensembles nulle part dense (c'est-à-dire d'ensembles denses sur aucun intervalle).

Théorème 7.232 (Baire[185]).

Une réunion dénombrable d'ensembles nulle part denses est d'intérieur vide.

Démonstration. Soient $a \in S$ et $\epsilon > 0$. Nous allons trouver un élément dans $B(a, \epsilon)$ qui n'est pas dans S . Nous commençons par choisir $x_1 \in B(a, \epsilon)$ et $r_1 < \frac{\epsilon}{2}$ tel que

$$B(x_1, r_1) \cap A_1 = \emptyset. \quad (7.270)$$

Ensuite nous choisissons $x_2 \in B(x_1, r_1)$ et $r_2 < \epsilon/4$ tel que $B(x_2, r_2) \subset B(x_1, r_1)$ et $B(x_2, r_2) \cap A_2 = \emptyset$. Notons que $B(x_2, r_2) \cap A_1 = \emptyset$ aussi, par construction.

Par récurrence nous construisons une suite d'éléments x_n et de rayons $r_n < \epsilon/2^n$ tels que

- (1) $B(x_n, r_n) \cap A_j = \emptyset$ pour tout $j \leq n$,
- (2) $\overline{B(x_n, r_n)} \subset B(x_{n-1}, r_{n-1})$.

Cette suite étant de Cauchy (parce que contenue dans des intervalles emboîtés de rayon décroissant vers zéro), elle converge⁷⁸ donc vers un point qui en particulier appartient à $B(a, \epsilon)$. Mais la limite n'est dans aucun des A_n et donc pas dans S . □

7.15 Topologie des seminormes

Les principaux espaces topologiques construits avec des seminormes seront les espaces de fonctions de la définition 30.13. Nous verrons également la topologie *-faible sur $\mathcal{D}'(\Omega)$ en la définition 30.21.

Définition 7.233.

Si E est un espace vectoriel, une **seminorme** sur E est une application $p: E \rightarrow \mathbb{R}$ telle que

- (1) $p(x) \geq 0$,

78. Par la proposition 1.275

$$(2) \quad p(\lambda x) = |\lambda|p(x)$$

$$(3) \quad p(x + y) \leq p(x) + p(y).$$

La seule différence avec une norme est simplement qu'une seminorme peut s'annuler en des éléments non-nuls de l'espace.

Lemme 7.234 ([186]).

Si p est une seminorme⁷⁹ nous avons

$$|p(x) - p(y)| \leq p(x - y). \quad (7.271)$$

Démonstration. Nous avons d'une part $p(x + h) \leq p(x) + p(h)$ et d'autre part $p(x) \leq p(x + h) + p(-h) = p(x + h) + p(h)$. En isolant $p(x + h) - p(x)$ dans chacune de ces deux inégalités,

$$-p(h) \leq p(x + h) - p(x) \leq p(h) \quad (7.272)$$

ou encore

$$|p(x + h) - p(x)| \leq p(h) \quad (7.273)$$

qui donne le résultat demandé en posant $h = y - x$. $\square$

Soit $(p_i)_{i \in I}$ une famille de seminormes sur E . Nous construisons alors une topologie sur E de la façon suivante.

Définition 7.235 (Topologie et seminormes[187, 188]).

Soient des seminormes $\{p_i\}_{i \in I}$. Pour tout J fini dans I nous définissons les **boules ouvertes**

$$B_J(x, r) = \{y \in E \text{ tel que } p_j(y - x) < r \forall j \in J\}. \quad (7.274)$$

La **topologie** sur E donnée par la famille de seminorme est définie en disant que $\mathcal{O} \subset E$ est ouvert si et seulement si chaque point de $\mathcal{O}$ est dans une boule contenue dans $\mathcal{O}$.

Proposition 7.236.

Soit un ensemble E muni de la topologie des seminormes $\{p_i\}_{i \in I}$. Une suite (x_n) dans E converge vers x si et seulement si pour tout $i \in I$,

$$p_i(x - x_n) \rightarrow 0. \quad (7.275)$$

Démonstration. Si la suite (x_n) converge⁸⁰ vers x , alors pour tout ouvert $\mathcal{O}$ autour de x , il existe un N tel que si $n \geq N$, alors $x_n \in \mathcal{O}$. En particulier pour tout j et pour tout $\epsilon > 0$, il doit exister un $n \geq N_j$ tel que $x_n \in B_j(x, \epsilon)$.

Voyons l'implication inverse. Soit $\epsilon > 0$. Pour tout $i \in I$, il existe un N_i tel que $n \geq N_i$ implique $p_i(x - x_n) \leq \epsilon$. Si $\mathcal{O}$ est un ouvert, il doit contenir une boule du type $B_J(x, r)$ pour un certain ensemble fini $J \subset I$.

En prenant $N = \max\{N_j \text{ tel que } j \in J\}$, nous avons $p_j(x - x_n) \leq \epsilon$ pour tout j et donc $x_n \in B_J(x, r)$. $\square$

La proposition suivante est un vulgaire plagiat de la proposition 7.208.

Proposition 7.237.

Soit $f: \mathbb{R} \rightarrow (E, p_i)_{i \in I}$ une application. Nous avons équivalence entre

(1) la fonction f est continue en $t_0 \in \mathbb{R}$,

(2) si W est un voisinage ouvert de $f(t_0)$ il existe un voisinage ouvert V de t_0 (dans $\mathbb{R}$) tel que $f(V) \subset W$,

79. Définition 7.233.

80. Définition 7.13.

(3) pour tout $i \in I$ et $\epsilon > 0$ il existe $\delta > 0$ tel que

$$f(B(t_0, \delta)) \subset B_i(f(t_0), \epsilon). \quad (7.276)$$

Démonstration. L'équivalence (1) $\Leftrightarrow$ (2) est la définition 7.75.

Prouvons (2) $\Rightarrow$ (3). Soient $i \in I$ et $\epsilon > 0$. Considérons la boule $B_i(f(t_0), \epsilon)$, qui est un ouvert de E contenant $f(t_0)$. Il existe donc un ouvert V autour de t_0 tel que $f(V) \subset B_i(f(t_0), \epsilon)$. En particulier V contient une boule $B(t_0, \delta)$ et nous avons

$$f(B(t_0, \delta)) \subset f(V) \subset B_i(f(t_0), \epsilon). \quad (7.277)$$

Prouvons (3) $\Rightarrow$ (2). Soit W un ouvert autour de $f(t_0)$. Il existe un $i \in I$ et $\epsilon > 0$ tel que $B_i(f(t_0), \epsilon) \subset W$. Nous avons alors un $\delta > 0$ tel que

$$f(B(t_0, \delta)) \subset B_i(f(t_0), \epsilon) \subset W. \quad (7.278)$$

□

Lorsqu'on a un espace E muni d'une quantité dénombrable de seminormes $\{p_k\}_{k \in I}$ nous définissons l'écart⁸¹

$$d(x, y) = \sup_{k \geq 1} \min \left\{ \frac{1}{k}, p_k(x - y) \right\}. \quad (7.279)$$

Notons que cet écart est invariant par translation au sens où pour tout x, y, h dans E nous avons

$$d(x + h, y + h) = \sup_{k \geq 1} \min \left\{ \frac{1}{k}, p_k(x - y) \right\} = d(x, y). \quad (7.280)$$

Proposition 7.238.

Si X est un espace topologique dont la topologie est donnée par une famille dénombrable de seminormes, alors il est métrisable.

Proposition 7.239 ([186]).

La topologie donnée par les boules

$$B_k(a, r) = \{x \in E \text{ tel que } \forall k \leq \frac{1}{r}, p_k(x - a) < r\} \quad (7.281)$$

est la même que celle « usuelle » donnée par les seminormes. En disant « la même » nous entendons le fait que les ouverts sont les mêmes : A est ouvert pour une des deux topologies si et seulement s'il est ouvert pour l'autre.

Démonstration. Pour cette démonstration nous allons préfixer par d les notions topologiques issues des boules (7.281) et par P celle des seminormes : P -continue, d -ouvert, etc.

D'abord nous avons

$$B(a, r) = \bigcap_{k \leq \frac{1}{r}} B_k(a, r). \quad (7.282)$$

Si $\mathcal{O}$ est un d -ouvert, il contient une d -boule autour de chacun de ses points. Or d'après la formule (7.282), une d -boule est une intersection finie de P -ouverts et donc est un P -ouvert par définition. Donc $\mathcal{O}$ contient un P -ouvert autour de tous ses points et est donc P -ouvert.

Inversement nous supposons que $\mathcal{O}$ est un P -ouvert. Commençons par prouver que les seminormes p_k sont d -continues. En effet soient $k \in \mathbb{N}$, $\epsilon \leq \frac{1}{k}$ et $x, y \in E$ tels que $d(x, y) \leq \epsilon$; nous avons

$$|p_k(y) - p_k(x)| \leq p_k(x - y) \quad (7.283a)$$

$$= \min \left\{ \frac{1}{k}, p_k(x - y) \right\} \quad (7.283b)$$

$$\leq d(x, y) \quad (7.283c)$$

$$\leq \epsilon. \quad (7.283d)$$

81. Dans le cas de $E = \mathcal{D}(K)$, la première seminorme est numérotée à zéro, donc il faudra poser $d(\varphi_1, \varphi_2)$ avec p_{k-1} au lieu de p_k .

Montrons à présent que $\mathcal{O}$ est d -ouverte. Si $a \in \mathcal{O}$, il existe k et r tels que $B_k(a, r) \subset \mathcal{O}$. Soit $x \in B_k(a, r)$. Montrons que si ϵ est suffisamment petit, la d -boule $B(x, \epsilon)$ est incluse à $B_k(a, r)$. Pour cela prenons $y \in B(x, \epsilon)$; nous avons

$$|p_k(a - x) - p_k(a - y)| \leq d(x, y) \leq \epsilon. \quad (7.284)$$

Par conséquent le nombre $p_k(a - y)$ est dans l'intervalle

$$p_k(a - x) \pm \epsilon \quad (7.285)$$

et il suffit de prendre $\epsilon < \frac{r - p_k(a - x)}{2}$. $\square$

7.15.1 Espace dual

Nous parlerons plus en détail d'espace dual d'un espace normé en la section 11.13.

Définition 7.240.

Soient F un espace métrique et E un espace topologique vectoriel. Une topologie possible⁸² sur l'espace des applications linéaires $\mathcal{L}(E, F)$ est la **topologie *-faible** qui est la topologie des seminormes

$$p_v(T) = \|T(v)\|_F. \quad (7.286)$$

C'est une famille de seminormes indicées par les éléments de E . Si E est un espace métrique, c'est cette topologie qui sera considérée sur son dual topologique E' des applications continues $E \rightarrow \mathbb{R}$.

La proposition suivante indique qu'elle est un peu la topologie de la convergence ponctuelle.

Proposition 7.241.

Soient E un espace muni de la topologie des seminormes $\{p_i\}_{i \in I}$ et F un espace métrique. Soient une suite (T_n) dans $\mathcal{L}(E, F)$ et $T \in \mathcal{L}(E, F)$. Nous avons $T_n \xrightarrow{*} T$ si et seulement si $T_n(v) \xrightarrow{F} T(v)$ pour tout $v \in E$.

Démonstration. Nous avons équivalence entre les lignes suivantes :

$$T_n \xrightarrow{*} T \quad (7.287a)$$

$$p_v(T_n - T) \rightarrow 0 \forall v \in E \quad \text{proposition 7.236} \quad (7.287b)$$

$$\|T_n(v) - T(v)\|_E \rightarrow 0 \forall v \in E \quad (7.287c)$$

$$T_n(v) \xrightarrow{E} T(v). \quad (7.287d)$$

$\square$

7.15.2 Espace $C^k(\mathbb{R}, E')$

Nous revenons à nos histoires de limites de la définition 7.13.

Proposition 7.242 (Unicité de la limite dans un dual topologique).

Soient E un espace métrique et E' son dual topologique muni de sa topologie de la définition 7.240. Il y a unicité de l'élément de E' vers lequel une fonction $u: \mathbb{R} \rightarrow E'$ peut converger.

Démonstration. Soit T un élément vers lequel u_t converge lorsque $t \rightarrow t_0$. Soient $\epsilon > 0$ et $x \in E$. La boule $B_x(T, \epsilon)$ de E' subordonnée à la norme p_x et centrée en T est un ouvert de E' . Étant donné que u converge vers T il existe $\delta > 0$ tel que $u_t \in B_x(T, \epsilon)$ dès que $|t - t_0| \leq \delta$. Nous avons donc, pour tout $x \in E$, la limite (dans $\mathbb{R}$) :

$$\lim_{t \rightarrow t_0} u_t(x) = T(x). \quad (7.288)$$

82. C'est, dans l'idée, celle qui sera choisie pour les espaces de distributions, voir la définition 30.21.

Cela prouve que la convergence de u vers T implique l'existence pour tout x de la limite de $u_t(x)$ dans $\mathbb{R}$. Si T' est un autre élément vers lequel u_t converge, nous avons par le même raisonnement que

$$\lim_{t \rightarrow t_0} u_t(x) = T'(x). \quad (7.289)$$

Par unicité de la limite dans $\mathbb{R}$ nous devons alors avoir $T(x) = T'(x)$ pour tout x , c'est-à-dire $T = T'$. $\square$

Proposition 7.243.

Soit $u: \mathbb{R} \rightarrow E'$ une fonction continue. Alors

- (1) pour tout $x \in E$ la fonction $t \mapsto u_t(x)$ est continue,
- (2) pour tout $x \in E$ nous avons la limite dans $\mathbb{R}$

$$\lim_{t \rightarrow t_0} u_t(x) = u_{t_0}(x), \quad (7.290)$$

- (3) nous avons la limite dans E'

$$\lim_{t \rightarrow t_0} u_t = u_{t_0}. \quad (7.291)$$

Démonstration. Soient $x \in E$ et $\epsilon > 0$. Par la proposition 7.237 la continuité de u donne un $\delta > 0$ tel que

$$u_{B(t_0, \delta)} \subset B_x(u_{t_0}, \epsilon). \quad (7.292)$$

C'est-à-dire que si $|t - t_0| \leq \delta$ nous avons

$$|u_{t_0}(x) - u_t(x)| < \epsilon, \quad (7.293)$$

ce qui signifie bien que la fonction $t \mapsto u_t(x)$ est continue en tant que fonction $\mathbb{R} \rightarrow \mathbb{R}$. Cela est le point (1). Le théorème de limite et continuité dans $\mathbb{R}$ nous donne immédiatement la limite (7.290).

Nous passons à la preuve du point (3). Soit $\mathcal{O}$ un ouvert de E' contenant u_{t_0} . Il existe donc un $i \in I$ et $\epsilon > 0$ tel que $B_i(u_{t_0}, \epsilon) \subset \mathcal{O}$. Étant donné que u est continue, il existe $\delta > 0$ tel que

$$u_{B(t_0, \delta)} \subset B_i(u_{t_0}, \epsilon) \subset \mathcal{O}. \quad (7.294)$$

Cela signifie bien que

$$|t - t_0| \leq \delta \Rightarrow u_t \in \mathcal{O}, \quad (7.295)$$

c'est-à-dire que nous avons la limite $\lim_{t \rightarrow t_0} u_t = u_{t_0}$ dans E' . Pour dire cela nous avons utilisé la définition 7.70 de la limite et le résultat d'unicité 7.242. $\square$

Définition 7.244.

Si nous avons une application $u: \mathbb{R} \rightarrow E'$ nous considérons sa **dérivée** donnée par la limite

$$u'_{t_0} = \lim_{t \rightarrow t_0} \frac{u_t - u_{t_0}}{t - t_0}. \quad (7.296)$$

Cela est un nouvel élément de E' (pour peu que la limite existe). La fonction $u': \mathbb{R} \rightarrow E'$ ainsi définie peut être continue ou non. Cela nous permet de définir les espaces $C^k(\mathbb{R}, E')$ et $C^\infty(\mathbb{R}, E')$.

Une des principales utilisations que nous ferons de ces espaces seront les espaces de fonctions à valeurs dans les distributions tempérées dont nous parlerons dans la section 30.4.

7.16 Espaces de Baire

Définition 7.245.

Un **espace de Baire** est un espace topologique dans lequel toute intersection dénombrable d'ouverts denses est dense.

Lemme 7.246 ([189]).

Un espace topologique est de Baire si et seulement si toute union dénombrable de fermés d'intérieur vides est d'intérieur vide.

Théorème 7.247 (Théorème de Baire[189]).

Les espaces suivants sont de Baire :

- (1) *les espaces topologiques localement compacts,*
- (2) *les espaces métriques complets (donc ceux de Banach en particulier),*
- (3) *tout ouvert d'un espace de Baire.*

Démonstration. **Espaces topologiques localement compacts**

Espaces métriques complets Soit (E, d) un espace métrique complet. Soient V un ouvert quelconque de E et U_n une suite d'ouverts denses. Le but est de prouver que l'ensemble $\bigcap_{n \in \mathbb{N}} U_n$ intersecte V . Vu que V est ouvert dans un espace métrique, il contient une boule ouverte et donc une boule fermée B_0 de rayon strictement positif. L'ensemble U_1 est dense et intersecte donc un ouvert contenu dans B_0 . L'intersection est un ouvert qui contient alors une boule fermée B_1 de rayon strictement positif. Continuant ainsi nous construisons une suite de fermés emboîtés B_n telle que

$$\bigcap_{n \in \mathbb{N}} U_n \cap V \quad (7.297)$$

contient l'intersection des B_n . Par le théorème 7.209 des fermés emboîtés (que nous utilisons parce que E est métrique et complet), cette intersection est non vide.

Ouvert d'un espace de Baire

□

Parmi les applications du théorème de Baire, nous avons

- Le théorème de Banach-Steinhaus 11.143.
- Le théorème de l'application ouverte 11.152.

Chapitre 8

Espaces affines

8.1 Vecteurs agissant sur un espace

Définition 8.1.

Soit E , un espace vectoriel. Un **espace affine modelé sur E** est un ensemble $\mathcal{E}$ sur lequel le groupe $(E, +)$ agit à droite transitivement et librement¹.

Étant donné que E est un groupe commutatif, l'action peut être vue indifféremment à gauche ou à droite. Si $M \in \mathcal{E}$ et si $x \in E$ nous notons $M + x$ au lieu de $x \cdot M$ le résultat de l'action de x sur M .

8.2.

Lorsque nous écrivons « $M + x$ », le symbole plus n'est pas une loi de composition interne de $\mathcal{E}$, mais une action.

Proposition-Définition 8.3.

Soient $N, M \in \mathcal{E}$. Il existe un unique $x \in E$ tel que $M + x = N$.

Nous noterons $\overrightarrow{MN}$ ce vecteur.

Démonstration. La transitivité de l'action assure l'existence et la liberté assure l'unicité. $\square$

Proposition 8.4.

Soit un espace affine $\mathcal{E}$ modelé sur l'espace vectoriel E . Soient $A, B, C \in \mathcal{E}$. Nous avons les égalités suivantes dans E :

$$(1) \overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC} \text{ (relations de Chasles),}$$

$$(2) \overrightarrow{AA} = 0,$$

$$(3) \overrightarrow{BA} = -\overrightarrow{AB}.$$

Démonstration. Point par point.

Pour (1) Nous avons, par définition 8.3 les égalités

$$\begin{cases} C = A + \overrightarrow{AC} & (8.1a) \\ B = A + \overrightarrow{AB} & (8.1b) \\ C = B + \overrightarrow{BC} & (8.1c) \end{cases}$$

En substituant les deux premières dans la troisième, nous trouvons $A + \overrightarrow{AB} + \overrightarrow{BC} = A + \overrightarrow{AC}$.

Par liberté de l'action, nous pouvons « simplifier » par A et trouver la relation de Chasles.

Pour (2) Nous avons $A + \overrightarrow{AA} = A$, mais aussi $A + 0 = A$. Par unicité nous avons $\overrightarrow{AA} = 0$.

Pour (3) Nous avons $B + \overrightarrow{BA} = A$ et $A + \overrightarrow{AB} = B$. En mettant bout à bout,

$$B + \overrightarrow{BA} + \overrightarrow{AB} = B. \quad (8.2)$$

1. Définition 2.62.

Donc $\overrightarrow{BA} + \overrightarrow{AB} = 0$.

□

8.5.

Si E est un espace vectoriel, le groupe $(E, +)$ agit sur E par l'action $t_y(x) = y + x$. Utilisant cette action nous construisons l'**espace affine canonique** de E . En particulier nous notons $\mathcal{E}_n(\mathbb{K})$ l'espace affine canonique de $\mathbb{K}^n$ vu comme espace vectoriel sur $\mathbb{K}$.

- En tant qu'ensembles, $\mathcal{E}_n(\mathbb{K}) = \mathbb{K}^n$.
- Sur cet espace en particulier, si $M, N \in \mathcal{E}_n(\mathbb{K})$, nous avons $\overrightarrow{MN} = N - M$ où à droite, la différence est la différence vectorielle dans $\mathbb{K}^n$.

Ces deux points se généralisent immédiatement à un espace vectoriel E au lieu de $\mathbb{K}^n$.

8.2 Repères cartésiens affines

Soit E un $\mathbb{K}$ -espace vectoriel de dimension n et $\mathcal{E}$ un espace affine construit sur E .

Définition 8.6.

Un *multiplé* $(A, e_1, \dots, e_n)$ où A est un point de $\mathcal{E}$ et $\{e_i\}$ est une base de E est un **repère cartésien** de $\mathcal{E}$.

Nous disons que $\{e_i\}$ est la **base associée** au repère.

Proposition 8.7.

Si $\mathcal{E}$ est un espace affine modelé sur l'espace vectoriel E de dimension n sur le corps $\mathbb{K}$, et si $(A, \{e_i\}_{i=1, \dots, n})$ est un repère cartésien, alors

$$\begin{aligned} \phi: \mathbb{K}^n &\rightarrow \mathcal{E} \\ (x_1, \dots, x_n) &\mapsto A + \sum_i x_i e_i. \end{aligned} \quad (8.3)$$

est une bijection.

Ces nombres x_i sont les **coordonnées** du point $A + \sum_i x_i e_i$ dans le repère (A, e_i) .

Démonstration. L'application φ est surjective parce que l'action de E sur $\mathcal{E}$ est transitive et injective parce que l'action est libre. □

8.3 Classification affine des conique

Soit une conique $f(x, y) = 0$ avec

$$f(x, y) = ax^2 + 2bxy + cy^2 + 2dx + 2ey + f \quad (8.4)$$

dans le repère $R = (A, e_i)$. La signature de la quadratique

$$q(x, y) = ax^2 + 2bx + cy^2 \quad (8.5)$$

ne dépend pas de la base choisie et un changement de variables

$$\begin{cases} \tilde{x} = \alpha x + \beta y \\ \tilde{y} = \gamma x + \delta y \end{cases} \quad (8.6a)$$

$$\quad (8.6b)$$

peut nous amener dans trois cas :

$$q(x, y) = \begin{cases} \tilde{x}^2 + \tilde{y}^2 & \text{genre ellipse} \\ \tilde{x}^2 - \tilde{y}^2 & \text{genre hyperbole} \\ \tilde{x}^2 & \text{genre parabole.} \end{cases} \quad (8.7)$$

Dans le troisième cas, la matrice de q est de rang 1.

Nous cherchons maintenant à savoir si un point $I = (x_0, y_0)$ est un centre de symétrie de $f(x, y) = 0$. Pour cela nous choisissons le repère centré en I , c'est-à-dire que nous posons

$$\begin{cases} x = x_0 + \tilde{x} \\ y = y_0 + \tilde{y}. \end{cases} \quad (8.8a)$$

$$(8.8b)$$

Un peu de calcul montre qu'alors la conique s'écrit

$$f(x_0, y_0) + q(\tilde{x}, \tilde{y}) + (2ax_0 + 2by_0 + 2d)\tilde{x} + (2bx_0 + 2cy_0 + 2e)\tilde{y} = 0. \quad (8.9)$$

Le point I sera un centre de symétrie si les termes linéaires en $\tilde{x}$ et $\tilde{y}$ s'annulent, c'est-à-dire si

$$\begin{cases} ax_0 + by_0 + d = 0 \\ bx_0 + cy_0 + e = 0. \end{cases} \quad (8.10a)$$

$$(8.10b)$$

Nous supposons que $(d, e) \neq (0, 0)$, sinon la conique de départ serait déjà centrée. Le déterminant du système (8.10) est

$$\delta = ac - b^2. \quad (8.11)$$

Si ce dernier est différent de zéro, le système possède une unique solution et la conique aura alors un unique centre de symétrie.

Si le déterminant du système est nul, il y a soit pas de centre de symétrie, soit une infinité. Dans le premier cas nous sommes en présence d'une parabole, et dans le second cas de deux droites parallèles.

Exemple 8.8.

Soit

$$f(x, y) = x^2 + 2xy - y^2 - 6x + 2y - 1 = 0 \quad (8.12)$$

donnée dans le repère affine $R = (A, \{e_i\})$. Nous commençons par étudier la signature de $q(x, y) = x^2 + 2xy - y^2$ dont la matrice symétrique est

$$Q = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \quad (8.13)$$

Son polynôme caractéristique est $\lambda^2 - 2$ dont les racines sont $\pm\sqrt{2}$. La signature est donc $(1, -1)$ et nous sommes en présence d'une conique de genre hyperbole. Nous cherchons le centre en posant $x = \tilde{x} + x_0$, $y = \tilde{y} + y_0$. Le système à résoudre est

$$\begin{cases} x_0 + y_0 - 3 = 0 \\ x_0 - y_0 + 1 = 0, \end{cases} \quad (8.14a)$$

$$(8.14b)$$

dont l'unique solution est $(x_0, y_0) = (1, 2)$. Nous considérons le repère centré en (x_0, y_0) , c'est-à-dire le repère

$$R' = (I, \{e_i\}) \quad (8.15)$$

avec $I = A + x_0e_1 + y_0e_2$ où A est l'origine du repère dans lequel l'équation (8.12) était donnée.

Par construction dans ce repère nous avons la conique

$$f(x_0, y_0) + q(\tilde{x}, \tilde{y}) = 0, \quad (8.16)$$

c'est-à-dire

$$\tilde{x}^2 + 2\tilde{x}\tilde{y} - \tilde{y}^2 = 0. \quad (8.17)$$

Maintenant là nous avons une quadrique centrée nous voulons la mettre sous une forme plus canonique :

$$\left(\frac{1}{\sqrt{2}}(\tilde{x} + \tilde{y}) \right)^2 - \tilde{y}^2 - 1 = 0. \quad (8.18)$$

Nous posons donc

$$\begin{cases} X = \frac{1}{\sqrt{2}}(\tilde{x} + \tilde{y}) \\ Y = \tilde{y}, \end{cases} \quad \begin{matrix} (8.19a) \\ (8.19b) \end{matrix}$$

et nous trouvons l'hyperbole

$$X^2 - Y^2 - 1 = 0. \quad (8.20)$$

Cela revient à faire le changement de base

$$\begin{cases} e'_1 = \sqrt{2}e_1 \\ e'_2 = -e_1 + e_2. \end{cases} \quad \begin{matrix} (8.21a) \\ (8.21b) \end{matrix}$$

Pour rappel, les vecteurs de bases se transforment avec la matrice inverse des coefficients. Étant donné que

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \tilde{x} \\ \tilde{y} \end{pmatrix}, \quad (8.22)$$

nous avons

$$\begin{pmatrix} e'_1 \\ e'_2 \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} e_1 \\ e_2 \end{pmatrix}. \quad (8.23)$$

C'est de là que provient le changement (8.21). $\triangle$

8.4 Applications affines

Voici la définition d'une application affine entre deux espaces affines. La définition 12.93 donnera la définition d'une application affine entre espaces vectoriels.

Définition 8.9.

Soient $\mathcal{E}$ et $\mathcal{E}'$ deux espaces affines sur les espaces vectoriels E et E' (sur le même corps $\mathbb{K}$). Une application $f: \mathcal{E} \rightarrow \mathcal{E}'$ est dite **affine** si pour tout $M \in \mathcal{E}$, il existe une application linéaire² $u_M: E \rightarrow E'$ telle que

$$f(M + x) = f(M) + u_M(x) \quad (8.24)$$

pour tout $x \in E$.

La définition suivante permet de décomposer une application affine en une partie linéaire et une translation. À partir de là, la proposition 8.57 nous donnera une structure de groupe sur $\text{Aff}(\mathbb{R}^n)$.

Lemme-Définition 8.10 ([1]).

Soient $\mathcal{E}$ et $\mathcal{E}'$ deux espaces affines sur les espaces vectoriels E et E' (sur le même corps $\mathbb{K}$). Nous considérons une application affine $f: \mathcal{E} \rightarrow \mathcal{E}'$.

Il existe une unique application linéaire $u: E \rightarrow E'$ telle que

$$f(M + x) = f(M) + u(x) \quad (8.25)$$

pour tout $x \in E$ et pour tout $M \in \mathcal{E}$.

Cette application linéaire est appelée **partie linéaire** de f . Pour varier les notations, nous noterons souvent $f = \alpha \circ \tau_v$ pour une application linéaire α et la translation τ_v de vecteur v .

Démonstration. En plusieurs coups.

Unicité Supposons que u_1 et u_2 vérifient la propriété, alors pour tout $x \in E$ et tout $M \in \mathcal{E}$ nous avons $f(M + x) = f(M) + u_1(x)$ et $f(M + x) = f(M) + u_2(x)$. Cela suffit à nous convaincre que $u_1 = u_2$.

2. Définition 4.25.

$u_M = u_N$ Avant de prouver l'existence, nous considérons $M, N \in \mathcal{E}$ et les applications linéaires u_M et u_N vérifiant l'équation (8.24) pour M et N respectivement. Prouvons que $u_M = u_N$.

Posons

$$f(M + x) = f(M) + u_M(x) \quad (8.26a)$$

$$f(N + y) = f(N) + u_N(y). \quad (8.26b)$$

Définissons $a \in E$ par $N = M + a$; nous avons d'une part que

$$f(N + y) = f(M + y + a) = f(M) + u_M(y + a), \quad (8.27)$$

et d'autre part

$$f(N + y) = f(M + a) + u_N(y) = f(M) + u_M(a) + u_N(y). \quad (8.28)$$

Par conséquent $u_M(y + a) = u_M(a) + u_N(y)$. Par linéarité $u_N = u_M$.

Existence Soit $M \in \mathcal{E}$. Nous affirmons que u_M fait l'affaire. En effet, soient $N \in \mathcal{E}$ et $x \in E$. Vu que $u_M = u_N$ nous avons

$$f(N + x) = f(M) + u_N(x) = f(M) + u_M(x). \quad (8.29)$$

Donc effectivement u_M peut être utilisé en tout point de $\mathcal{E}$.

□

Ce lemme est important car il permet de démontrer qu'une application est affine en prouvant la linéarité des u_M séparément sans devoir prouver qu'elles sont égales.

8.4.1 Autres propriétés

Lemme 8.11 ([1]).

Soient $M \in \mathcal{E}$ et $A, B \in \mathcal{E}$ deux points donnés par $A = M + x_a$, $B = M + x_b$. Soit encore une application affine f sur $\mathcal{E}$. Alors

$$\overrightarrow{AB} = u_f(x_b - x_a). \quad (8.30)$$

Démonstration. En appliquant f à $A = M + x_a$ et $B = M + x_b$,

$$f(A) = f(M) + u_f(x_a) \quad (8.31a)$$

$$f(B) = f(M) + u_f(x_b). \quad (8.31b)$$

Donc $f(B) = f(A) - u_f(x_a) + u_f(x_b)$ ou encore

$$f(B) = f(A) + u_f(x_b - x_a). \quad (8.32)$$

□

Remarque 8.12.

La condition (8.24) pour tout $M \in \mathcal{E}$ est équivalente à demander

$$f \circ t_x = t_{u(x)} \circ f \quad (8.33)$$

pour tout $x \in E$.

Proposition 8.13.

Soit f une application affine.

- (1) Il existe une unique application linéaire u_f telle que $f(M + x) = f(M) + u_f(x)$ pour tout $M \in \mathcal{E}$ et tout $x \in E$.
- (2) L'application u_f est injective si et seulement si f est injective.

(3) L'application u_f est surjective si et seulement si f est surjective.

Si de plus les espaces $\mathcal{E}$ et $\mathcal{E}'$ ont même dimension finie, alors f est injective si et seulement si f est surjective.

Démonstration. La partie (1) est le lemme 8.10. □

Exemple 8.14.

L'espace $\mathbb{R}^n$ est très particulier parce qu'il agit sur lui-même; il est donc un espace affine à lui tout seul : $\mathcal{E} = E = \mathbb{R}^n$.

Dans le cas de $\mathbb{R}^n$, en posant $M = 0$ dans la condition (8.24), si f est une application affine il existe une application linéaire α et un vecteur v tel que $f = \tau_v \circ \alpha$.

Notons que ça n'a pas de sens de poser $M = 0$, et la décomposition $f = \tau_v \circ \alpha$ n'a aucun sens en général. En particulier, nous ne pouvons pas appliquer une application linéaire à un élément d'un espace affine général. △

Proposition 8.15.

Si $f: \mathcal{E} \rightarrow \mathcal{E}'$ et $g: \mathcal{E} \rightarrow \mathcal{E}''$ sont des applications affines, alors $g \circ f: \mathcal{E} \rightarrow \mathcal{E}''$ est affine et $u_{g \circ f} = u_g \circ u_f$.

Démonstration. Si $M \in \mathcal{E}$ et $x \in E$ nous avons

$$\begin{aligned} (g \circ f)(M + x) &= g(f(M) + u_f(x)) \\ &= f(f(M)) + u_g(u_f(x)) \\ &= (g \circ f)(M) + (u_g \circ u_f)(x). \end{aligned} \tag{8.34}$$

□

Théorème 8.16.

Soient $\mathcal{E}$ et $\mathcal{E}'$ deux espaces affines de dimensions finies p et q sur $\mathbb{K}$. Soient les repères cartésiens $R = (O, \{e_i\})$ et $R' = (O', \{e'_i\})$. Une application $f: \mathcal{E} \rightarrow \mathcal{E}'$ est affine si et seulement s'il existe une matrice $a \in \mathbb{M}_{p,q}(\mathbb{K})$ et $b \in \mathbb{K}^q$ tels que

$$f(x) = b + ax. \tag{8.35}$$

Remarque 8.17.

L'équation (8.35) est écrite en utilisant un abus de notation entre le vecteur $x \in \mathbb{K}^p$ et le point de $\mathcal{E}$ qui est représenté par x dans le repère $(A, \{e_i\})$.

8.5 Isomorphismes

Définition 8.18.

Un **isomorphisme** entre les espaces affines $\mathcal{E}$ et $\mathcal{E}'$ est une application affine $f: \mathcal{E} \rightarrow \mathcal{E}'$ inversible dont l'inverse est affine.

Proposition 8.19.

Une application affine bijective est un isomorphisme. Si f est un isomorphisme d'espaces affines, alors $u_{f^{-1}} = (u_f)^{-1}$.

Proposition 8.20.

Un espace affine de dimension finie n sur un corps $\mathbb{K}$ est isomorphe à l'espace affine canonique $\mathcal{E}_n(\mathbb{K})$.

Démonstration. Si nous considérons le repère $R = (A, \{e_i\})$ de l'espace affine $\mathcal{E}$ alors l'application

$$\begin{aligned} \varphi: \mathbb{K}^n &\rightarrow \mathcal{E} \\ (x_1, \dots, x_n) &\mapsto A + \sum_i x_i e_i \end{aligned} \tag{8.36}$$

est un isomorphisme. □

8.6 Sous espaces affines

Définition 8.21.

Soit $\mathcal{E}$ un espace affine sur l'espace vectoriel E . Un **sous-espace affine** de $\mathcal{E}$ est une orbite de l'action d'un sous-espace vectoriel de E .

Si $\mathcal{F}$ est un sous-ensemble de $\mathcal{E}$, il sera un sous-espace affine de $\mathcal{E}$ si et seulement si l'ensemble

$$F = \{AB \text{ tel que } A, B \in \mathcal{F}\} \quad (8.37)$$

est un sous-espace vectoriel de E . Dans ce cas nous disons que F est la **direction** de $\mathcal{F}$. Si $A \in \mathcal{F}$, alors l'orbite de A sous F est $\mathcal{F}$. La **dimension** de $\mathcal{F}$ est la dimension de sa direction.

Si $\mathcal{F}$ et $\mathcal{G}$ sont des sous-espaces affines de $\mathcal{E}$ de directions F et G , nous disons que $\mathcal{F}$ est **parallèle** à $\mathcal{G}$ si $F \subset G$.

Proposition 8.22.

Soit $\mathcal{F}$ un sous-espace affine de dimension k dans l'espace affine $\mathcal{E}$ de dimension n . Alors il existe une application affine $f: \mathcal{E} \rightarrow \mathbb{K}^{n-k}$ telle que $\mathcal{F} = f^{-1}(0)$.

Démonstration. Soient F la direction de $\mathcal{F}$ et $A \in \mathcal{F}$. Nous considérons une base $\{e_i\}$ adaptée à F au sens $\{e_1, \dots, e_k\}$ est une base de F . Nous considérons maintenant le repère cartésien $(A, \{e_i\})$ avec $A \in \mathcal{F}$ et nous construisons l'application affine

$$f: \mathcal{E} \rightarrow \mathbb{K}^{n-k} \\ A + \sum_{i=1}^n x_i e_i \mapsto \begin{pmatrix} x_{k+1} \\ \vdots \\ x_n \end{pmatrix}. \quad (8.38)$$

Par construction nous avons $f(M) = 0$ si et seulement si $M \in \mathcal{F}$. □

Proposition 8.23 ([32]).

Soit σ une partie de l'espace affine $\mathcal{E}$.

- (1) L'intersection de tous les sous-espaces affines contenant σ est un sous-espace affine, noté $\mathcal{F}$.
- (2) Si $A \in \sigma$, alors la direction de $\mathcal{F}$ est le sous-espace vectoriel

$$F = \text{Span}\{\overrightarrow{AM} \text{ tel que } M \in \sigma\}. \quad (8.39)$$

Le sous-espace affine donné par la proposition 8.23 est le sous-espace affine **engendré** par la partie σ , et il est noté $\text{eae}(\sigma)$.

Proposition 8.24.

Soit $\mathcal{E}$ un espace affine de dimension n sur $\mathbb{K}$, soit $f: \mathcal{E} \rightarrow \mathbb{K}^r$ une fonction affine. Pour tout $a = (a_1, \dots, a_r) \in \mathbb{K}^r$, l'ensemble $f^{-1}(a)$ est un sous-espace affine de dimension $\dim \ker(u_f)$.

Démonstration. Nous considérons le repère $(A, \{e_i\})$ de $\mathcal{E}$. Étant donné que f est affine nous avons

$$f\left(A + \sum_i x_i e_i\right) = f(A) + u_f\left(\sum_i x_i e_i\right). \quad (8.40)$$

Nous avons donc $f\left(A + \sum_i x_i e_i\right) = a$ lorsque

$$u_f\left(\sum_i x_i e_i\right) = a - f(A). \quad (8.41)$$

Nous avons donc

$$f^{-1}(a) = A + (u_f)^{-1}(a - f(A)), \quad (8.42)$$

dont la dimension est le rang de $(u_f)^{-1} = u_{f^{-1}}$ (proposition 8.19). Le rang de $(u_f)^{-1}$ est la dimension du noyau de u_f . □

Définition 8.25 (Partie convexe).

Une partie A d'un espace vectoriel est **convexe** si pour tout $a, b \in A$ et pour tout $t \in [0, 1]$, le point $ta + (1 - t)b$ est dans A .

Autrement dit, une partie est convexe lorsqu'elle contient tous les segments joignant ses points.

Proposition 8.26.

Soit un espace vectoriel normé³ $(V, \|\cdot\|)$. Pour tout $a \in V$ et $r > 0$, la boule $B(a, r)$ est convexe. La boule fermée $B(a, r)$ également.

Démonstration. En deux parties.

La boule centrée en zéro Soient $x, y \in B(0, r)$ et $\lambda \in]0, 1[$. Alors

$$\|\lambda x + (1 - \lambda)y\| \leq |\lambda|\|x\| + |1 - \lambda|\|y\| < (|\lambda| + |1 - \lambda|)r \leq r \quad (8.43)$$

où nous avons utilisé le fait que $|\lambda| = \lambda$ et $|1 - \lambda| = 1 - \lambda$.

Cela prouve que $\lambda x + (1 - \lambda)y \in B(0, r)$. Notez l'inégalité stricte due au fait que $\|x\| < r$ et $\|y\| < r$. Dans le cas de la boule fermée, nous avons une inégalité large.

La boule centrée autre part Soient $x, y \in B(a, r)$. Alors $x - a$ et $y - a$ sont dans $B(0, r)$, de telle sorte que

$$\lambda(x - a) + (1 - \lambda)(y - a) \in B(0, r) \quad (8.44)$$

par la première partie. En développant et simplifiant,

$$\lambda x + (1 - \lambda)y - a \in B(0, r), \quad (8.45)$$

ce qui signifie que $\lambda x + (1 - \lambda)y \in B(a, r)$.

□

Proposition 8.27.

Soit A un ensemble convexe⁴ dans un espace vectoriel et $v_1, \dots, v_n$ des éléments de A . Alors toute combinaison

$$a_1 v_1 + \dots + a_n v_n \quad (8.46)$$

telle que $a_1 + \dots + a_n = 1$ et $a_i \in [0, 1]$ appartient à A .

Démonstration. Nous prouvons la proposition pour $n = 3$. Nous devons trouver des nombres $t_1, t_2 \in [0, 1]$ tels que

$$t_2(t_1 v_1 + (1 - t_1)v_2) + (1 - t_2)v_3 = a v_1 + b v_2 + c v_3. \quad (8.47)$$

La réponse est immédiatement donnée par

$$t_2 a = 1 - c \quad (8.48a)$$

$$t_1 = a/t_2. \quad (8.48b)$$

Étant donné que $c \in [0, 1]$ nous avons $t_2 \in [0, 1]$. En ce qui concerne t_1 nous avons

$$t_1 = \frac{a}{t_2} \leq \frac{1 - c}{1 - c} = 1. \quad (8.49)$$

□

3. Définition 7.118.

4. Définition 8.25.

8.7 Barycentre

Soit $\mathcal{E}$ un espace affine sur le $\mathbb{K}$ -espace vectoriel E . Un couple (A, λ) avec $A \in \mathcal{E}$ et $\lambda \in \mathbb{K}$ est un **point pondéré**.

Lemme-Définition 8.28 ([190]).

Soit une famille de points pondérés $\{(A_i, \lambda_i)\}_{i=1\dots r}$. Si $\sum_i \lambda_i \neq 0$, alors il existe un unique $G \in \mathcal{E}$ tel que

$$\sum_{i=1}^r \lambda_i \overrightarrow{GA_i} = 0. \quad (8.50)$$

Le point G donné par le lemme 8.28 est le **barycentre** des points pondérés (A_i, λ_i) .

Notons que l'on peut toujours supposer que $\sum_i \lambda_i = 1$ parce que le barycentre ne change pas lorsque tous les λ_i sont multipliés par un même nombre.

Définition 8.29 (Combinaison convexe).

Des nombres $\lambda_1, \dots, \lambda_n$ vérifiant $\sum_i \lambda_i = 1$ forment une **combinaison convexe**.

Le théorème suivant donne quelques caractérisations équivalentes du barycentre.

Théorème 8.30 ([190]).

Soient $\{(A_i, \lambda_i)\}_{i=1,\dots,r}$ une famille de points pondérés. Les conditions suivantes sur le point $G \in \mathcal{E}$ sont équivalentes.

- (1) Le point G est barycentre de la famille.
- (2) Pour tout $\alpha \in \mathbb{R}^*$, $\sum_i (\alpha \lambda_i) \overrightarrow{GA_i} = 0$.
- (3) Il existe $A \in \mathcal{E}$ tel que $(\sum_i \lambda_i) \overrightarrow{AG} = \sum_i \lambda_i \overrightarrow{AA_i}$.
- (4) Pour tout $B \in \mathcal{E}$, nous avons $(\sum_i \lambda_i) \overrightarrow{BG} = \sum_i \lambda_i \overrightarrow{BA_i}$.

Définition 8.31.

Si $A, B \in \mathcal{E}$, le **segment** $[AB]$ est l'ensemble des barycentres de A et B pondérés par des poids positifs (ouvert ou fermé suivant que l'on accepte que l'un ou l'autre des poids soit nul).

Lorsque tous les λ_i sont égaux, nous parlons d'**isobarycentre**. Autrement dit, l'isobarycentre des points A_i est le barycentre des points pondérés $(A_i, 1)$.

8.7.1 Sous-espaces affines

Proposition 8.32.

Une partie $\mathcal{F}$ des $\mathcal{E}$ est un sous-espace affine si et seulement si elle est stable par barycentrisation.

Démonstration. Soit $\mathcal{F}$ une sous-espace affine de direction F et $A_1, \dots, A_n$ des points de $\mathcal{F}$. Nous devons voir que le barycentre des points A_i pondérés de n'importe quelles masses appartient à $\mathcal{F}$. Pour ce faire nous faisons appel à la caractérisation (4) du théorème 8.30 : pour tout $B \in \mathcal{F}$,

$$\overrightarrow{BG} = \sum_i \lambda_i \overrightarrow{BA_i}. \quad (8.51)$$

Vu que B et A_i sont dans $\mathcal{F}$, nous avons $\overrightarrow{BA_i} \in F$ et donc $\overrightarrow{BG} \in F$. Mais comme $B \in \mathcal{F}$, le point G est à son tour dans $\mathcal{F}$.

Réciproquement, nous supposons que $\mathcal{F}$ est stable par barycentrisme. Nous voudrions montrer que l'ensemble

$$F = \{\overrightarrow{AB} \text{ tel que } A, B \in \mathcal{F}\} \quad (8.52)$$

est un sous-espace vectoriel. Soit $A \in \mathcal{F}$. Nous commençons par prouver que les vecteurs de la forme $\overrightarrow{AX}$ ($X \in \mathcal{F}$) forment un espace vectoriel. Considérons $\overrightarrow{AX} + \overrightarrow{AY}$ qui est un élément de E ; il existe donc $V \in \mathcal{E}$ tel que

$$\overrightarrow{AV} = \overrightarrow{AX} + \overrightarrow{AY}. \quad (8.53)$$

Par les relations de Chasles,

$$\overrightarrow{AV} = \overrightarrow{AV} + \overrightarrow{VX} + \overrightarrow{AV} + \overrightarrow{VY}, \quad (8.54)$$

donc

$$0 = \overrightarrow{VX} - \overrightarrow{VA} + \overrightarrow{VY}, \quad (8.55)$$

ce qui prouve que V est un barycentre de X, A, Y , et donc que $V \in \mathcal{F}$. De la même manière si $W \in \mathcal{E}$ est défini par $\overrightarrow{AW} = \mu \overrightarrow{AX}$, alors

$$\overrightarrow{AW} = \mu \overrightarrow{AX} = \mu(\overrightarrow{AW} + \overrightarrow{WX}), \quad (8.56)$$

ce qui signifie que

$$(1 - \mu)\overrightarrow{AW} + \mu\overrightarrow{XW} = 0 \quad (8.57)$$

et que W est un barycentre.

Afin de montrer que (8.52) est bien un espace vectoriel, nous devons considérer $A, B, X, Y \in \mathcal{F}$ et prouver que $\overrightarrow{AX} + \overrightarrow{BY} \in F$. Nous avons

$$\overrightarrow{AX} + \overrightarrow{BY} = \overrightarrow{AX} + \overrightarrow{BA} + \overrightarrow{AY} \quad (8.58a)$$

$$= \overrightarrow{AV} + \overrightarrow{BA} \quad V \text{ est celui donné plus haut} \quad (8.58b)$$

$$= \overrightarrow{AV} - \overrightarrow{AB} \quad (8.58c)$$

$$= \overrightarrow{AV} + \overrightarrow{AW} \quad W \text{ est donné par } \mu = -1. \quad (8.58d)$$

$$= \overrightarrow{AV'}. \quad (8.58e)$$

□

Proposition 8.33 ([190]).

Soient $A_0, \dots, A_r$ des points de $\mathcal{E}$. L'ensemble des barycentres de ces points (avec des masses de somme 1) est le sous-espace affine engendré par les A_i que nous nommons $\mathcal{F}$.

Démonstration. Soit G le barycentre associé aux poids λ_i . Nous avons

$$G = A_0 + \overrightarrow{A_0G} = A_0 + \sum_{i=1}^r \lambda_i \overrightarrow{A_0A_i}. \quad (8.59)$$

Notons que les vecteurs $\overrightarrow{A_0A_i}$ sont dans la direction du sous-espace affine engendré par les A_i par (8.39). Donc G est bien dans $\mathcal{F}$.

Inversement si X est dans $\mathcal{F}$, on a

$$X = A_0 + \sum_i \lambda_i \overrightarrow{A_0A_i} \quad (8.60)$$

parce que $\sum_i \lambda_i \overrightarrow{A_0A_i}$ est un élément général de la direction de $\mathcal{F}$. Du coup

$$\overrightarrow{A_0X} = \sum_i \lambda_i \overrightarrow{A_0A_i}, \quad (8.61)$$

et en utilisant la relation de Chasles sur chacun des $\overrightarrow{A_0A_i}$,

$$\overrightarrow{A_0X} = \sum_i \lambda_i (\overrightarrow{A_0X} + \overrightarrow{XA_i}). \quad (8.62)$$

De là nous concluons que

$$(1 - \sum_i \lambda_i) \overrightarrow{A_0X} + \sum_i \lambda_i \overrightarrow{XA_i} = 0, \quad (8.63)$$

ce qui signifie précisément que X est un barycentre des A_i . □

Proposition 8.34.

Soient $r + 1$ point $A_0, \dots, A_r$ dans $\mathcal{E}$. Le sous-espace affine engendré par les A_i est au plus de dimension r .

Démonstration. La direction de l'espace engendré $\text{Aff}\{A_i\}$ est l'espace

$$\text{Span}\{\overrightarrow{A_0 A_{i=1, \dots, r}}\} \quad (8.64)$$

qui est engendré par r vecteurs et donc est au plus de dimension r . $\square$

En deux mots, la proposition suivante signifie que le barycentre des barycentres est le barycentre.

Proposition 8.35 (Associativité des barycentres[191]).

Soit $I = \{0, 1, \dots, n\}$ et une partition $I = J_0 \cup \dots \cup J_r$. Soient des points $a_0, \dots, a_n \in \mathcal{E}$ et $\lambda_0, \dots, \lambda_n$ des nombres tels que $\sum_i \lambda_i \neq 0$. Nous supposons que $\mu_k = \sum_{i \in J_k} \lambda_i \neq 0$ pour tout k , et enfin nous nommons b_k le barycentre de la famille $\{(a_i, \lambda_i), i \in J_k\}$.

Alors le barycentre de la famille $\{(b_k, \mu_k)\}_{k=1, \dots, r}$ est le barycentre de la famille $\{(a_i, \lambda_i)\}_{i \in I}$.

Démonstration. Nous nommons b le barycentre des b_k pondérés par les μ_k , donc par définition

$$0 = \sum_{k=0}^r \mu_k \overrightarrow{bb_k} \quad (8.65a)$$

$$= \sum_k \sum_{i \in J_k} \lambda_i \overrightarrow{bb_k} \quad (8.65b)$$

$$= \sum_{k=0}^r \sum_{i \in J_k} \lambda_i (\overrightarrow{ba_i} + \overrightarrow{a_i b_k}) \quad (8.65c)$$

$$= \sum_{k=0}^r \sum_{i \in J_k} \lambda_i \overrightarrow{ba_i} + \underbrace{\sum_{k=0}^r \sum_{i \in J_k} \lambda_i \overrightarrow{a_i b_k}}_{=0} \quad (8.65d)$$

$$= \sum_{i \in I} \lambda_i \overrightarrow{ba_i}. \quad (8.65e)$$

Donc b est bien barycentre des a_i avec les poids λ_i . $\square$

8.7.2 Enveloppe convexe**Définition 8.36.**

Soit A une partie d'un espace vectoriel E . L'**enveloppe convexe** de A , notée $\text{Conv}(A)$ est l'intersection de tous les convexes contenant A .

L'enveloppe convexe est un convexe. En effet soit C un convexe contenant A et $x, y \in \text{Conv}(A)$; alors x et y sont dans C et par conséquent le segment $[x, y]$ est inclus dans C . Ce segment étant inclus dans tout convexe contenant A , il est inclus dans $\text{Conv}(A)$.

Proposition 8.37 ([192]).

Soit C un convexe dans l'espace affine $\mathcal{E}$ et une famille de points pondérés $\{(a_i, \lambda_i)\}_{i=1, \dots, r}$ dont tous les poids sont positifs (et non tous nuls). Alors le barycentre est aussi dans C .

En d'autres termes, un convexe est stable par barycentrage à poids positifs⁵.

Démonstration. Nous prouvons par récurrence. D'abord pour $r = 2$. Le barycentre des points pondérés (a_1, λ_1) , (a_2, λ_2) est le point b tel que

$$\lambda_1 \overrightarrow{ba_1} + \lambda_2 \overrightarrow{ba_2} = 0. \quad (8.66)$$

5. Sauf si on prend tous les poids nuls; mais contre ce genre d'idées, on ne peut rien faire.

Par définition, ce qui est noté $\overrightarrow{ab}$ n'est rien d'autre que $b - a$; en déballant (8.66), nous trouvons

$$\lambda_1(a_1 - b) + \lambda_2(a_2 - b) = 0 \quad (8.67)$$

et donc

$$b = \frac{\lambda_1}{\lambda_1 + \lambda_2}a_1 + \frac{\lambda_2}{\lambda_1 + \lambda_2}a_2, \quad (8.68)$$

qui est bien un point du segment $[a_1, a_2]$ parce que c'est une combinaison à coefficients positifs de somme 1.

Nous passons maintenant à la vraie récurrence avec un ensemble de points pondérés

$$A_r = \{(a_1, \lambda_1), \dots, (a_r, \lambda_r)\} \quad (8.69)$$

de masse totale non nulle; et en vous laissant deviner ce que va désigner A_{r-1} . Si une des masses est nulle (disons λ_r), alors le barycentre de A_r est le même que celui de A_{r-1} et l'hypothèse de récurrence nous enseigne que ledit barycentre est dans C . Nous supposons donc que $\lambda_i \neq 0$ pour tout i . Dans ce cas le théorème d'associativité des barycentres 8.35 dit que le barycentre de A_r est le barycentre entre le barycentre de A_{r-1} et (a_r, λ_r) , qui sont deux points de C par hypothèse de récurrence. $\square$

Si E est un espace vectoriel et si $x_i \in E$ et $\lambda_i \in \mathbb{R}$, alors le barycentre des couples (x_i, λ_i) est le point g tel que $\sum_i \lambda_i \overrightarrow{gx_i}$, c'est-à-dire $\sum_i \lambda_i (x_i - g) = 0$ ou encore

$$\sum_i \lambda_i x_i = \sum_i \lambda_i g. \quad (8.70)$$

Donc quitte à diviser tous les λ_i par la somme, nous pouvons supposer que la somme des poids est 1. C'est pourquoi lorsque nous parlerons de barycentre dans un espace vectoriel sans contexte affin, nous allons toujours supposer $\sum_i \lambda_i = 1$ et avoir le barycentre

$$g = \sum_i \lambda_i x_i. \quad (8.71)$$

Proposition 8.38.

Soit E , un espace vectoriel et $A \subset E$. L'enveloppe convexe $\text{Conv}(A)$ est l'ensemble des barycentres de familles finies de points affublés de masses positives.

Démonstration. Nous notons $\mathcal{B}$ l'ensemble des dits barycentres. Par la proposition 8.37, ces barycentres sont dans l'enveloppe convexe et donc $\mathcal{B} \subset \text{Conv}(A)$. A contrario, si nous prouvons que $\mathcal{B}$ était convexe, alors nous aurions $\text{Conv}(A) \subset \mathcal{B}$ parce que l'enveloppe convexe est l'intersection des convexes contenant A .

Soient $a, b \in \mathcal{B}$, c'est-à-dire que l'on a $a_0, \dots, a_n$ et $b_0, \dots, b_m$ dans A ainsi que les nombres strictement positifs $\lambda_0, \dots, \lambda_n$ et $\mu_0, \dots, \mu_m$ tels que

$$a = \sum_i \lambda_i a_i \quad \sum_{i=1}^n \lambda_i = 1 \quad (8.72a)$$

$$b = \sum_j \mu_j b_j \quad \sum_{j=1}^m \mu_j = 1 \quad (8.72b)$$

Un point du segment $[a, b]$ est de la forme $p = ta + (1 - t)b$ avec $t \in [0, 1]$. En développant,

$$p = \sum_{i=0}^n (t\lambda_i) a_i + \sum_{j=0}^m (1 - t)\mu_j b_j. \quad (8.73)$$

Cela est le barycentre de la famille $\{(a_i, \lambda_i), (b_j, \mu_j)\}$, parce que la somme des coefficients est bien 1 :

$$\sum_i (t\lambda_i) + \sum_j (1 - t)\mu_j = t + (1 - t) = 1. \quad (8.74)$$

$\square$

Théorème 8.39 (Carathéodory[79]).

Dans un espace affine de dimension n , l'enveloppe convexe⁶ de A est l'ensemble des barycentres à coefficients positifs ou nuls de familles de $n + 1$ points.

Démonstration. Soit $x \in \text{Conv}(A)$; on sait par la proposition 8.38 que x est barycentre de points de A avec des coefficients positifs :

$$x = \sum_{k=1}^p \lambda_k x_k \quad (8.75)$$

avec $\sum_k \lambda_k = 1$. Nous supposons que $p > n + 1$ (sinon le théorème est réglé), et nous allons faire une récurrence à l'envers en montrant qu'on peut aussi écrire x sous forme d'un barycentre de strictement moins de p points.

Étant donné que $p - 1 > n$, la famille $\{x + i - x_1\}_{i=2,\dots,p}$ est liée et il existe donc $\alpha_1, \dots, \alpha_p \in \mathbb{R}$ tels que $\sum_{i=2}^p \alpha_i (x_i - x_1) = 0$, c'est-à-dire telle que

$$\sum_{i=2}^p \alpha_i x_i = \sum_{i=2}^p \alpha_i x_1. \quad (8.76)$$

Nous posons $\alpha_1 = -\sum_{i=2}^p \alpha_i$. Remarquons qu'alors $\sum_{i=1}^p \alpha_i x_i = 0$ parce que

$$\sum_{i=1}^p \alpha_i x_i = \alpha_1 x_1 + \sum_{i=2}^p \alpha_i x_i = \alpha_1 x_1 + \sum_{i=2}^p \alpha_i x_1 = \sum_{i=1}^p \alpha_i x_1 = 0. \quad (8.77)$$

Par conséquent ça ne coûte rien de récrire (8.75) sous la forme

$$x = \sum_{i=1}^p (\lambda_i + t\alpha_i) x_i. \quad (8.78)$$

Les α_i ne sont pas tous nuls, mais leur somme est nulle, donc il y en a au moins un négatif. Nous notons

$$\tau = \min\left\{-\frac{\lambda_i}{\alpha_i} \text{ tel que } \alpha_i < 0\right\}, \quad (8.79)$$

et J l'ensemble de i pour lesquels ce minimum est atteint. Nous considérons aussi le nombres $\mu_i = \lambda_i + \tau\alpha_i$. Plusieurs remarques.

- (1) Si $j \in J$, alors $\mu_j = 0$
- (2) Si $\alpha_i > 0$ alors $\mu_i \geq 0$, mais si $\alpha_i < 0$ alors

$$\lambda_i + \tau\alpha_i \geq \lambda_i + \left(-\frac{\lambda_i}{\alpha_i}\right)\alpha_i = 0 \quad (8.80)$$

donc $\mu_i \geq 0$ quand même.

- (3) $\sum_{i=1}^p \mu_i = 1$, toujours parce que $\sum_{i=1}^p \alpha_i = 0$.

Avec tout ça, nous avons

$$\sum_{i \notin J} \mu_i x_i = \sum_{i=1}^p \mu_i x_i = x. \quad (8.81)$$

Et voilà, nous avons écrit x comme un barycentre à coefficients positifs de moins de p éléments parce que J n'est pas vide. $\square$

Corolaire 8.40.

Dans un espace affine de dimension finie, l'enveloppe convexe d'un compact est compacte.

6. Définition 8.36.

Démonstration. Soit A une partie compacte de l'espace vectoriel E , et $\text{Conv}(A)$ son enveloppe convexe. Nous allons montrer que toute suite dans $\text{Conv}(A)$ admet une sous-suite convergente en écrivant un point de $\text{Conv}(A)$ comme le théorème de Carathéodory 8.39 nous le suggère. Pour cela nous considérons le simplexe

$$\Lambda = \left\{ \lambda \in \mathbb{R}^{n+1} \text{ tel que } \sum_{k=1}^{n+1} \lambda_k = 1 \text{ et } \lambda_k \geq 0 \forall k \right\}. \quad (8.82)$$

Montrons en passant que Λ est compact. Si $\lambda_k \in \Lambda$ est une suite, alors chacun des λ_k est un $(n+1)$ -uplet de nombres dans $[0, 1]$:

$$k \mapsto (\lambda_k)_i \quad (8.83)$$

est une suite qui possède une sous-suite convergente. En passant $n+1$ fois à une sous-suite, nous tombons sur une suite convergente vers $\lambda \in \Lambda$, grâce à la convergence composante par composante. De plus pour chaque k nous avons $\sum_{i=1}^{n+1} (\lambda_k)_i = 1$, et en passant à la limite, la somme étant une application continue, $\sum_i \lambda_i = 1$.

Considérons l'application

$$\begin{aligned} f: \Lambda \times A^{n+1} &\rightarrow \text{Conv}(A) \\ (\lambda, x) &\mapsto \sum_{k=1}^{n+1} \lambda_k x_k. \end{aligned} \quad (8.84)$$

C'est une application continue parce qu'elle est bilinéaire en dimension finie ; son image est contenue dans $\text{Conv}(A)$ par la proposition 8.37, et elle est surjective par le théorème de Carathéodory 8.39. Bref, $\text{Conv}(A) = f(\Lambda \times A^{n+1})$ est donc l'image d'un compact par une application continue ; elle est donc compacte par le théorème 7.97. $\square$

Notons que sans le théorème de Carathéodory, peut être que le nombre de points utiles pour décomposer les différents a_k n'était pas borné ; dans ce cas nous aurions dû prendre une infinité de sous-suites et rien n'aurait été sûr.

8.7.3 Applications affines et barycentre

Proposition 8.41 ([193]).

Une application $f: \mathcal{E} \rightarrow \mathcal{E}'$ entre deux espaces affines est affine si et seulement si pour tout système $\{(A_i, \lambda_i)\}_{i=1, \dots, k}$ de barycentre G et de poids total non nul, le point $f(G)$ est barycentre du système $\{(f(A_i), \lambda_i)\}$.

Démonstration. En deux parties.

Si f est affine Par définition d'un barycentre,

$$\sum_i \lambda_i \overrightarrow{GA_i} = 0. \quad (8.85)$$

Nous considérons un point arbitraire $O \in \mathcal{E}$ et nous écrivons $A_i = O + x_i$, $G = O + x_g$. Ensuite nous utilisons le lemme 8.11 pour le calcul suivant :

$$\sum_i \lambda_i \overrightarrow{g(G)f(A_i)} = \sum_i \lambda_i u_f(x_i - x_g) \quad (8.86a)$$

$$= u_f\left(\sum_i \lambda_i (x_i - x_g)\right) \quad (8.86b)$$

$$= u_f\left(\sum_i \lambda_i \overrightarrow{GA_i}\right) \quad (8.86c)$$

$$= u_f(0) = 0. \quad (8.86d)$$

Donc $f(G)$ est bien le barycentre du nouveau système.

Si f conserve les barycentres Nous définissons u par $f(O + x) = f(O) + u(x)$. À priori, ce u dépend de O et n'est pas linéaire.

u est linéaire Soient $M, N \in \mathcal{E}$ et les éléments $x_m, x_n \in E$ tels que $\overrightarrow{OM} = x_m$ et $\overrightarrow{ON} = x_n$. Nous définissons enfin P par

$$\overrightarrow{OP} = \alpha \overrightarrow{OM} + \beta \overrightarrow{ON}, \quad (8.87)$$

et $P = O + x_p$. En décomposant $\overrightarrow{MO}$ et $\overrightarrow{NO}$ par les relations de Chasles de la proposition 8.4(1) nous avons

$$(\alpha + \beta - 1)\overrightarrow{PO} - \alpha \overrightarrow{PM} - \beta \overrightarrow{PN} \quad (8.88)$$

et donc P est barycentre du système

$$\{(\alpha + \beta - 1, O), (\alpha, M), (\beta, N)\}. \quad (8.89)$$

Le point $f(P)$ sera barycentre du système

$$\{(\alpha + \beta - 1, f(O)), (\alpha, f(M)), (\beta, f(N))\}. \quad (8.90)$$

Cela signifie que

$$(\alpha + \beta - 1)\overrightarrow{f(P)f(O)} - \alpha \overrightarrow{f(P)f(M)} - \beta \overrightarrow{f(P)f(N)} = 0. \quad (8.91)$$

En y substituant $\overrightarrow{f(P)f(O)} = u(-x_p)$, $\overrightarrow{f(P)f(M)} = u(x_m - x_p)$ et $\overrightarrow{f(P)f(N)} = u(x_n - x_p)$ ainsi que $x_p = \alpha x_m + \beta x_n$ nous trouvons

$$u(\alpha x_m + \beta x_n) = \alpha u(x_m) + \beta u(x_n). \quad (8.92)$$

Donc u est linéaire.

u ne dépend pas du point O Il n'est pas besoin de démontrer cela parce que la définition 8.9 ne le demande pas. Note : c'est le lemme 8.10 qui dit que c'est par ailleurs vrai.

□

8.8 Repères, coordonnées cartésiennes et barycentriques

Définition 8.42.

On dit que les points $A_0, \dots, A_r \in \mathcal{E}$ sont **affinement indépendants** si le sous-espace affine engendré est de dimension r .

Proposition 8.43 ([190]).

Pour $r + 1$ points $A_0, \dots, A_r$ dans $\mathcal{E}$, les propriétés suivantes sont équivalentes.

- (1) Les A_i sont affinement indépendants.
- (2) Pour tout $i = 0, \dots, r$, le point A_i n'est pas dans $\text{Aff}\{A_0, \dots, \hat{A}_i, \dots, A_r\}$.
- (3) Les points $A_0, \dots, A_{r-1}$ sont affinement indépendants et $A_r \notin \text{Aff}\{A_0, \dots, A_{r-1}\}$.
- (4) Il existe i tel que les vecteurs $\overrightarrow{A_k A_i}$ ($k \in i$) sont linéairement indépendants.
- (5) Pour tout $i \in \{1, \dots, r\}$, les vecteurs $\overrightarrow{A_k A_i}$ ($k \neq i$) sont linéairement indépendants.

Notons à propos de la condition (3) que l'existence d'un i tel que $A_i \notin \text{Aff}\{A_0, \dots, \hat{A}_i, \dots, A_r\}$ n'implique pas l'indépendance des $r + 1$ points. En effet dans $\mathbb{R}^2$ nous considérons les 4 points $A_0 = (0, 0)$, $A_1 = (1, 0)$, $A_2 = (2, 0)$ et $A_3 = (0, 1)$. Évidemment le point A_3 n'est pas dans l'espace engendré par les trois autres; il n'empêche que ces points ne sont pas affinement indépendants parce que la direction est de dimension 2 au lieu de 3.

Définition 8.44.

Soit $\mathcal{E}$ un espace affine de dimension n et $\mathcal{F}$ un sous-espace affine de dimension k . Un **repère affine** de $\mathcal{F}$ est la donnée de $k+1$ points affinement indépendants de $\mathcal{F}$.

Si $\{A_0, \dots, A_n\}$ est un repère affine, le point A_0 est l'**origine**. C'est un choix complètement arbitraire ; et c'est bien cet arbitraire qui nous amènera à considérer les coordonnées barycentriques au lieu des coordonnées cartésiennes.

Soit $M \in \mathcal{E}$; par définition nous avons

$$M = A_0 + \overrightarrow{A_0 M}. \quad (8.93)$$

Mais nous savons que les vecteurs $\overrightarrow{A_0 A_i}$ forment une base de E , nous avons donc des nombres λ_i tels que

$$\overrightarrow{A_0 M} = \sum_{i=1}^n \lambda_i \overrightarrow{A_0 A_i}. \quad (8.94)$$

Les nombres λ_i ainsi construits sont les **coordonnées cartésiennes** du point M dans le repère $\{A_0, \dots, A_n\}$ d'origine A_0 .

À partir de ces coordonnées, le point $M \in \mathcal{E}$ se retrouve par la formule

$$M = A_0 + \sum_{i=1}^n \lambda_i \overrightarrow{A_0 A_i}. \quad (8.95)$$

Proposition 8.45 ([1]).

La paire $(O, \{e_1, \dots, e_n\})$ est un repère cartésien de $\mathcal{E}$ si et seulement si $\{O, O + e_1, \dots, O + e_n\}$ est un repère affine.

Démonstration. En deux parties.

Sens direct Vue la proposition 8.43, il suffit de prouver que les vecteurs $\overrightarrow{O(O + e_i)}$ sont linéairement indépendants. Mais $\overrightarrow{O(O + e_i)} = e_i$, donc oui, ils sont linéairement indépendants.

Sens inverse Il s'agit d'utiliser la même proposition 8.43 qui est encore fonctionnelle parce qu'elle est une équivalence.

□

Soient (A, e_i) et (A', e'_i) deux repères cartésiens pour l'espace affine $\mathcal{E}$. Soit (a_{ij}) la matrice de changement de base entre $\{e_i\}$ et $\{e'_i\}$ dans E . Nous voudrions trouver les x_i en termes des x'_i .

Pour cela nous considérons un point M dans $\mathcal{E}$ et nous l'écrivons dans les deux bases. Cela fournit l'égalité

$$A + \sum_i x_i e_i = A' + \sum_i x'_i e'_i. \quad (8.96)$$

Nous considérons les coordonnées (a_i) de A' dans le repère (A, e_i) , c'est-à-dire

$$A' = A + \sum_i a_i e_i. \quad (8.97)$$

En substituant $e'_i = \sum_k a_{jk} e_k$ et (8.97) dans (8.96) nous trouvons

$$\sum_k x_k e_k = \sum_k a_k e_k + \sum_{jk} a_{jk} x'_j e_k, \quad (8.98)$$

et par conséquent

$$x_k = a_k + \sum_j a_{jk} x'_j. \quad (8.99)$$

Les coordonnées barycentriques sont données par la proposition suivante.

Proposition 8.46 ([190]).

Soient $A_0, \dots, A_r$ des points affinement indépendants dans $\mathcal{E}$ et $\mathcal{F} = \text{Aff}\{A_0, \dots, A_r\}$. Tout point $M \in \mathcal{F}$ s'écrit de façon unique comme barycentre⁷ des A_i affectés de poids λ_i tels que $\sum_{i=0}^r \lambda_i = 1$.

Démonstration. Nous avons vu plus haut (définition 8.44) que l'afine indépendance des points A_i assurait que $(A_0, \dots, A_r)$ était un repère de $\mathcal{F}$.

En ce qui concerne l'existence de l'écriture de M comme barycentre, nous savons que les sous-espace affine sont exactement les ensembles de barycentres (proposition 8.33), c'est-à-dire que si on a des points dans un sous-espace affine, alors les barycentres de ces points est encore dans le sous-espace affine.

L'unicité est comme suit. Si M est barycentre des A_i avec poids λ_i , nous écrivons la caractérisation (4) du théorème 8.30 avec $B = A_0$:

$$\overrightarrow{A_0 M} = \sum_{i=1}^r \lambda_i \overrightarrow{A_0 A_i} \quad (8.100)$$

où la somme à droite s'étend à priori de 0 à r , mais comme $\overrightarrow{A_0 A_0} = 0$, nous l'avons limitée à 1. Si M s'écrit comme barycentre de deux façons différentes, nous aurions

$$\overrightarrow{A_0 M} = \sum_{i=1}^r \lambda_i \overrightarrow{A_0 A_i} = \sum_{i=1}^r \mu_i \overrightarrow{A_0 A_i} \quad (8.101)$$

avec $\sum_i \lambda_i = \sum_i \mu_i = 1$. Étant donné que les points $A_0, \dots, A_r$ forment un repère, les vecteurs $\overrightarrow{A_0 A_i}$ sont linéairement indépendants (point (5) de la proposition 8.43) et donc $\lambda_i = \mu_i$ pour $i = 1, \dots, r$. La condition de somme des points égale à 1 impose alors immédiatement $\lambda_0 = \mu_0$. $\square$

Définition 8.47.

Soit un espace affine $\mathcal{E}$ de dimension n . Soient des points affinement indépendants $A_1, \dots, A_n$. Pour $M \in \mathcal{E}$, la proposition 8.46 indique qu'il existe un unique choix de λ_i tel que

$$\left\{ \begin{array}{l} \sum_i \lambda_i = 1 \end{array} \right. \quad (8.102a)$$

$$\left\{ \begin{array}{l} \sum_i \lambda_i \overrightarrow{M A_i} = 0. \end{array} \right. \quad (8.102b)$$

Ces λ_i sont les **coordonnées barycentriques** de M dans le repère $\{A_i\}_{i=1, \dots, n}$.

8.48.

Soit $\mathbb{R}^2$ et les points non alignés A, B, C . Les coordonnées barycentriques (α, β, γ) dans ce système correspondent à l'unique $X \in \mathbb{R}^2$ tel que

$$\alpha \overrightarrow{X A} + \beta \overrightarrow{X B} + \gamma \overrightarrow{X C} = 0. \quad (8.103)$$

Exemple 8.49.

Soient les points $A = (3, 1)$, $B = (-1, 2)$ et $C = (0, -1)$ dans $\mathbb{R}^2$. Nous allons montrer qu'il forment un repère affine de $\mathbb{R}^2$. L'espace engendré par ces trois points est l'espace des

$$A + \alpha \overrightarrow{AB} + \beta \overrightarrow{AC}, \quad (8.104)$$

et la direction correspondante est l'espace vectoriel donné par $\alpha \overrightarrow{AB} + \beta \overrightarrow{AC}$ qui est de dimension deux. Donc l'espace affine engendré par A, B et C est de dimension 2. $\triangle$

Exemple 8.50.

Dans le repère (A, B, C) , quel est le point de coordonnées barycentriques $(\frac{1}{6}, \frac{1}{3}, \frac{1}{2})$? D'abord nous vérifions que

$$\frac{1}{6} + \frac{1}{3} + \frac{1}{2} = 1. \quad (8.105)$$

7. Définition 8.28.

Ensuite nous cherchons $X \in \mathbb{R}^2$ tel que

$$\frac{1}{6}\overrightarrow{AX} + \frac{1}{3}\overrightarrow{BX} + \frac{1}{2}\overrightarrow{CX} = 0, \quad (8.106)$$

c'est-à-dire

$$\frac{1}{6} \begin{pmatrix} x-3 \\ y-1 \end{pmatrix} + \frac{1}{3} \begin{pmatrix} x+1 \\ y-2 \end{pmatrix} + \frac{1}{2} \begin{pmatrix} x \\ y+1 \end{pmatrix} = 0. \quad (8.107)$$

Nous trouvons immédiatement $x = 1/6$ et $y = 1/3$. Le point cherché est donc le point $\begin{pmatrix} 1/6 \\ 1/3 \end{pmatrix}$. $\triangle$

Lemme 8.51 ([1]).

Une application affine $f: \mathcal{E} \rightarrow \mathcal{E}$ qui préserve les points d'une base affine de $\mathcal{E}$ est l'identité.

Démonstration. Une base affine de $\mathcal{E}$ consiste en $n+1$ points $\{A_0, \dots, A_n\}$ affinement indépendants. Nous utilisons la proposition 8.45 pour dire que $(A_0, \{\overrightarrow{A_0A_i}\}_{i=1, \dots, n})$ est un repère cartésien.

En utilisant la formule du lemme 8.10,

$$f(A_i) = f(A_0 + \overrightarrow{A_0A_i}) = f(A_0) + u(\overrightarrow{A_0A_i}). \quad (8.108)$$

Donc $A_i = A_0 + u(\overrightarrow{A_0A_i})$, ce qui signifie que

$$u(\overrightarrow{A_0A_i}) = \overrightarrow{A_0A_i} \quad (8.109)$$

Par ailleurs, tout point M^8 de $\mathcal{E}$ peut être écrit sous la forme

$$M = A_0 + \sum_i \lambda_i \overrightarrow{A_0A_i}. \quad (8.110)$$

En appliquant M , et en utilisant (8.109),

$$f(M) = f(A_0) + \sum_i \lambda_i u(\overrightarrow{A_0A_i}) = A_0 + \sum_i \lambda_i \overrightarrow{A_0A_i} = M. \quad (8.111)$$

Donc tout point de $\mathcal{E}$ est fixé par f , ce qui signifie que f est l'identité. $\square$

8.8.1 Équation de droite

Soit $\mathcal{E}$ un espace affine de dimension trois muni d'un repère barycentrique. Une droite est donnée par trois nombres : $D = D(a, b, c)$ est l'ensemble des points dont les coordonnées barycentriques (normalisées) (x, y, z) vérifient $ax + by + cz = 0$. C'est un espace de dimension un parce qu'il y a aussi la condition $x + y + z = 1$.

La droite $D(1, 1, 1)$ n'existe pas parce que ce serait $x + y + z = 0$, qui est incompatible avec $x + y + z = 1$.

Les droites $D(a, b, c)$ et $D(a', b', c')$ s'intersectent selon les solutions du système

$$\begin{cases} x + y + z = 1 & (8.112a) \\ ax + by + cz = 0 & (8.112b) \\ a'x + b'y + c'z = 0 & (8.112c) \end{cases}$$

Donc deux droites affines ont un unique point d'intersection si et seulement si

$$d = \begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a' & b' & c' \end{vmatrix} \neq 0. \quad (8.113)$$

Elles seront parallèles ou confondues si et seulement si $d = 0$.

8. Même les points qui ne s'appellent pas « M » en fait.

8.8.2 Associativité, coordonnées barycentriques dans un triangle

Lemme 8.52 ([194]).

Soient trois points non alignés A, B, C ainsi que des nombres α, β, γ tels que $\alpha + \beta \neq 0$ et $\alpha + \beta + \gamma \neq 0$.

Soit H le barycentre du système $\{(A, \alpha), (B, \beta)\}$ et G le barycentre de $\{(A, \alpha), (B, \beta), (C, \gamma)\}$.

Alors G est barycentre de $\{(H, \alpha + \beta), (C, \gamma)\}$.

Démonstration. Vues les définitions de H et G nous avons

$$\alpha \overrightarrow{HA} + \beta \overrightarrow{HB} = 0 \quad (8.114a)$$

$$\alpha \overrightarrow{GA} + \beta \overrightarrow{GB} + \gamma \overrightarrow{GC} = 0. \quad (8.114b)$$

En utilisant les relations de Chasles nous introduisons H dans la seconde relation :

$$\alpha(\overrightarrow{GH} + \overrightarrow{HA}) + \beta(\overrightarrow{GH} + \overrightarrow{HB}) + \gamma \overrightarrow{GC} = 0 \quad (8.115a)$$

$$(\alpha + \beta)\overrightarrow{GH} + \underbrace{\alpha \overrightarrow{HA} + \beta \overrightarrow{HB}}_{=0} + \gamma \overrightarrow{GC} = 0 \quad (8.115b)$$

$$(\alpha + \beta)\overrightarrow{GH} + \gamma \overrightarrow{GC} = 0. \quad (8.115c)$$

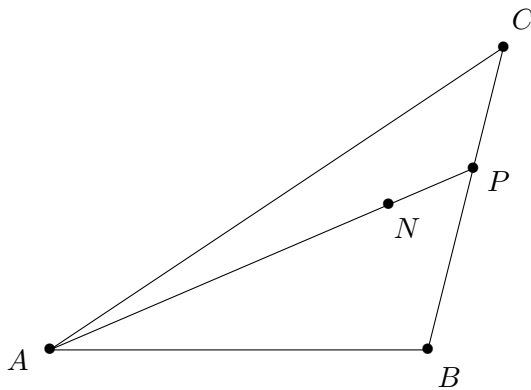
□

Les coordonnées barycentriques dans un triangle (et plus généralement en fait) permettent de faire des projections.

Proposition 8.53.

Soient trois points non alignés A, B, C ainsi qu'un point N de coordonnées barycentriques (α, β, γ) dans le système (A, B, C) . Si P est l'intersection $(AN) \cap (BC)$ alors les coordonnées de P sont $(0, \beta, \gamma)$.

Démonstration. Un dessin de la situation :



Dire que les coordonnées de N sont (α, β, γ) signifie que

$$\alpha \overrightarrow{NA} + \beta \overrightarrow{NB} + \gamma \overrightarrow{NC} = 0. \quad (8.116)$$

Nous voudrions montrer que le point P est bien le point de coordonnées $(0, \beta, \gamma)$. Soit donc le point P tel que

$$\beta \overrightarrow{PB} + \gamma \overrightarrow{PC} = 0 \quad (8.117)$$

et montrons que ce point est l'intersection $(BC) \cap (NA)$.

D'abord la relation (8.117) nous dit immédiatement que P est sur la droite (BC) . Ensuite, en utilisant les relations de Chasles pour introduire N :

$$\beta(\overrightarrow{PN} + \overrightarrow{NB}) + \gamma(\overrightarrow{PN} + \overrightarrow{NC}) = 0. \quad (8.118)$$

Nous remplaçons $\beta\overrightarrow{NB} + \gamma\overrightarrow{NC}$ par $-\alpha\overrightarrow{NA}$ pour obtenir :

$$(\beta + \gamma)\overrightarrow{PN} - \alpha\overrightarrow{NA} = 0. \quad (8.119)$$

Cela montre que les vecteurs $\overrightarrow{PN}$ et $\overrightarrow{NA}$ sont colinéaires, et donc que P , N et A sont alignés. $\square$

8.9 Applications affines sur $\mathbb{R}^n$

Soit $v \in \mathbb{R}^n$; nous notons $\tau_v : \mathbb{R}^n \rightarrow \mathbb{R}^n$ la translation donnée par $\tau_v(x) = x + v$. Le groupe de toutes les translations de $\mathbb{R}^n$ est noté $T(n)$ et est isomorphe au groupe abélien $(\mathbb{R}^n, +)$.

Nous avons déjà discuté de la structure d'un espace vectoriel (en particulier $\mathbb{R}^n$) comme espace affine en 8.5.

Lemme 8.54.

Décomposition d'une application affine.

- (1) Une application $f : E \rightarrow E$ est affine si et seulement si il existe $v \in E$ et une application linéaire α sur E telle que $f = \tau_v \circ \alpha$.
- (2) Dans ce cas, le choix de (v, α) est unique.
- (3) Si f est bijective, alors α est bijective.

Démonstration. Nous supposons d'abord que f est affine. Alors il existe une application linéaire u_f sur E telle que

$$f(M + x) = f(M) + u_f(x) = (\tau_{f(M)} + u_f)(x) \quad (8.120)$$

pour tout x et M . De plus l'application u_f ne dépend ni de M ni de x (c'est la proposition 8.13(1)). En posant $M = 0$ nous avons :

$$f(x) = (\tau_{f(0)} \circ u_f)(x). \quad (8.121)$$

Dans l'autre sens nous supposons avoir $v \in E$ et α linéaire sur E telles que

$$f(M) = (\tau_v \circ \alpha)(M). \quad (8.122)$$

Notons qu'il y a un abus de notation entre α qui est linéaire sur l'espace *vectoriel* E et l'application α qui est une application sur l'espace *affine* E . Cet abus est légitime parce que les deux espaces sont identiques en tant qu'ensembles. Ce qui est vraiment abuser par contre, c'est de se poser ce genre de questions.

Nous avons :

$$\begin{aligned} f(M + x) &= \tau_v(\alpha(M + x)) = \alpha(M + x) + v = \alpha(M) + v + \alpha(x) \\ &= (\tau_v \circ \alpha)(M) + \alpha(x) = f(M) + \alpha(x). \end{aligned} \quad (8.123)$$

Donc la fonction f vérifie la définition 8.9. La partie (1) est prouvée.

Pour prouver l'unicité de la partie (2), nous supposons que $\tau_v \circ \alpha = \tau_w \circ \alpha$. En appliquant cela à 0 nous trouvons $v = w$. Nous avons donc $\tau_v \circ \alpha = \tau_v \circ \beta$. Comme τ_v est inversible, nous en déduisons $\alpha = \beta$.

Enfin le point (3) est relativement évident du fait que τ_v , elle, est sûrement bijective. $\square$

Corolaire 8.55.

Une application affine qui conserve l'origine est linéaire.

Démonstration. Conserver l'origine demande de poser $v = 0$ dans l'expression du lemme 8.54. $\square$

Proposition 8.56.

Soit une application affine $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$. L'ensemble des points fixes

$$\text{Fix}(f) = \{x \in \mathbb{R}^n \text{ tel que } f(x) = x\} \quad (8.124)$$

est soit vide soit un sous-espace affine de $\mathbb{R}^n$.

Démonstration. Soit $f = \tau_v \circ \alpha$; nous avons $x \in \text{Fix}(f)$ si et seulement si

$$x = \tau_v(\alpha(x)) = \alpha(x) + v, \quad (8.125)$$

autrement dit, en considérant l'application linéaire $\beta = \text{Id} - \alpha$, si et seulement si $\beta(x) = v$. Nous écrivons $\text{Fix}(f) = \beta^{-1}(v)$. Supposons que ce soit non vide et considérons $x_0 \in \beta^{-1}(v)$. Nous avons

$$\beta^{-1}(v) = \{x \in \mathbb{R}^n \text{ tel que } \beta(x) = \beta(x_0)\} \quad (8.126a)$$

$$= \{x \text{ tel que } \beta(x - x_0) = 0\} \quad (8.126b)$$

$$= \{x \text{ tel que } x - x_0 \in \ker(\beta)\} \quad (8.126c)$$

$$= \ker(\beta) + x_0 \quad (8.126d)$$

$$= \tau_{x_0}(\ker(\beta)). \quad (8.126e)$$

Mais comme $\ker(\beta)$ est un sous-espace vectoriel, $\beta^{-1}(v)$ est le translaté d'un sous-espace vectoriel, c'est-à-dire un sous-espace affine. $\square$

8.9.1 Structure de groupe pour les applications affines

Proposition-Définition 8.57 ([1]).

L'ensemble des applications affines bijectives de $\mathbb{R}^n$ forment un groupe pour la composition. Les lois de groupe sont données par les formules suivantes :

(1) *Le neutre est l'identité.*

(2) *Le produit est donné par*

$$(\tau_v \circ \alpha)(\tau_w \circ \beta) = \tau_{\alpha(w)+v} \circ \alpha\beta. \quad (8.127)$$

(3) *L'inverse est donné par*

$$(\tau_v \circ \alpha)^{-1} = \tau_{-\alpha^{-1}(v)} \circ \alpha^{-1}. \quad (8.128)$$

Ce groupe est noté $\text{Aff}(\mathbb{R}^n)$.

Démonstration. Pour l'identité, oui, composer par l'identité est neutre.

Le fait que la formule (8.127) soit vraie est un simple calcul :

$$(\tau_v \circ \alpha) \circ (\tau_w \circ \beta)(x) = (\alpha\beta)(x) + \alpha(w) + v = (\tau_{\alpha(w)+v} \circ \alpha\beta)x. \quad (8.129)$$

Le fait que la formule (8.127) donne bien un produit pour tous les éléments de $\text{Aff}(\mathbb{R}^n)$ est le lemme 8.54.

En ce qui concerne l'inverse, c'est un calcul :

$$(\tau_{-\alpha^{-1}(v)} \circ \alpha^{-1})(\tau_v \circ \alpha)(x) = (\tau_{-\alpha^{-1}(v)} \circ \alpha^{-1})(\alpha(x) + v) \quad (8.130a)$$

$$= \tau_{-\alpha^{-1}(v)}(x + \alpha^{-1}(v)) \quad (8.130b)$$

$$= x. \quad (8.130c)$$

$\square$

Si $f: \mathbb{R}^n \rightarrow \mathbb{R}^n$ est une application affine, la proposition 8.54 affirme qu'il existe une application linéaire u telle que

$$f(x + y) = f(x) + u(y). \quad (8.131)$$

En écrivant cela pour $x = 0$,

$$f(y) = f(0) + u(y), \quad (8.132)$$

ou encore $f = \tau_{f(0)} \circ u$.

Proposition 8.58.

L'ensemble $\text{Aff}(\mathbb{R}^n)$ est isomorphe au produit semi-direct⁹

$$\text{Aff}(\mathbb{R}^n) \simeq T(n) \times_{\mathbf{Ad}} \text{GL}(n, \mathbb{R}) \quad (8.133)$$

où $\mathbf{Ad}$ est l'action adjointe, c'est-à-dire

$$\begin{aligned} \mathbf{Ad}: \text{GL}(n, \mathbb{R}) &\rightarrow \text{Aut}(T(n)) \\ \alpha &\mapsto (\tau_v \mapsto \alpha \circ \tau_v \circ \alpha^{-1}). \end{aligned} \quad (8.134)$$

Démonstration. L'application que nous allons montrer être un isomorphisme est ψ qui à $f = \tau_v \circ \alpha$ fait correspondre le couple $(\tau_v, \alpha) \in T(n) \times \text{GL}(n, \mathbb{R})$.

Égalité d'ensembles Il faut que $\text{Aff}(\mathbb{R}^n)$ soit en bijection avec $T(n) \times \text{GL}(n, \mathbb{R})$. En effet si $f \in \text{Aff}(\mathbb{R}^n)$, la décomposition $f = \tau_v \circ \alpha$ est unique. D'abord en appliquant à 0, $f(0) = \tau_v(\alpha(v)) = v$. Donc v est fixé par la valeur de $f(0)$. Ensuite $\alpha = f \circ \tau_v^{-1}$, donc α fixé.

L'action adjointe fonctionne Il faut vérifier que $\alpha \circ \tau_v \circ \alpha^{-1}$ est bien dans $T(n)$. Pour cela, en agissant sur $x \in \mathbb{R}^n$ nous trouvons

$$\alpha \tau_v \alpha^{-1}(x) = \alpha(\alpha^{-1}(x) + v) = x + \alpha(v) = \tau_{\alpha(v)}(x). \quad (8.135)$$

Le fait que $\mathbf{Ad}(\alpha)$ soit un automorphisme est toujours correct.

Morphisme Il faut vérifier que l'application ψ est un morphisme de groupe. D'abord la loi de groupe sur $\text{Aff}(\mathbb{R}^n)$ est donnée par

$$(\tau_v \circ \alpha) \circ (\tau_w \circ \beta) = \tau_{v+\alpha(w)} \circ (\alpha \circ \beta). \quad (8.136)$$

Ensuite le loi de groupe de le produit semi-direct est donnée par

$$(\tau_v, \alpha) \cdot (\tau_w, \beta) = (\tau_v \mathbf{Ad}(\alpha) \tau_w, \alpha \beta) = (\tau_v \tau_{\alpha(w)}, \alpha \beta) = (\tau_{\alpha(w)+v}, \alpha \beta). \quad (8.137)$$

Nous avons donc bien

$$\psi((\tau_v, \beta) \cdot (\tau_w, \beta)) = \psi(\tau_v, \beta) \circ \psi(\tau_w, \beta). \quad (8.138)$$

□

8.10 Isométries

Définition 8.59 (Isométrie d'espace affine).

Si $\mathcal{E}$ est un espace affine muni d'une distance d , une isométrie de $\mathcal{E}$ est une application $f: \mathcal{E} \rightarrow \mathcal{E}$ préservant d .

Notons que toutes les applications affines ne sont pas des isométries : par exemple les homothéties.

Proposition 8.60.

Si $\mathcal{E}$ est modelé sur un espace euclidien $(E, \|\cdot\|)$ alors la formule

$$d(A, B) = \|\overrightarrow{AB}\| \quad (8.139)$$

définit une distance sur $\mathcal{E}$.

Démonstration. Étant donné la proposition 8.3, la formule a un sens parce qu'à A et B donnés dans $\mathcal{E}$, il est associé un unique vecteur $\overrightarrow{AB} \in E$. □

Nous parlons d'isométries affines ou linéaires dans le thème 69.

9. Définition 2.64.

Chapitre 9

Espaces vectoriels (encore)

9.1 Déterminants

9.1.1 Formes multilinéaires alternées

Définition 9.1.

Soit E , un $\mathbb{K}$ -espace vectoriel. Une forme linéaire **alternée** sur E est une application linéaire $f: E \rightarrow \mathbb{K}$ telle que $f(v_1, \dots, v_k) = 0$ dès que $v_i = v_j$ pour certains $i \neq j$.

Lemme 9.2.

Une forme linéaire alternée est antisymétrique. Si $\mathbb{K}$ est de caractéristique différente de 2, alors une forme antisymétrique est alternée.

Démonstration. Soit f une forme alternée; quitte à fixer toutes les autres variables, nous pouvons travailler avec une 2-forme et simplement montrer que $f(x, y) = -f(y, x)$. Pour ce faire nous écrivons

$$0 = f(x + y, x + y) = f(x, x) + f(x, y) + f(y, x) + f(y, y) = f(x, y) + f(y, x). \quad (9.1)$$

Pour la réciproque, si f est antisymétrique, alors $f(x, x) = -f(x, x)$. Cela montre que $f(x, x) = 0$ lorsque $\mathbb{K}$ est de caractéristique différente de deux. $\square$

Proposition 9.3 ([195]).

Soit E , un $\mathbb{K}$ -espace vectoriel de dimension n , où la caractéristique de $\mathbb{K}$ n'est pas deux. L'espace des n -formes multilinéaires alternées sur E est de $\mathbb{K}$ -dimension 1.

Démonstration. Soient $\{e_i\}$, une base de E , une n -forme linéaire alternée $f: E \rightarrow \mathbb{K}$ ainsi que des vecteurs $(v_1, \dots, v_n)$ de E . Nous pouvons les écrire dans la base

$$v_j = \sum_{i=1}^n \alpha_{ij} e_i \quad (9.2)$$

et alors exprimer f par

$$f(v_1, \dots, v_n) = f\left(\sum_{i_1=1}^n \alpha_{1i_1} e_{i_1}, \dots, \sum_{i_n=1}^n \alpha_{ni_n} e_{i_n}\right) \quad (9.3a)$$

$$= \sum_{i,j} \alpha_{1i_1} \dots \alpha_{ni_n} f(e_{i_1}, \dots, e_{i_n}). \quad (9.3b)$$

Étant donné que f est alternée, les seuls termes de la somme sont ceux dont les i_k sont tous différents, c'est-à-dire ceux où $\{i_1, \dots, i_n\} = \{1, \dots, n\}$. Il y a donc un terme par élément du groupe des permutations S_n et

$$f(v_1, \dots, v_n) = \sum_{\sigma \in S_n} \alpha_{\sigma(1)1} \dots \alpha_{\sigma(n)n} f(e_{\sigma(1)}, \dots, e_{\sigma(n)}). \quad (9.4)$$

En utilisant encore une fois le fait que la forme f soit alternée, $f = f(e_1, \dots, e_n)\Pi$ où

$$\Pi(v_1, \dots, v_n) = \sum_{\sigma \in S_n} \epsilon(\sigma) \alpha_{\sigma(1)1} \dots \alpha_{\sigma(n)n}. \quad (9.5)$$

Pour rappel, la donnée des v_i est dans les nombres α_{ij} .

L'espace des n -formes alternées est donc *au plus* de dimension 1. Pour montrer qu'il est exactement de dimension 1, il faut et suffit de prouver que Π est alternée. Par le lemme 9.2, il suffit de prouver que cette forme est antisymétrique¹.

Soient donc $v_1, \dots, v_n$ tels que $v_i = v_j$. En posant $\tau = (1i)$ et $\tau' = (2j)$ et en sommant sur $\sigma\tau\tau'$ au lieu de σ , nous pouvons supposer que $i = 1$ et $j = 2$. Montrons que $\Pi(v, v, v_3, \dots, v_n) = 0$ en tenant compte que $\alpha_{i1} = \alpha_{i2}$:

$$\Pi(v, v, v_3, \dots, v_n) = \sum_{\sigma \in S_n} \epsilon(\sigma) \alpha_{\sigma(1)1} \alpha_{\sigma(2)2} \alpha_{\sigma(3)3} \dots \alpha_{\sigma(n)n} \quad (9.6a)$$

$$= \sum_{\sigma \in S_n} \epsilon(\sigma\tau) \alpha_{\sigma\tau(1)1} \alpha_{\sigma\tau(2)2} \alpha_{\sigma\tau(3)3} \dots \alpha_{\sigma\tau(n)n} \quad \text{où } \tau = (12) \quad (9.6b)$$

$$= - \sum_{\sigma \in S_n} \epsilon(\sigma) \alpha_{\sigma(1)1} \alpha_{\sigma(2)2} \alpha_{\sigma(3)3} \dots \alpha_{\sigma(n)n} \quad (9.6c)$$

$$= -\Pi(v, v, v_3, \dots, v_n). \quad (9.6d)$$

□

9.1.2 Déterminant d'une famille de vecteurs

Nous considérons un corps $\mathbb{K}$ et l'espace vectoriel E de dimension n sur $\mathbb{K}$.

Définition 9.4 (Déterminant d'une famille de vecteurs[7]).

Le **déterminant** de la famille de vecteurs $(v_1, \dots, v_n)$ dans la base B est l'élément de $\mathbb{K}$

$$\det_{(e_1, \dots, e_n)}(v_1, \dots, v_n) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^n e_{\sigma(i)}^*(v_i) \quad (9.7)$$

où

- la somme porte sur le groupe symétrique,
- le nombre $\epsilon(\sigma)$ est la signature de la permutation σ ,
- les éléments $\{e_i\}$ forment la base canonique de $\mathbb{K}^n$.
- les éléments $\{e_i^*\}$ sont la base duale de $\{e_i\}$.

Nous le notons $\det_{(e_1, \dots, e_n)}(v_1, \dots, v_n)$.

9.5.

La base $\{e_i\}$ est la base canonique de $\mathbb{K}^n$, et l'élément e_k^* est la forme linéaire définie par

$$\begin{aligned} e_k^* : \mathbb{K}^n &\rightarrow \mathbb{K} \\ \sum_i x_i e_i &\mapsto x_k. \end{aligned} \quad (9.8)$$

Il n'est pas sous-entendu que $\mathbb{K}^n$ ait un produit scalaire. Il n'est donc pas autorisé de dire que $\{e_i\}$ est une base orthonormée et que $e_k^*(x) = \langle e_k, x \rangle$. Ce genre d'égalités sont vraies dans le cas $\mathbb{K} = \mathbb{R}$, mais n'ont pas de sens en général.

Le lemme 11.4 va un peu parler du cas où $\mathbb{K}^n$ est muni d'une base orthonormée.

Lemme 9.6 ([7]).

Les propriétés du déterminant. Soit B une base de E .

1. C'est ici que joue l'hypothèse sur la caractéristique de $\mathbb{K}$.

- (1) L'application $\det_B: E^n \rightarrow \mathbb{K}$ est n -linéaire.
 (2) L'application $\det_B: E^n \rightarrow \mathbb{K}$ est n -linéaire est antisymétrique et alternée².
 (3) Pour toute base, $\det_B(B) = 1$.
 (4) Le déterminant ne change pas si on remplace un vecteur par une combinaison linéaire des autres :

$$\det_B(v_1, \dots, v_n) = \det_B\left(v_1 + \sum_{s=2}^n a_s v_s, v_2, \dots, v_n\right). \quad (9.9)$$

- (5) Si on permute les vecteurs,

$$\det_B(v_1, \dots, v_n) = \epsilon(\sigma) \det_B(v_{\sigma(1)}, \dots, v_{\sigma(n)}). \quad (9.10)$$

- (6) Si B' est une autre base :

$$\det_B = \det_B(B') \det_{B'} \quad (9.11)$$

- (7) Nous avons aussi la formule $\det_B(B') \det_{B'}(B) = 1$.

- (8) Les vecteurs $\{v_1, \dots, v_n\}$ forment une base si et seulement si $\det_B(v_1, \dots, v_n) \neq 0$.

Démonstration. Point par point.

- (1)** En posant $v_1 = x_1 + \lambda x_2$ nous avons

$$\det_B(x_1 + \lambda x_2, v_2, \dots, v_n) = \sum_{\sigma} \epsilon(\sigma) \prod_{i=1}^n e_{\sigma(i)}^*(v_i) \quad (9.12a)$$

$$= \sum_{\sigma} \epsilon(\sigma) \left(e_{\sigma(1)}^*(x_1 + \lambda x_2) \right) \prod_{i=2}^n e_{\sigma(i)}^*(v_i). \quad (9.12b)$$

À partir de là, la linéarité de $e_{\sigma(1)}^*$ montre que $\det_B$ est linéaire en son premier argument. Pour les autres arguments, le même calcul tient.

- (2)** Nous prouvons à présent que $\det$ est alternée. Si votre corps est de caractéristique différente de deux, vous pouvez lire la proposition 9.7.

Supposons $v_k = v_l$, et considérons la permutation $\beta = (k, l)$. Nous savons par la proposition 5.32 que $S_n = A_n \cup A_n \beta$. Cela nous permet de décomposer la somme sur S_n en deux parties :

$$\sum_{\sigma \in S_n} (-1)^{\sigma} \prod_i \epsilon_{\sigma(i)}^*(v_i) = \sum_{\sigma \in A_n} (-1)^{\sigma} \prod_i \epsilon_{\sigma(i)}^*(v_i) + \sum_{\sigma \in A_n} (-1)^{\sigma \beta} \prod_i \epsilon_{(\sigma \beta)(i)}^*(v_i). \quad (9.13)$$

D'abord $(-1)^{\sigma} = 1$ et $(-1)^{\sigma \beta} = -1$. Ensuite, pour un $\sigma \in A_n$ donné, nous avons

$$\prod_i \epsilon_{(\sigma \beta)(i)}^*(v_i) = \epsilon_{(\sigma \beta)(k)}^*(v_k) \epsilon_{(\sigma \beta)(l)}^*(v_l) \prod_{i \neq k, l} \epsilon_{(\sigma \beta)(i)}^*(v_i) \quad (9.14a)$$

$$= \epsilon_{\sigma(l)}^*(v_k) \epsilon_{\sigma(k)}^*(v_l) \prod_{i \neq k, l} \epsilon_{\sigma(i)}^*(v_i) \quad (9.14b)$$

$$= \epsilon_{\sigma(l)}^*(v_l) \epsilon_{\sigma(k)}^*(v_k) \prod_{i \neq k, l} \epsilon_{\sigma(i)}^*(v_i) \quad (9.14c)$$

$$= \prod_i \epsilon_{\sigma(i)}^*(v_i). \quad (9.14d)$$

Donc les deux termes de la somme (9.13) ne diffèrent que par un signe. Elle est donc nulle, et la forme déterminant est alternée.

La fonction $\det$ est antisymétrique parce que alternée, voir le lemme 9.2.

2. Alternée, définition 9.1. En caractéristique 2, alternée n'est pas équivalent à symétrique.

(3) Nous avons

$$\det_B(B) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^n \underbrace{e_{\sigma(i)}^*(e_i)}_{=\delta_{\sigma(i),i}}. \quad (9.15)$$

Si σ n'est pas l'identité, le produit contient forcément un facteur nul. Il ne reste de la somme que $\sigma = \text{Id}$ et le résultat est 1.

(4) Vu que $\det_B$ est linéaire en tous ses arguments,

$$\det_B(v_1 + \sum_{s=2}^n a_s v_s, v_2, \dots, v_n) = \det_B(v_1, \dots, v_n) + \sum_{s=2}^n a_s \det_B(v_s, v_2, \dots, v_n). \quad (9.16)$$

Chacun des termes de la somme est nul parce qu'il y a répétition de v_s parmi les arguments alors que la forme est alternée.

(5) Nous devons calculer $\det_B(v_{\sigma(1)}, \dots, v_{\sigma(n)})$, et pour y voir plus clair nous posons $w_i = v_{\sigma(i)}$. Alors :

$$\det_B(v_{\sigma(1)}, \dots, v_{\sigma(n)}) = \sum_{\sigma'} \epsilon(\sigma') \prod_{i=1}^n e_{\sigma'(i)}^*(w_i) \quad (9.17a)$$

$$= \sum_{\sigma'} \epsilon(\sigma') \prod_{i=1}^n e_{\sigma'(i)}^*(v_{\sigma(i)}) \quad (9.17b)$$

$$= \sum_{\sigma'} \epsilon(\sigma') \prod_{i=1}^n e_{\sigma^{-1}\sigma'(i)}^*(v_i) \quad (9.17c)$$

$$= \sum_{\sigma'} \epsilon(\sigma\sigma') \prod_{i=1}^n e_{\sigma'(i)}^*(v_i) \quad (9.17d)$$

$$= \epsilon(\sigma) \det_B(v_1, \dots, v_n). \quad (9.17e)$$

Justifications : nous avons d'abord modifié l'ordre des éléments du produit et ensuite l'ordre des éléments de la somme. Nous avons ensuite utilisé le fait que $\epsilon: S_n \rightarrow \{0, 1\}$ était un morphisme de groupe (proposition 1.159).

(6) Étant donné que l'espace des formes multilinéaires alternées est de dimension 1, il existe un $\lambda \in \mathbb{K}$ tel que $\det_B = \lambda \det_{B'}$. Appliquons cela à B' :

$$\det_B(B') = \lambda \det_{B'}(B'), \quad (9.18)$$

donc $\lambda = \det_B(B')$.

(7) Il suffit d'appliquer l'égalité précédente à B en nous souvenant que $\det_B(B) = 1$.

(8) Si $B' = \{v_1, \dots, v_n\}$ est une base alors $\det_B(B') \neq 0$, sinon il n'est pas possible d'avoir $\det_B(B') \det_{B'}(B) = 1$.

À l'inverse, si B' n'est pas une base, c'est que $\{v_1, \dots, v_n\}$ est liée par la proposition 4.16. Il y a donc moyen de remplacer un des vecteurs par une combinaison linéaire des autres. Le déterminant s'annule alors.

□

Proposition 9.7.

Si la caractéristique du corps de base n'est pas deux, le déterminant est antisymétrique et alterné.

Démonstration. Si la caractéristique du corps de base n'est pas deux, une forme antisymétrique est alternée (lemme 9.2).

Pour prouver que le déterminant est antisymétrique, remarquez que permuter v_k et v_l revient à calculer le nombre $\det_B(v_{\sigma_{kl}(1)}, \dots, v_{\sigma_{kl}(n)})$ au lieu de $\det_B(v_1, \dots, v_n)$. Cela revient à changer la somme $\sum_{\sigma}$ en $\sum_{\sigma \circ \sigma_{kl}}$. Cela ajoute 1 à $\epsilon(\sigma)$ vu que l'on ajoute une permutation.

Donc le déterminant est antisymétrique. Nous en déduisons qu'il est alterné parce que, en permutant trivialement v_1 et v_1 , nous obtenons $\det_B(v_1, v_1) = -\det_B(v_1, v_1)$. Si le corps est de caractéristique différente de deux, cela implique que $\det_B(v_1, v_1) = 0$.

□

D'après la proposition 9.3, il existe une unique forme n -linéaire alternée égale à 1 sur B , et c'est $\det_B: E^n \rightarrow \mathbb{K}$.

9.1.3 Déterminant d'un endomorphisme

L'interprétation géométrique du déterminant en termes d'aires et de volumes est donnée après la théorème 14.259.

Lemme-Définition 9.8.

Si $f: E \rightarrow E$ est un endomorphisme, et si les parties B et B' sont deux bases, alors

$$\det_B(f(B)) = \det_{B'}(f(B')). \quad (9.19)$$

Ce nombre, indépendant de la base choisie est nommé le **déterminant** de f et est noté $\det(f)$.

Démonstration. L'application

$$\begin{aligned} \varphi: E^n &\rightarrow \mathbb{K} \\ v_1, \dots, v_n &\mapsto \det_B(f(v_1), \dots, f(v_n)) \end{aligned} \quad (9.20)$$

est n -linéaire et alternée; il existe donc $\lambda \in \mathbb{K}$ tel que $\varphi = \lambda \det_B$. En appliquant cela à B :

$$\det_B(f(B)) = \lambda \det_B(B) = \lambda. \quad (9.21)$$

Nous avons donc déjà prouvé que $\lambda = \det_B(f(B))$, c'est-à-dire

$$\det_B(f(v)) = \det_B(f(B)) \det_B(v). \quad (9.22)$$

Nous allons maintenant introduire B' là où il y a du v en utilisant les formules (9.11):

$$\det_B(f(v)) = \det_B(B') \det_{B'}(f(v)) \quad (9.23a)$$

$$\det_B(v) = \det_B(B') \det_{B'}(v). \quad (9.23b)$$

Nous obtenons

$$\det_{B'}(f(v)) = \det_B(f(B)) \det_{B'}(v). \quad (9.24)$$

Et on applique cela à $v = B'$:

$$\det_{B'}(f(B')) = \det_B(f(B)) \underbrace{\det_{B'}(B')}_{=1}. \quad (9.25)$$

□

Proposition 9.9.

Principales propriétés géométriques du déterminant d'un endomorphisme.

- (1) Si f et g sont des endomorphismes, alors $\det(f \circ g) = \det(f) \det(g)$.
- (2) L'endomorphisme f est un automorphisme³ si et seulement si $\det(f) \neq 0$.
- (3) Si $\det(f) \neq 0$ alors $\det(f^{-1}) = \det(f)^{-1}$.
- (4) L'application $\det: \text{GL}(E) \rightarrow \mathbb{K} \setminus \{0\}$ est un morphisme de groupe.

Démonstration. Point par point.

- (1) Nous considérons l'application

$$\begin{aligned} \varphi: E^n &\rightarrow \mathbb{K} \\ v &\mapsto \det_B(f(v)). \end{aligned} \quad (9.26)$$

3. Endomorphisme inversible, définition 4.32.

Comme d'habitude nous avons $\varphi(v) = \lambda \det_B(v)$. En appliquant à B et en nous souvenant que $\det_B(B) = 1$ nous avons $\det_B(f(B)) = \lambda$. Autrement dit :

$$\lambda = \det(f). \quad (9.27)$$

Calculons à présent $\varphi(g(B))$: d'une part,

$$\varphi(g(B)) = \det_B((f \circ g)(B)) \quad (9.28)$$

et d'autre part,

$$\varphi(g(B)) = \lambda \det_B(g(B)) = \lambda \det(g) \quad (9.29)$$

En égalisant et en reprenant la la valeur déjà trouvée de λ ,

$$\det(f \circ g)(B) = \det(f) \det(g), \quad (9.30)$$

ce qu'il fallait.

- (2) Supposons que f soit un automorphisme. Alors si B est une base, $f(B)$ est une base. Par conséquent $\det(f) = \det_B(f(B)) \neq 0$ parce que $f(B)$ est une base (lemme 9.6(8)).

Réciproquement, supposons que $\det(f) \neq 0$. Alors si B est une base quelconque nous avons $\det_B(f(B)) \neq 0$, ce qui est uniquement possible lorsque $f(B)$ est une base. L'application f transforme donc toute base en une base et est alors un automorphisme d'espace vectoriel.

- (3) Vu que le déterminant de l'identité est 1 et que f est inversible, $1 = \det(f \circ f^{-1}) = \det(f) \det(f^{-1})$.

□

Proposition 9.10.

Soient deux espaces vectoriels E et F de dimension finies n et m sur le corps $\mathbb{K}$ munis de bases $\{e_i\}$ et $\{f_\alpha\}$. À une matrice $A \in \mathbb{M}(m \times n, \mathbb{K})$ nous associons l'application linéaire⁴

$$f_A(x) = \sum_{i\alpha} A_{\alpha i} x_i f_\alpha. \quad (9.31)$$

Alors, en ce qui concerne les déterminants⁵, nous avons

$$(1) \det(f_A) = \det(A)$$

$$(2) \det(f_{AB}) = \det(f_A) \det(f_B)$$

Démonstration. Nous devons étudier la formule

$$\det(f_A) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^n e_{\sigma(i)}^*(f_A(e_i)). \quad (9.32)$$

En premier lieu nous avons

$$f_A(e_i) = \sum_{jk} A_{jk}(e_i)_k e_j = \sum_j A_{ji} e_j. \quad (9.33)$$

Nous avons alors

$$e_{\sigma(i)}^*(f_A(e_i)) = \sum_j A_{ji} \underbrace{e_{\sigma(i)}^*(e_j)}_{\delta_{j\sigma(i)}} = A_{\sigma(i)i}. \quad (9.34)$$

Au final,

$$\det(f_A) = \sum_{\sigma} \epsilon(\sigma) \prod_{i=1}^n A_{\sigma(i)i} = \det(A^t) = \det(A) \quad (9.35)$$

où la dernière égalité est autorisée par le lemme 4.74.

Cela prouve la formule $\det(f_A) = \det(A)$.

En ce qui concerne la seconde formule, il s'agit de se souvenir de la proposition 4.68 qui donne $f_{AB} = f_A \circ f_B$, et ensuite de la proposition 9.9(1) qui donne $\det(f_A \circ f_B) = \det(f_A) \det(f_B)$. □

4. Dont nous avons déjà beaucoup parlé entre autres dans la proposition 4.68.

5. Définition 9.8 pour les applications linéaires et 4.72 pour les matrices.

9.1.4 Déterminant de Vandermonde

Proposition 9.11 ([90]).

Le *déterminant de Vandermonde* est le polynôme en n variables donné par

$$V(T_1, \dots, T_n) = \det \begin{pmatrix} 1 & 1 & \dots & 1 \\ T_1 & T_2 & \dots & T_n \\ \vdots & \ddots & \ddots & \vdots \\ T_1^{n-1} & T_2^{n-1} & \dots & T_n^{n-1} \end{pmatrix} = \prod_{1 \leq i < j \leq n} (T_j - T_i). \quad (9.36)$$

Notez que l'inégalité du milieu est stricte (sinon d'ailleurs l'expression serait nulle).

Démonstration. Nous considérons le polynôme

$$f(X) = V(T_1, \dots, T_{n-1}, X) \in (\mathbb{K}[T_1, \dots, T_{n-1}])[X]. \quad (9.37)$$

C'est un polynôme de degré au plus $n-1$ en X et il s'annule aux points $T_1, \dots, T_{n-1}$. Par conséquent⁶ nous pouvons factoriser les $X - T_i$, c'est à dire qu'il existe $\alpha \in \mathbb{K}[T_1, \dots, T_{n-1}]$ tel que

$$f = \alpha \prod_{i=1}^{n-1} (X - T_i). \quad (9.38)$$

Nous trouvons α en écrivant $f(0)$. D'une part la formule (9.38) nous donne

$$f(0) = \alpha(-1)^{n-1} T_1 \dots T_{n-1}. \quad (9.39)$$

D'autre par la définition donne

$$f(0) = \det \begin{pmatrix} 1 & \dots & 1 & 1 \\ T_1 & & T_{n-1} & 0 \\ \vdots & & \vdots & \vdots \\ T_1^{n-1} & \dots & T_{n-1}^{n-1} & 0 \end{pmatrix} \quad (9.40a)$$

$$= (-1)^{n-1} \det \begin{pmatrix} T_1 & \dots & T_{n-1} \\ \vdots & \ddots & \vdots \\ T_1^{n-1} & \dots & T_{n-1}^{n-1} \end{pmatrix} \quad (9.40b)$$

$$= (-1)^{n-1} T_1 \dots T_{n-1} \det \begin{pmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ T_1^{n-1} & \dots & T_{n-1}^{n-1} \end{pmatrix} \quad (9.40c)$$

$$= (-1)^{n-1} T_1 \dots T_{n-1} V(T_1, \dots, T_{n-1}) \quad (9.40d)$$

En égalisant avec (9.39), nous trouvons $\alpha = V(T_1, \dots, T_{n-1})$, et donc

$$f = V(T_1, \dots, T_{n-1}) \prod_{j \leq n-1} (X - T_j) \quad (9.41)$$

Enfin, une récurrence montre que

$$V(T_1, \dots, T_n) = f(T_n) \quad (9.42a)$$

$$= V(T_1, \dots, T_{n-1}) \prod_{j \leq n-1} (T_n - T_j) \quad (9.42b)$$

$$= \prod_{k \leq n} \prod_{j \leq k-1} (T_k - T_j) \quad (9.42c)$$

$$= \prod_{1 \leq j < k \leq n} (T_k - T_j). \quad (9.42d)$$

□

6. Proposition 3.137.

Exemple 9.12.

Le déterminant de Vandermonde (proposition 9.11) est alterné, semi-symétrique et non symétrique. Le fait qu'il soit alterné est le fait qu'il soit un déterminant. Étant donné qu'il est alterné, il est semi-symétrique parce que sur A_n , nous avons $\epsilon = 1$. Étant donné qu'il est alterné, il change de signe sous l'action des éléments impairs de S_n et n'est donc pas symétrique. $\triangle$

Proposition 9.13.

Un polynôme semi-symétrique $f \in \mathbb{K}[T_1, \dots, T_n]$ se décompose de façon unique en

$$f = P + VQ \quad (9.43)$$

où P et Q sont deux polynômes symétriques.

Démonstration. Nous commençons par prouver l'unicité en montrant que si $f = PVQ$ avec P et Q symétrique, alors P et Q sont donnés par des formules explicites en termes de f .

Si σ_1 et σ_2 sont deux permutations impaires de $\{1, \dots, n\}$, alors $\sigma_1 \cdot f = \sigma_2 \cdot f$ parce que l'élément $\sigma_2^{-1}\sigma_1$ est pair (proposition 1.159), de telle sorte que $\sigma_2^{-1}\sigma_1 \cdot f = f$. Nous posons donc $g = \tau \cdot f$ où τ est une permutation impaire quelconque – par exemple une transposition.

Vu que V est alternée et que τ est une transposition nous avons

$$g = \tau \cdot f = P - VQ. \quad (9.44)$$

Donc $f + g = 2P$ et $f - g = 2VQ$. Cela donne P et Q en termes de f et g , et donc l'unicité.

Attention : cela ne donne pas un moyen de prouver l'existence parce que rien ne prouve pour l'instant que $f - g$ peut effectivement être écrit sous la forme VQ , c'est-à-dire que $f - g$ soit divisible par V . C'est cela que nous allons nous atteler à démontrer maintenant.

Nous commençons par prouver que $f + g$ est symétrique et $f - g$ alterné. Si σ est une transposition,

$$\sigma \cdot (f + g) = \sigma \cdot f + \sigma \tau \cdot f = g + f \quad (9.45)$$

parce que $\sigma\tau$ est pair. De la même façon,

$$\sigma \cdot (f - g) = g - f = \epsilon(\sigma)(f - g). \quad (9.46)$$

Dans les deux cas nous concluons en utilisant le fait que toute permutation est un produit de transpositions (proposition 1.156) et que ϵ est un homomorphisme.

Soient maintenant deux entiers $h < k$ dans $\{1, \dots, n\}$ et l'anneau

$$(\mathbb{K}[T_1, \dots, \hat{T}_k, \dots, T_n])[T_k]. \quad (9.47)$$

Cet anneau contient le polynôme $T_k - T_h$ où T_k est la variable et T_h est un coefficient. Nous faisons la division euclidienne de $f - g$ par $T_k - T_h$ parce que nous avons dans l'idée de faire arriver le déterminant de Vandermonde et donc le produit de toutes les différences $T_k - T_h$:

$$f - g = (T_k - T_h)q + r \quad (9.48)$$

où $\deg_{T_k} r < 1$, c'est-à-dire que r ne dépend pas de T_k . Nous revoyons maintenant l'égalité (9.48) dans $\mathbb{K}[T_1, \dots, T_n]$ et nous y appliquons la transposition τ_{kh} . Nous savons que $\tau_{kh}(f - g) = -(f - g)$ et $\tau_{kh}(T_k - T_h) = -(T_k - T_h)$, et donc

$$-(f - g) = -(T_k - T_h)\tau_{kh} \cdot q + \tau_{kh} \cdot r \quad (9.49)$$

où $\tau_{kh} \cdot r$ ne dépend pas de T_h . Nous appliquons à (9.49) l'application

$$\begin{aligned} t\alpha: \mathbb{K}[T_1, \dots, T_n] &\rightarrow \mathbb{K}[T_1, \dots, \hat{T}_k, \dots, T_n] \\ \alpha(PT_1, \dots, \hat{T}_k, \dots, T_n) &= P(T_1, \dots, T_h, \dots, T_n). \end{aligned} \quad (9.50)$$

Cette application vérifie $\alpha(\tau_{kh} \cdot r) = \alpha(r)$ et nous avons

$$-\alpha(f - g) = \alpha(r). \quad (9.51)$$

Puis en appliquant α à la relation $f - g = (T_k - T_h)q + r$, nous trouvons

$$\alpha(f - g) = \alpha(r), \quad (9.52)$$

et par conséquent $\alpha(r) = 0$. Ici nous utilisons l'hypothèse de caractéristique différente de deux. Dire que $\alpha(r) = 0$, c'est dire que r est divisible par $T_k - T_h$, mais r étant de degré zéro en T_k , nous avons $r = 0$. Par conséquent $T_k - T_h$ divise $f - g$ pour tout $h < k$, et nous pouvons définir un polynôme Q par

$$f - g = 2Q \prod_{h < k} \prod_{k \leq n} (T_k - T_h) = 2Q(T_1, \dots, T_n)V(T_1, \dots, T_n), \quad (9.53)$$

où nous avons utilisé la formule du déterminant de Vandermonde de la proposition 9.11.

Étant donné que $f + g$ est un polynôme symétrique, nous allons aussi poser $f + g = 2P$ avec P symétrique.

Montrons à présent que Q est un polynôme symétrique. Soit $\sigma \in S_n$; vu que nous savons déjà que $f - g$ est alternée, nous avons

$$\sigma \cdot (f - g) = \epsilon(\sigma)(f - g) = \epsilon(\sigma)2QV, \quad (9.54)$$

Mais en appliquant σ à l'équation (9.53),

$$\sigma \cdot (f - g) = 2(\sigma \cdot V)(T_1, \dots, T_n)(\sigma \cdot Q)(T_1, \dots, T_n) \quad (9.55a)$$

$$= 2\epsilon(\sigma)V(T_1, \dots, T_n)(\sigma \cdot Q)(T_1, \dots, T_n). \quad (9.55b)$$

Nous égalisons cela avec (9.54) et nous souvenant que l'anneau $\mathbb{K}[T_1, \dots, T_n]$ est intègre par le théorème 3.121. Ensuite nous simplifions par $2\epsilon(\sigma)V$ pour obtenir

$$Q = \sigma \cdot Q, \quad (9.56)$$

c'est-à-dire que Q est symétrique.

Au final nous avons $f + g = 2P$ et $f - g = 2VQ$ avec P et Q symétriques. En faisant la somme,

$$f = P + VQ. \quad (9.57)$$

□

9.1.5 Déterminant de Gram

Si $x_1, \dots, x_r$ sont des vecteurs d'un espace vectoriel, alors le **déterminant de Gram** est le déterminant

$$G(x_1, \dots, x_r) = \det(\langle x_i, x_j \rangle). \quad (9.58)$$

Notons que la matrice est une matrice symétrique.

Proposition 9.14.

Si F est un sous-espace vectoriel de base $\{x_1, \dots, x_n\}$ et si x est un vecteur, alors le déterminant de Gram est un moyen de calculer la distance entre x et F par

$$d(x, F)^2 = \frac{G(x, x_1, \dots, x_n)}{G(x_1, \dots, x_n)}. \quad (9.59)$$

9.1.6 Déterminant de Cauchy

Soient des nombres a_i et b_i ($i = 1, \dots, n$) tels que $a_i + b_j \neq 0$ pour tout couple (i, j) . Le **déterminant de Cauchy** est

$$D_n = \det \left(\frac{1}{a_i + b_j} \right). \quad (9.60)$$

Proposition 9.15 ([196]).

Le déterminant de Cauchy est donné par la formule

$$D_n = \frac{\prod_{i < j} (a_j - a_i) \prod_{i < j} (b_j - b_i)}{\prod_{i,j} (a_i + b_j)}. \quad (9.61)$$

9.1.7 Matrice de Sylvester

La définition est pompée de [wikipédia](#). Soient P et Q deux polynômes non nuls, de degrés respectifs m et n :

$$P(x) = p_0 + p_1x + \dots + p_nx^n \quad (9.62a)$$

$$Q(x) = q_0 + q_1x + \dots + q_mx^m. \quad (9.62b)$$

La **matrice de Sylvester** associée à P et Q est la matrice carrée $m + n \times m + n$ définie ainsi :

- (1) la première ligne est formée des coefficients de P , suivis de 0 :

$$(p_n \ p_{n-1} \ \dots \ p_1 \ p_0 \ 0 \ \dots \ 0); \quad (9.63)$$

- (2) la seconde ligne s'obtient à partir de la première par permutation circulaire vers la droite ;

- (3) les $(m-2)$ lignes suivantes s'obtiennent en répétant la même opération ;

- (4) la ligne $(m+1)$ est formée des coefficients de Q , suivis de 0 :

$$(q_m \ q_{m-1} \ \dots \ q_1 \ q_0 \ 0 \ \dots \ 0); \quad (9.64)$$

- (5) les $(m-1)$ lignes suivantes sont formées par des permutations circulaires.

Ainsi dans le cas $n = 4$ et $m = 3$, la matrice obtenue est

$$S_{p,q} = \begin{pmatrix} p_4 & p_3 & p_2 & p_1 & p_0 & 0 & 0 \\ 0 & p_4 & p_3 & p_2 & p_1 & p_0 & 0 \\ 0 & 0 & p_4 & p_3 & p_2 & p_1 & p_0 \\ q_3 & q_2 & q_1 & q_0 & 0 & 0 & 0 \\ 0 & q_3 & q_2 & q_1 & q_0 & 0 & 0 \\ 0 & 0 & q_3 & q_2 & q_1 & q_0 & 0 \\ 0 & 0 & 0 & q_3 & q_2 & q_1 & q_0 \end{pmatrix}. \quad (9.65)$$

Le déterminant de la matrice de Sylvester associée à P et Q est appelé le **résultant** de P et Q et noté $\text{res}(P, Q)$.

Attention : si P est de degré n et Q de degré m , il y a m lignes pour P et n pour Q dans le déterminant du résultant (et non le contraire).

Lemme 9.16 ([197]).

Si P et Q sont deux polynômes de degrés n et m à coefficients dans l'anneau $\mathbb{A}$, alors pour tout $\lambda \in \mathbb{A}$,

$$\text{res}(\lambda P, Q) = \lambda^m \text{res}(P, Q) \quad (9.66a)$$

$$\text{res}(P, \lambda Q) = \lambda^n \text{res}(P, Q). \quad (9.66b)$$

Démonstration. Cela est simplement un comptage du nombre de lignes. Il y a m lignes contenant les coefficients de P ; donc prendre λP revient à multiplier m lignes dans un déterminant et donc le multiplier par λ^m . $\square$

L'équation de Bézout (6.82) peut être traitée avec une matrice de Sylvester. Soient P et Q , deux polynômes donnés et à résoudre l'équation

$$xP + yQ = 0 \quad (9.67)$$

par rapport aux polynômes inconnus x et y dont les degrés sont $\deg(x) < \deg(Q)$ et $\deg(y) < \deg(P)$. Si nous notons $\tilde{x}$ et $\tilde{y}$ la liste des coefficients de x et y (dans l'ordre décroissant de degré), nous pouvons récrire l'équation (9.67) sous la forme

$$S_{PQ}^t \begin{pmatrix} \tilde{x} \\ \tilde{y} \end{pmatrix} = 0. \quad (9.68)$$

Pour s'en convaincre, écrivons pour les polynômes de l'exemple (9.65) :

$$\begin{pmatrix} p_4 & 0 & 0 & q_3 & 0 & 0 & 0 \\ p_3 & p_4 & 0 & q_2 & q_3 & 0 & 0 \\ p_2 & p_3 & p_4 & q_1 & q_2 & q_3 & 0 \\ p_1 & p_2 & p_3 & q_0 & q_1 & q_2 & q_3 \\ p_0 & p_1 & p_2 & 0 & q_0 & q_1 & q_2 \\ 0 & p_0 & p_1 & 0 & 0 & q_0 & q_1 \\ 0 & 0 & p_0 & 0 & 0 & 0 & q_0 \end{pmatrix} \begin{pmatrix} x_2 \\ x_1 \\ x_0 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{pmatrix} = \begin{pmatrix} x_2 p_4 + y_2 q_3 \\ p_3 x_2 + p_4 x_1 + q_2 y_3 + q_3 y_2 \\ \vdots \end{pmatrix} \quad (9.69)$$

Nous voyons que sur la ligne numéro k (en partant du bas et en numérotant de 0 à partir de zéro) nous avons les produits $p_i x_j$ et $q_i y_j$ avec $i + j = k$. La colonne de droite représente donc bien les coefficients du polynôme $xP + yQ$.

Proposition 9.17.

Le résultant de deux polynômes est non nul si et seulement si les deux polynômes sont premiers entre eux.

Un polynôme P a une racine double en a si et seulement si P et P' ont a comme racine commune, ce qui revient à dire que P et P' ne sont pas premiers entre eux.

Une application importante de ces résultats sera le théorème de Rothstein-Trager 20.98 sur l'intégration de fractions rationnelles.

Exemple 9.18.

Si nous prenons $P = aX^2 + bX + c$ et $P' = 2aX + b$ alors la taille de la matrice de Sylvester sera $2 + 1 = 3$ et

$$S_{P,P'} = \begin{pmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{pmatrix}. \quad (9.70)$$

Le résultant est alors

$$\text{res}(P, P') = -a(b^2 - 4ac). \quad (9.71)$$

Donc un polynôme du second degré a une racine double si et seulement si $b^2 - 4ac = 0$. Cela est un résultat connu depuis longtemps mais qui fait toujours plaisir à revoir. $\triangle$

La matrice de Sylvester permet aussi de récrire l'équation de Bézout pour les polynômes ; voir le théorème 6.43 et la discussion qui s'ensuit.

Une proposition importante du résultant est qu'il peut s'exprimer à l'aide des racines des polynômes.

Proposition 9.19.

Si

$$P(X) = a_p \prod_{i=1}^p (X - \alpha_i) \quad (9.72a)$$

$$Q(X) = b_q \prod_{j=1}^q (X - \beta_j) \quad (9.72b)$$

alors nous avons les expressions suivantes pour le résultant :

$$\text{res}(P, Q) = a_p^q b_q^p \prod_{i=1}^p \prod_{j=1}^q (\beta_j - \alpha_i) = b_q^p \prod_{j=1}^q P(\beta_j) = (-1)^{pq} a_p^q \prod_{i=1}^p Q(\alpha_i). \quad (9.73)$$

Démonstration. Si P et Q ne sont pas premiers entre eux, d'une part la proposition 9.17 nous dit que $\text{res}(P, Q) = 0$ et d'autre part, P et Q ont un facteur irréductible en commun, ce qui signifie que nous devons avoir un des $X - \alpha_i$ égal à un des $X - \beta_j$. Autrement dit, nous avons $\alpha_i = \beta_j$ pour un couple (i, j) . Par conséquent tous les membres de l'équation (9.73) sont nuls.

Nous supposons donc que P et Q sont premiers entre eux. Nous commençons par supposer que les polynômes P et Q sont unitaires, c'est-à-dire que $a_p = b_q = 1$. Nous considérons alors l'anneau

$$\mathbb{A} = \mathbb{Z}[\alpha_1, \dots, \alpha_p, \beta_1, \dots, \beta_q]. \quad (9.74)$$

Dans cet anneau, l'élément $\beta_j - \alpha_i$ est irréductible (tout comme $X - Y$ est irréductible dans $\mathbb{Z}[X, Y]$). Le résultant $R = \text{res}(P, Q)$ est un élément de $\mathbb{A}$ parce que tous leurs coefficients peuvent être exprimés à l'aide des α_i et des β_j . Dans $\mathbb{A}$, l'élément $\beta_j - \alpha_i$ divise R . En effet lorsque $\beta_j = \alpha_i$, le déterminant définissant le résultant est nul, ce qui signifie que $\beta_j - \alpha_i$ est un facteur irréductible de R .

Par conséquent il existe un polynôme $T \in \mathbb{A}$ tel que

$$R = \lambda(\alpha_1, \dots, \beta_q) \prod_{i=1}^p \prod_{j=1}^q (\beta_j - \alpha_i). \quad (9.75)$$

Comptons les degrés. Pour donner une idée de ce calcul de degré, voici comment se présente, au niveau des dimensions, le déterminant :

$$\begin{array}{ccccccc} & \xleftarrow{p+1} & & \xleftarrow{q-1} & & & \\ & & & & & & \\ a_p & \cdots & a_{p-1} & \cdots & a_0 & \cdots & 0 \cdots 0 \\ & \searrow & & & \searrow & & \\ 0 \cdots 0 & & a_p & \cdots & a_1 & \cdots & a_0 \end{array} \quad \begin{array}{c} \uparrow q \\ \downarrow q \end{array} \quad (9.76)$$

$\xleftarrow{p+q}$

si les a_i sont les coefficients de P . Mais chacun des a_i est de degré 1 en les α_i , donc le déterminant dans son ensemble est de degré q en les α_i , parce que R contient q lignes telles que (9.76). Le même raisonnement montre que R est de degré p en les β_j . Par ailleurs le polynôme $\prod_{i=1}^p \prod_{j=1}^q (\beta_j - \alpha_i)$ est de degré p en les β_j et q en les α_i . Nous en déduisons que T doit être un polynôme ne dépendant pas de α_i ou de β_j .

Nous pouvons donc calculer la valeur de T en choisissant un cas particulier. Avec $P(X) = X^p$ et $Q(X) = X^q + 1$, il est vite vu que $R(P, Q) = 1$ et donc que $T = 1$.

Si les polynômes P et Q ne sont pas unitaires, le lemme 9.16 nous permet de conclure. □

9.1.8 Théorème de Kronecker

Nous considérons K_n l'ensemble des polynômes de $\mathbb{Z}[X]$

- (1) unitaires de degré n ,
- (2) dont les racines dans $\mathbb{C}$ sont de modules plus petits ou égaux à 1,
- (3) et qui ne sont pas divisés par X .

Un tel polynôme s'écrit sous la forme

$$P = X^n + \sum_{k=0}^{n-1} a_k X^k. \quad (9.77)$$

Théorème 9.20 (Kronecker[79]).

Les racines des éléments de K_n sont des racines de l'unité.

Démonstration. Vu que $\mathbb{C}$ est algébriquement clos nous pouvons considérer les racines $\alpha_1, \dots, \alpha_n$ de P dans $\mathbb{C}$. Nous les considérons avec leurs multiplicités.

Soit $R = X^n + \sum_{k=0}^{n-1} b_k X^k$ un élément de K_n dont nous notons $\beta_1, \dots, \beta_n$ les racines dans $\mathbb{C}$. Les relations coefficients-racines stipulent que

$$b_k = \sum_{1 \leq i_1 < \dots < i_{n-k} \leq n} \prod_{j=1}^{n-k} \beta_{i_j}. \quad (9.78)$$

En prenant le module et en se souvenant que $|\beta_l| \leq 1$ pour tout l , nous trouvons que

$$|b_k| \leq \binom{n}{n-k}. \quad (9.79)$$

Mais comme $b_k \in \mathbb{Z}$, nous avons

$$b_k \in \left\{ -\binom{n}{n-k}, -\binom{n}{n-k} + 1, \dots, 0, \dots, \binom{n}{n-k} \right\} \quad (9.80)$$

qui est de cardinal $\binom{n}{n-k} + 1$. Nous avons donc

$$\text{Card}(K_n) \leq \prod_{k=0}^{n-1} (1 + \binom{n}{n-k}) < \infty. \quad (9.81)$$

La conclusion jusqu'ici est que K_n est un ensemble fini.

Pour chaque $k \in \mathbb{N}^*$ nous considérons les polynômes

$$P_k = \prod_{i=1}^n (X - \alpha_i^k) \quad (9.82a)$$

$$Q_k = X^k - Y \in \mathbb{Z}[X, Y], \quad (9.82b)$$

et puis nous considérons le résultant $R_k = \text{res}_X(P, Q_k) \in \mathbb{Z}[Y]$:

$$R_k = \text{res}_X(P, Q_k) = \begin{pmatrix} 1 & a_{n-1} & \cdots & a_0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & a_{n-1} & \cdots & a_0 & 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & & & \\ 0 & \cdots & 0 & 1 & a_{n-1} & \cdots & a_0 & 0 & 0 \\ 0 & \cdots & 0 & 0 & 1 & a_{n-1} & \cdots & a_0 & 0 \\ 0 & \cdots & 0 & 0 & 0 & 1 & a_{n-1} & \cdots & a_0 \\ 1 & 0 & \cdots & 0 & -Y & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & -Y & 0 & \cdots & 0 \\ & & \ddots & & & \ddots & \ddots & & \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 & -Y & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 & -Y \end{pmatrix} \quad (9.83)$$

Cela est un polynôme en Y dont le terme de plus haut degré est $(-1)^n Y^n$. Les petites formules de la proposition 9.19 nous permettent d'exprimer $R_k(Y)$ en termes des racines de P :

$$R_k(Y) = \prod_{i=1}^n Q_k(\alpha_i) = \prod_{i=1}^n (\alpha_i^k - Y) = (-1)^n \prod_{i=1}^n (Y - \alpha_i^k) = (-1)^n P_k(Y). \quad (9.84)$$

Vu que $P \in K_n$ nous savons que les α_i ne sont pas tous nuls ; donc $P_k \in K_n$. Cependant nous avons vu que K_n est un ensemble fini ; donc parmi les P_k , il y a des doublons (et pas un peu)⁷. Nous regardons même l'ensemble des P_{2^n} dans lequel nous pouvons en trouver deux les mêmes. Soit $l > k$ tels que $P_{2^k} = P_{2^l}$. Si α est racine de P_{2^k} , alors il est de la forme $\alpha = \beta^{2^k}$ pour une certaine racines β de P . Par conséquent

$$\alpha^{2^l/2^k} = \alpha^{2^{l-k}} \quad (9.85)$$

est racine de P_{2^l} . Notons que dans cette expression il n'y a pas de problèmes de définition d'exposant fractionnaire dans $\mathbb{C}$ parce que $l > k$. Vu que (9.85) est racine de P_{2^l} , il est aussi racine de P_{2^k} . Donc

$$(\alpha^{2^{l-k}})^{2^{l-k}} = \alpha^{2^{2(l-k)}} \quad (9.86)$$

est racine de P_{2^l} et donc de P_{2^k} . Au final nous savons que tous les nombres de la forme $\alpha^{2^{n(l-k)}}$ sont racines de P_{2^k} . Mais comme P_{2^k} a un nombre fini de racines, nous pouvons en trouver deux égales. Si nous avons

$$\alpha^{2^{n(l-k)}} = \alpha^{2^{m(l-k)}} \quad (9.87)$$

pour certains entiers $m > n$, alors

$$\alpha^{2^{n(l-k)} - 2^{m(l-k)}} = 1, \quad (9.88)$$

ce qui prouve que α est une racine de l'unité. Nous avons donc prouvé que toutes les racines de P_{2^k} sont des racines de l'unité et donc que les racines de P sont racines de l'unité. $\square$

9.2 Orientation

9.2.1 Cas vectoriel

Proposition-Définition 9.21 ([198]).

Soient deux bases $\mathcal{B}$ et $\mathcal{B}'$ d'un espace vectoriel réel E . Nous définissons la relation $\mathcal{B} \sim \mathcal{B}'$ si et seulement si $\det_{\mathcal{B}}(\mathcal{B}') > 0$ ⁸.

Cela est une relation d'équivalence⁹ sur l'ensemble des bases de E , et les classes sont les **orientations** de E .

Démonstration. Tout est dans le lemme 9.6. D'abord quand $\mathcal{B}$ et $\mathcal{B}'$ sont des bases, $\det_{\mathcal{B}}(\mathcal{B}') \neq 0$ ensuite, nous passons en revue les points qu'il faut pour être une relation d'équivalence.

- (1) $\mathcal{B} \sim \mathcal{B}$ parce que $\det_{\mathcal{B}}(\mathcal{B}) = 1 > 0$.
- (2) Vu que $\det_{\mathcal{B}}(\mathcal{B}') = \frac{1}{\det_{\mathcal{B}'}(\mathcal{B})}$, les deux sont positifs en même temps ou pas du tout.
- (3) Si $\mathcal{B} \sim \mathcal{B}'$ et $\mathcal{B}' \sim \mathcal{B}''$, alors en utilisant la formule

$$\det_{\mathcal{B}}(\mathcal{B}'') = \det_{\mathcal{B}}(\mathcal{B}') \det_{\mathcal{B}'}(\mathcal{B}''), \quad (9.89)$$

nous voyons que $\det_{\mathcal{B}}(\mathcal{B}'') > 0$. $\square$

7. Ici dans [79], il déduit qu'on a un k tel que $P_k = P_1 = P$. Mais je vois pourquoi on a un k et un l tels que $P_k = P_l$, mais pourquoi on peut en trouver un spécialement égal au premier ? Une réponse à cette question permettrait de solidement réduire la lourdeur de la suite de la preuve.

8. Définition 9.4.

9. Définition 1.23.

Lemme 9.22.

Soit un espace vectoriel réel E . L'ensemble des bases de E possède exactement deux orientations¹⁰

Démonstration. Nous considérons une base $\mathcal{B} = (e_1, \dots, e_n)$ ¹¹ à partir de laquelle nous définissons une autre base : $\mathcal{B}' = (-e_1, e_2, \dots, e_n)$. Nous allons prouver que ces deux bases ne sont pas équivalentes, et que toute base de E est équivalente soit à $\mathcal{B}$ soit à $\mathcal{B}'$.

Au moins deux classes Le fait que $\det_{\mathcal{B}}(\mathcal{B}') = -1$ vient du fait que $\det_{\mathcal{B}}(\mathcal{B}') = 1$ et que l'application $\det_{\mathcal{B}}$ est n -linéaire ; en multipliant par -1 le premier argument, la valeur du déterminant est multipliée par -1 .

Donc les bases $\mathcal{B}$ et $\mathcal{B}'$ ne sont pas équivalentes et il existe au moins deux classes.

Au plus deux classes Nous montrons à présent que toute base est équivalente soit à $\mathcal{B}$ soit à $\mathcal{B}'$.

Supposons que $\mathcal{B}''$ ne soit pas équivalente à $\mathcal{B}$, c'est-à-dire que $\det_{\mathcal{B}}(\mathcal{B}'') < 0$. Nous utilisons encore la formule (9.11),

$$\underbrace{\det_{\mathcal{B}}(\mathcal{B}'')}_{<0} = \underbrace{\det_{\mathcal{B}}(\mathcal{B}')}_{<0} \det_{\mathcal{B}'}(\mathcal{B}''), \quad (9.90)$$

et nous déduisons que $\det_{\mathcal{B}'}(\mathcal{B}'') > 0$.

□

9.23.

Vu qu'il n'y a que deux classes d'équivalence parmi les bases, nous pouvons utiliser le vocable « avoir la même orientation que » ou « avoir l'orientation contraire de ». Ce n'est pas ambigu.

Proposition 9.24 ([198]).

Si $\mathcal{B}$ est une base de l'espace vectoriel E de dimension n , et si τ est une transposition¹² de S_n , alors la base $\tau(\mathcal{B})$ est de sens contraire.

Démonstration. Le lemme 9.6(2) dit que $\det_{\mathcal{B}}$ est une forme anti-symétrique ; donc

$$\det_{\mathcal{B}}(\mathcal{B}') = -\det_{\mathcal{B}}(\tau(\mathcal{B})). \quad (9.91)$$

Si l'un est positif, l'autre est négatif. Elles ont donc des orientations contraires.

□

Corolaire 9.25.

Si $\mathcal{B}$ est une base de l'espace vectoriel E de dimension n , et si $\sigma \in S_n$, la base $\sigma(\mathcal{B})$ a même orientation que $\mathcal{B}$ si et seulement si $\sigma \in A_n$.

Démonstration. Notons c_1 la classe d'orientation de $\mathcal{B}$ et c_2 l'autre classe. La permutation σ se décompose en produit de transpositions dont la parité est fixée (proposition 1.157). Posons $\sigma = \tau_k \dots \tau_1$.

En posant $\mathcal{B}_0 = \mathcal{B}$ et $\mathcal{B}_{l+1} = \tau_{l+1}(\mathcal{B}_l)$, pour tout l , la base $\mathcal{B}_l$ est d'orientation contraire à celle de la base $\mathcal{B}_{l-1}$. Une base sur deux a l'orientation de $\mathcal{B}$ et l'autre sur deux a l'orientation contraire.

Donc $\sigma(\mathcal{B})$ a la même orientation que $\mathcal{B}$ si et seulement si k est pair. Mais $\sigma \in A_n$ si et seulement si k est pair. C'est bon.

□

Proposition-Définition 9.26 ([198]).

Soit un espace vectoriel réel, et un endomorphisme f de E . Deux définitions.

- (1) L'endomorphisme f est **direct** si son déterminant est strictement positif.
- (2) L'endomorphisme **préserve l'orientation** si il transforme toute base de E en une base de même orientation.

Un endomorphisme est direct si et seulement si il préserve l'orientation.

10. Définition 9.21.

11. Nous notons (e_1, e_2) et non $\{e_1, e_2\}$ parce que l'ordre est important.

12. Définition 1.147.

Démonstration. En deux sens.

Direct implique préserve l'orientation Soit une base $\mathcal{B}$ de E et un endomorphisme direct u .

D'abord, u est inversible du fait que son déterminant est non nul par la proposition 9.9(2).

Donc u transforme une base en une base par le lemme 4.7.

La définition 9.8 du déterminant de u est que

$$\det(u) = \det_{\mathcal{B}}(u(\mathcal{B})) > 0. \quad (9.92)$$

Donc $\mathcal{B}$ et $u(\mathcal{B})$ ont même orientation.

Préserve l'orientation implique direct Le fait que u préserve l'orientation signifie en particulier qu'il transforme une base en une base et qu'il est inversible par le lemme 4.7.

Donc si $\mathcal{B}$ est une base, $u(\mathcal{B})$ est encore une base et nous avons, parce que $\mathcal{B}$ et $u(\mathcal{B})$ ont même orientation,

$$0 < \det_{\mathcal{B}}(u(\mathcal{B})) = \det(u). \quad (9.93)$$

□

9.2.2 Cas affine

Définition 9.27.

Soit un espace affine $\mathcal{E}$ modelé sur E . Les repères cartésiens¹³ $(O, \mathcal{B})$ et $(O', \mathcal{B}')$ ont **même orientation** si les bases $\mathcal{B}$ et $\mathcal{B}'$ ont même orientation.

Les classes d'équivalence (il y en a deux) sont les orientations de $\mathcal{E}$.

Une application affine $f: \mathcal{E} \rightarrow \mathcal{E}$ **préserve l'orientation** si sa partie linéaire¹⁴ préserve l'orientation.

9.3 Hermitien, orthogonal, adjoint

9.28.

Une des choses à retenir de la définition de l'opérateur adjoint est que la notion de A^* dépend du produit scalaire considéré.

Il se fait que le plus souvent, sur $\mathbb{R}^n$, nous considérons le produit scalaire usuel et la base canonique. De ce fait, les notions d'opérateur adjoint et d'opérateur transposés se confondent avec la notion de matrice transposée. Ce sont pourtant, en général, trois notions distinctes.

Proposition-Définition 9.29 (Définition de la transposée[1]).

Soient deux espaces vectoriels euclidiens ou hermitiens E et F et une application linéaire $A: E \rightarrow F$.

(1) Il existe une unique application linéaire $B: F \rightarrow E$ telle que

$$\langle Ax, y \rangle_F = \langle x, By \rangle_E \quad (9.94)$$

pour tout $x \in E$ et $y \in F$.

(2) Si $\{e_i\}$ est une base orthonormée de E et $\{f_\alpha\}$ est une base orthonormée de F , alors la matrice de A et B pour ces bases sont liées par

$$B_{i\alpha} = A_{\alpha i}. \quad (9.95)$$

L'application B ainsi définie est nommée **adjoint** de A et sera notée $B = A^*$.

13. Définition 8.6.

14. Définition 8.10.

Démonstration. Pour l'unicité, nous écrivons la condition avec $x = e_j$ pour obtenir :

$$\langle Ae_j, y \rangle = \langle e_j, By \rangle = (By)_j \quad (9.96)$$

c'est-à-dire que les coefficients $B(y)_j$ de $B(y)$ dans la base canonique sont fixés par la condition.

Pour l'existence, il suffit de vérifier que poser

$$B(y) = \sum_j \langle Ae_j, y \rangle e_j \quad (9.97)$$

fonctionne. Pour cela il faut utiliser la bilinéarité du produit scalaire et le fait que $\langle x, e_j \rangle = x_j$. Nous avons :

$$\langle x, B(y) \rangle = \langle x, \sum_j \langle Ae_j, y \rangle e_j \rangle \quad (9.98a)$$

$$= \sum_j \langle Ae_j, y \rangle \langle x, e_j \rangle \quad (9.98b)$$

$$= \sum_j \langle A(x_j e_j), y \rangle \quad (9.98c)$$

$$= \langle A(x), y \rangle. \quad (9.98d)$$

En ce qui concerne la matrice de l'application B ainsi définie, nous écrivons la condition (9.94) avec $y = e'_\alpha$ et $x = e_i$, de telle sorte que

$$A(x) = A(e_i) = \sum_\beta A_{\beta i} e'_\beta \quad (9.99)$$

et

$$B(y) = B(e'_\alpha) = \sum_j B_{j\alpha} e_j. \quad (9.100)$$

Alors nous avons :

$$\sum_\beta A_{\beta i} \langle e'_\beta, e'_\alpha \rangle = \sum_j B_{j\alpha} \langle e_i, e_j \rangle, \quad (9.101)$$

donc

$$A_{\alpha i} = B_{i\alpha}. \quad (9.102)$$

□

9.30.

À cause de l'expression (9.95) pour la matrice de A^* , cette application est souvent appelé **transposé** de A et noté A^t . Nous savons, nous, que la transposée de A est une application $A^t: F^* \rightarrow E^*$ donnée par la définition 4.135. Il nous arrivera donc d'écrire des égalités comme $\langle Ax, y \rangle = \langle x, A^t y \rangle$.

Proposition 9.31.

En ce qui concerne le déterminant,

$$\det(A^*) = \det(A)^* \quad (9.103)$$

où l'étoile à droite dénote la conjugaison complexe dans $\mathbb{C}$.

Démonstration. Écrivons l'expression explicite (9.7) du déterminant. Le tout avec la base canonique :

$$\det(A) = \det_{(e_1, \dots, e_n)}(Ae_1, \dots, Ae_n) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^n e_{\sigma(i)}^*(Ae_i). \quad (9.104)$$

Mais nous pouvons développer :

$$e_{\sigma(i)}^*(Ae_i) = \langle e_{\sigma(i)}, Ae_i \rangle = \langle A^* e_{\sigma(i)}, e_i \rangle = \langle e_i, A^* e_{\sigma(i)} \rangle^* = e_i^*(A^* e_{\sigma(i)})^*. \quad (9.105)$$

Notez que dans la dernière expression, les trois $*$ ont trois significations différentes. Par conséquent,

$$\det(A) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^n e_i^*(A^* e_{\sigma(i)})^*. \quad (9.106)$$

Mais $e_i^*(A^* e_{\sigma(i)}) = e_{\sigma(j)}^*(A^* e_j)$ pour $j = \sigma(i)$, donc le produit ne change pas si on déplace le σ :

$$\det(A) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^n e_{\sigma(i)}^*(A^* e_i)^* = \det(A^*)^*. \quad (9.107)$$

Nous avons donc $\det(A) = \det(A^*)^*$, c'est-à-dire $\det(A)^* = \det(A^*)$. Pour information, la dernière étoile est la conjugaison complexe. $\square$

Proposition 9.32 ([1]).

Si $A: E_2 \rightarrow E_3$ et $B: E_1 \rightarrow E_2$ sont des applications linéaires, alors

$$(AB)^* = B^* A^* \quad (9.108)$$

où la « multiplication » est la composition.

Démonstration. L'existence de $(AB)^*$, de A^* et de B^* ne donne pas lieu à débat parce que la proposition 9.29 ne souffre pas de discussions. La propriété que $(AB)^*$ est unique à avoir est que

$$\langle ABx, y \rangle = \langle x, (AB)^* y \rangle \quad (9.109)$$

pour tout $x \in E_1$ et $y \in E_3$. Or l'application $B^* A^*$ possède également cette propriété parce que

$$\langle x, B^* A^* y \rangle = \langle Bx, A^* y \rangle = \langle ABx, y \rangle. \quad (9.110)$$

La partie unicité de la proposition 9.29 nous impose donc d'accepter que les applications $(AB)^*$ et $B^* A^*$ sont en réalité les mêmes¹⁵. $\square$

9.33.

Un grand moment d'utilisation de la notion d'adjoint pour un opérateur non carré sera la définition d'une intégrale sur une variété ; en particulier dans la proposition 20.9.

Définition 9.34.

Un opérateur A est **hermitien** si $A^* = A$. On dit aussi **autoadjoint**.

9.35.

Le mot « hermitien » est réservé aux opérateurs sur des espaces hermitiens, c'est-à-dire des espaces vectoriels sur $\mathbb{C}$. Le mot « autoadjoint » par contre est plutôt utilisé dans le cadre d'opérateurs sur les espaces réels. En conséquence de quoi, ces deux mots sont synonymes, mais il est préférable d'utiliser « hermitien » lorsque l'espace vectoriel est sur $\mathbb{C}$ et « autoadjoint » lorsqu'il est sur $\mathbb{R}$.

L'ensemble des opérateurs autoadjoints de E est noté $S(E)$. Cette notation provient du fait que dans $\mathbb{R}^n$ muni du produit scalaire usuel, les opérateurs autoadjoints sont les matrices symétriques.

Remarque 9.36.

Le fait d'être hermitien n'implique en rien le fait d'être inversible.

Lemme 9.37.

Si E est un espace euclidien, un endomorphisme $f: E \rightarrow E$ est autoadjoint si et seulement si pour tout $x, y \in E$ nous avons $\langle x, f(y) \rangle = \langle f(x), y \rangle$.

Démonstration. Dans le sens direct, nous avons

$$\langle f(x), y \rangle = \langle x, f^*(y) \rangle = \langle x, f(y) \rangle. \quad (9.111)$$

La première égalité est la définition de f^* et la seconde est l'hypothèse $f = f^*$.

Dans l'autre sens, l'hypothèse est que l'endomorphisme f vérifie $\langle x, f(y) \rangle = \langle f(x), y \rangle$. Mais la proposition 9.29(1) spécifie que f^* est l'unique endomorphisme à satisfaire cette égalité. Donc $f = f^*$. $\square$

¹⁵. Et ce même si vous croyez les avoir déjà vu ensemble dans la même pièce.

9.3.1 Opérateur orthogonal, matrice orthogonale

Définition 9.38.

Un opérateur est **orthogonal** lorsque $A^* = A^{-1}$ où A^* est l'adjoint de A défini en 9.29.

Définition 9.39.

Une matrice U est **orthogonale** si $U^t = U^{-1}$. Le **groupe orthogonal** noté $O(n)$ est l'ensemble des matrices orthogonales $n \times n$.

Lemme 9.40.

Soit un opérateur $A: \mathbb{R}^n \rightarrow \mathbb{R}^n$ muni du produit scalaire usuel. Il est orthogonal si et seulement si sa matrice dans la base canonique est orthogonale¹⁶.

Démonstration. Soit la base canonique $\{e_i\}_{i=1,\dots,n}$ de $\mathbb{R}^n$. Nous avons

$$\langle AA^*e_i, e_j \rangle = \langle e_i, e_j \rangle = \delta_{ij}, \quad (9.112)$$

donc $((AA^*)e_i)_j = \delta_{ij}$, ou encore $(AA^*)_{ij} = \delta_{ij}$, ce qui signifie que la matrice AA^* est l'identité. $\square$

Proposition 9.41 (Thème 69).

À propos de matrices orthogonales.

- (1) L'ensemble des matrices réelles orthogonales forme un groupe noté $O(n, \mathbb{R})$.
- (2) Si A est une matrice orthogonale, alors $\det(A) = \pm 1$.
- (3) Le groupe $O(n)$ est le groupe des isométries linéaires¹⁷ de $\mathbb{R}^n$.

Démonstration. Si A et B sont orthogonales, alors

$$(AB)(AB)^t = ABB^tA^t = A\mathbb{1}A^t = \mathbb{1}. \quad (9.113)$$

Vu que $\mathbb{1}$ est orthogonale, nous avons bien un groupe.

En ce qui concerne le déterminant, $AA^t = \mathbb{1}$ donne $\det(A)\det(A^t) = 1$, mais la proposition 9.31 dit que $\det(A) = \det(A^t)$, donc $\det(A)^2 = 1$. D'où le fait que $\det(A) = \pm 1$.

D'autre part si A est une isométrie de $\mathbb{R}^n$ alors pour tout $x, y \in \mathbb{R}^n$ nous avons $\langle Ax, Ay \rangle = \langle x, y \rangle$. En particulier,

$$\langle A^t Ax, y \rangle = \langle x, y \rangle \quad (9.114)$$

pour tout $x, y \in \mathbb{R}^n$. En prenant $y = e_i$ nous trouvons

$$(A^t Ax)_i = x_i, \quad (9.115)$$

ce qui signifie que pour tout x , $A^t Ax = x$, ou encore que $A^t A$ est l'identité.

Réciproquement si $A^t A$ est l'identité nous avons

$$\langle x, y \rangle = \langle A^t Ax, y \rangle = \langle Ax, Ay \rangle, \quad (9.116)$$

ce qui prouve que A est une isométrie. $\square$

En ce qui concerne les valeurs propres des matrices de $O(n)$ ainsi que leurs formes canoniques (avec des fonctions trigonométriques) pour $O(3)$ et $SO(3)$, ce sera pour la proposition 18.195 et ce qui s'ensuit.

Définition 9.42.

Le sous-groupe des matrices orthogonales de déterminant 1 est le groupe **spécial orthogonal** noté $SO(n)$.

16. Définition 9.39.

17. Au sens où, parmi les applications linéaires, les isométries sont les éléments de $O(n)$. À part ça, il y a aussi les translations, mais c'est une autre histoire qui vous sera contée une autre fois.

9.4 Topologie

9.4.1 Boules et sphères

Définition 9.43.

Soit $(V, \|\cdot\|)$, un espace vectoriel normé, $a \in V$ et $r > 0$. Nous allons abondamment nous servir des ensembles suivants :

- (1) la **boule ouverte** $B(a, r) = \{x \in V \text{ tel que } \|x - a\| < r\}$;
- (2) la **boule fermée** $\bar{B}(a, r) = \{x \in V \text{ tel que } \|x - a\| \leq r\}$;
- (3) la **sphère** $S(a, r) = \{x \in V \text{ tel que } \|x - a\| = r\}$.

Les différences entre ces trois ensembles sont très importantes. D'abord, les *boules* sont pleines tandis que la *sphère* est creuse. En comparant à une pomme, la boule ouverte serait la pomme « sans la peau », la boule fermée serait « avec la peau » tandis que la sphère serait seulement la peau. Nous avons

$$\bar{B}(a, r) = B(a, r) \cup S(a, r). \quad (9.117)$$

Définition 9.44.

Une partie A de V est dite **bornée** s'il existe un réel R tel que $A \subset B(0_V, R)$.

Une partie est donc bornée si elle est contenue dans une boule de rayon fini.

Exemple 9.45.

Dans $\mathbb{R}$, les boules sont les intervalles ouverts et fermés tandis que la sphère est donnée par les points extrêmes des intervalles :

$$\begin{aligned} B(a, r) &=]a - r, a + r[, \\ \bar{B}(a, r) &= [a - r, a + r], \\ S(a, r) &= \{a - r, a + r\}. \end{aligned} \quad (9.118)$$

△

Exemple 9.46.

Si nous considérons $\mathbb{R}^2$, la situation est plus riche parce que nous avons plus de normes. Essayons de voir les sphères de centre $(0, 0) \in \mathbb{R}^2$ et de rayon r pour les normes $\|\cdot\|_1$, $\|\cdot\|_2$ et $\|\cdot\|_\infty$.

Pour la norme $\|\cdot\|_1$, la sphère de rayon r est donnée par l'équation

$$|x| + |y| = r. \quad (9.119)$$

Pour la norme $\|\cdot\|_2$, l'équation de la sphère de rayon r est

$$\sqrt{x^2 + y^2} = r, \quad (9.120)$$

et pour la norme supremum, la sphère de rayon r a pour équation

$$\max\{|x|, |y|\} = r. \quad (9.121)$$

Elles sont dessinées sur la figure 9.1

△

Proposition 9.47.

Soient V un espace vectoriel normé, a dans V et x tel que $d(a, x) = r$, c'est-à-dire $x \in S(a, r)$. Dans ce cas, toute boule centrée en x contient un point P tel que $d(P, a) > r$ et un point Q tel que $d(Q, a) < r$.

Démonstration. Soit une boule de rayon δ autour de x . Le but est de trouver un point P tel que $d(P, a) > r$ et $d(P, x) < \delta$. Pour cela, nous prenons P sur la même droite que x (en partant de a), mais juste « un peu plus loin », comme sur la figure suivante :

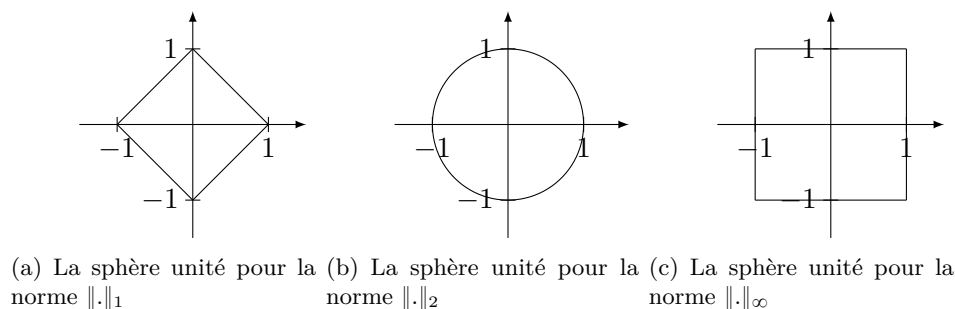
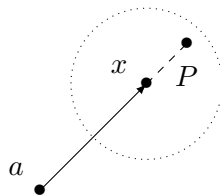


FIGURE 9.1 – Les sphères de rayon 1 pour les trois normes classiques.



Plus précisément, nous considérons le point

$$P = x + \frac{v}{N} \quad (9.122)$$

où $v = x - a$ et N est suffisamment grand pour que $d(x, P)$ soit plus petit que δ . Cela est toujours possible parce que

$$d(P, x) = \|P - x\| = \frac{\|v\|}{N} \quad (9.123)$$

peut être rendu aussi petit que l'on veut par un choix approprié de N . Montrons maintenant que $d(a, P) > d(a, x)$:

$$\begin{aligned} d(a, P) &= \left\| a - x - \frac{v}{N} \right\| \\ &= \left\| a - x + \frac{a}{N} - \frac{x}{N} \right\| \\ &= \left\| \left(1 + \frac{1}{N}\right)(a - x) \right\| \\ &> \|a - x\| = d(a, x). \end{aligned} \quad (9.124)$$

Nous laissons en exercice le soin de trouver un point Q tel que $d(Q, a) < r$ et $d(Q, x) < \delta$. $\square$

9.4.2 Ouverts, fermés, intérieur et adhérence

Définition 9.48.

Soit $(V, \|\cdot\|)$ un espace vectoriel normé et A , une partie de V . Un point a est dit **intérieur** à A s'il existe une boule ouverte centrée en a et contenue dans A .

On appelle **l'intérieur** de A l'ensemble des points qui sont intérieurs à A . Nous notons $\text{Int}(A)$ l'intérieur de A .

Notons que $\text{Int}(A) \subset A$ parce que si $a \in \text{Int}(A)$, nous avons $B(a, r) \subset A$ pour un certain r et en particulier $a \in A$.

Exemple 9.49.

Trouver l'intérieur d'un intervalle dans $\mathbb{R}$ consiste à « ouvrir là où c'est fermé ».

$$(1) \text{Int}([0, 1]) =]0, 1[.$$

Prouvons d'abord que $]0, 1[\subset \text{Int}([0, 1])$. Si $a \in]0, 1[$, alors a est strictement supérieur à 0 et strictement inférieur à 1. Dans ce cas, la boule de centre a et de rayon $\frac{\min\{a, 1-a\}}{2}$ est contenue dans $]0, 1[$ (voir figure 9.2). Cela prouve que a est dans l'intérieur de $[0, 1]$.

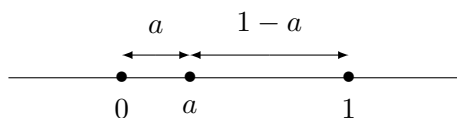


FIGURE 9.2 – Trouver le rayon d’une boule autour de a . Une boule qui serait centrée en a avec un rayon strictement plus petit à la fois de a et de $1 - a$ est entièrement contenue dans le segment $]0, 1[$.

Prouvons maintenant que $\text{Int}([0, 1]) \subset]0, 1[$. Vu que l’intérieur d’un ensemble est inclus dans l’ensemble, nous savons déjà que $\text{Int}([0, 1]) \subset [0, 1]$. Nous devons donc seulement montrer que 0 n’est pas dans l’intérieur de $[0, 1]$. C’est le cas parce que toute boule du type $B(0, r)$ contient le point $-r/2$ qui n’est pas dans $[0, 1]$.

$$(2) \text{Int}([0, \infty[) =]0, \infty[.$$

$$(3) \text{Int}(]2, 3]) =]2, 3[.$$

△

Exemple 9.50.

Les intérieurs des boules et sphères sont importantes à savoir.

- (1) $\text{Int}(B(a, r)) = B(a, r)$. Si $x \in B(a, r)$, nous avons $d(a, x) < r$. Alors la boule $B(x, r - d(x, a))$ est incluse à $B(a, r)$, et donc x est dans l’intérieur de $B(a, r)$. Conseil : faire un dessin.
- (2) $\text{Int}(\bar{B}(a, r)) = B(a, r)$. Par le point précédent, la boule $B(a, r)$ est certainement dans l’intérieur de la boule fermée. Il reste à montrer que les points de $\bar{B}(a, r)$ qui ne sont pas dans $B(a, r)$ ne sont pas dans l’intérieur. Ces points sont ceux dont la distance à a est égale à r . Le résultat découle alors de la proposition 9.47.
- (3) $\text{Int}(S(a, r)) = \emptyset$. Si $x \in S(a, r)$, toute boule centrée en a contient des points qui ne sont pas à distance r de a .

Notez que la sphère est un exemple d’ensemble non vide mais d’intérieur vide.

△

Définition 9.51.

Une partie A de l’espace vectoriel normé $(V, \|\cdot\|)$ est dite **ouverte** si chacun de ses points est intérieur. La partie A est donc ouverte si $A \subset \text{Int}(A)$. Par convention, nous disons que l’ensemble vide $\emptyset$ est ouvert.

Une partie est dite **fermée** si son complémentaire est ouvert. La partie A est donc fermée si $V \setminus A$ est ouvert.

Remarque : un ensemble A est ouvert si et seulement si $\text{Int}(A) = A$.

Définition 9.52.

Une partie A de l’espace vectoriel normé V est dite **compacte** si elle est fermée et bornée.

Nous verrons tout au long de ce cours que les ensembles compacts, et les fonctions définies sur ces ensembles ont de nombreuses propriétés agréables.

Exemple 9.53.

En ce qui concerne les intervalles de $\mathbb{R}$,

- $]1, 2[$ est ouvert ;
- $[3, 4]$ est fermé ;
- $[5, 6[$ n’est ni ouvert ni fermé ;

Les intervalles fermés de $\mathbb{R}$ sont toujours compacts.

△

Proposition 9.54.

Soit V un espace vectoriel normé.

- (1) L'ensemble V lui-même et le vide sont à la fois fermés et ouverts.
- (2) Toute union d'ouverts est ouverte.
- (3) Toute intersection finie d'ouverts est ouverte.
- (4) Le vide et V sont les seules parties de V à être à la fois fermées et ouvertes.

Démonstration. L'ingrédient principal de cette démonstration est que si a est un point d'un ouvert $\mathcal{O}$, alors il existe une boule autour de a contenue dans $\mathcal{O}$ parce que a doit être dans l'intérieur de $\mathcal{O}$.

- (1) Nous avons déjà dit que, par définition, l'ensemble vide est ouvert. Cela implique que V lui-même est fermé (parce que son complémentaire est le vide). De plus, V est ouvert parce que toutes les boules sont incluses à V . Le vide est alors fermé (parce que son complémentaire est V).
- (2) Soit une famille $(\mathcal{O}_i)_{i \in I}$ d'ouverts¹⁸, et l'union

$$\mathcal{O} = \bigcup_{i \in I} \mathcal{O}_i. \quad (9.125)$$

Soit maintenant $a \in \mathcal{O}$. Nous devons prouver qu'il existe une boule centrée en a entièrement contenue dans $\mathcal{O}$. Étant donné que $a \in \mathcal{O}$, il existe $i \in I$ tel que $a \in \mathcal{O}_i$ (c'est-à-dire que a est au moins dans un des $\mathcal{O}_i$). Par hypothèse l'ensemble $\mathcal{O}_i$ est ouvert et donc tous ses points (en particulier a) sont intérieurs; il existe donc une boule $B(a, r)$ centrée en a telle que $B(a, r) \subset \mathcal{O}_i \subset \mathcal{O}$.

- (3) Soit une famille finie d'ouverts $(\mathcal{O}_k)_{k \in \{1, \dots, n\}}$, et $a \in \mathcal{O}$ où

$$\mathcal{O} = \bigcap_{k=1}^n \mathcal{O}_k. \quad (9.126)$$

Vu que a appartient à chaque ouvert $\mathcal{O}_k$, nous pouvons trouver, pour chacun de ces ouverts, une boule $B(a, r_k)$ contenue dans $\mathcal{O}_k$. Chacun des r_k est strictement positif, et nous n'en avons qu'un nombre fini, donc le nombre $r = \min\{r_1, \dots, r_n\}$ est strictement positif. La boule $B(a, r)$ est incluse dans toutes les autres (parce que $B(a, r) \subset B(a, r')$ lorsque $r \leq r'$), par conséquent

$$B(a, r) \subset \bigcap_{k=1}^n B(a, r_k) \subset \bigcap_{k=1}^n \mathcal{O}_k = \mathcal{O}, \quad (9.127)$$

c'est-à-dire que la boule de rayon r est une boule centrée en a contenue dans $\mathcal{O}$, ce qui fait que a est intérieur à $\mathcal{O}$.

- (4) Nous acceptons ce point sans démonstration.

□

La proposition dit que toute intersection *finie* d'ouvert est ouverte. Il est faux de croire que cela se généralise aux intersections infinies, comme le montre l'exemple suivant :

$$\bigcap_{i=1}^{\infty}]-\frac{1}{n}, \frac{1}{n}[= \{0\}. \quad (9.128)$$

Chacun des ensembles $] -\frac{1}{n}, \frac{1}{n}[$ est ouvert, mais le singleton $\{0\}$ est fermé (pourquoi?).

Nous reportons à la proposition 1.323 la preuve du fait que tout ensemble borné de $\mathbb{R}$ possède un infimum et un supremum.

18. L'ensemble I avec lequel nous « numérotions » les ouverts $\mathcal{O}_i$ est *quelconque*, c'est-à-dire qu'il peut être $\mathbb{N}$, $\mathbb{R}$, $\mathbb{R}^n$ ou n'importe quel autre ensemble, fini ou infini.

Définition 9.55.

L'ensemble des ouverts de V est la **topologie** de V . La topologie dont nous parlons ici est dite **induite** par la norme $\|\cdot\|$ de V (parce que cette norme définit la notion de boule et qu'à son tour la notion de boule définit la notion d'ouverts). Un **voisinage** de a dans V est un ensemble contenant un ouvert contenant a .

Il existe de nombreuses topologies sur un espace vectoriel donné, mais certaines sont plus fameuses que d'autres. Dans le cas de $V = \mathbb{R}^n$, la topologie **usuelle** est celle induite par la norme euclidienne. Lorsque nous parlons de boules, de fermés, de voisinages ou d'autres notions topologiques (y compris de convergence, voir plus bas) dans $\mathbb{R}^n$, nous sous-entendons toujours la topologie de la norme euclidienne.

Exemple 9.56.

Les ensembles suivants sont des voisinages de 3 dans $\mathbb{R}$:

- $]1, 5[$;
- $[0, 10]$;
- $\mathbb{R}$.

Les ensembles suivants ne sont pas des voisinages de 3 dans $\mathbb{R}$:

- $]1, 3[$;
- $]1, 3]$;
- $[0, 5] \setminus \{3\}$.

△

Proposition 9.57.

Dans un espace vectoriel normé,

- (1) toute intersection de fermés est fermée ;
- (2) toute union finie de fermés est fermée.

Encore une fois, l'hypothèse de finitude de l'intersection est indispensable comme le montre l'exemple suivant :

$$\bigcup_{n=1}^{\infty} \left[-1 + \frac{1}{n}, 1 - \frac{1}{n}\right] =]-1, 1[. \quad (9.129)$$

Chacun des intervalles dont on prend l'union est fermé tandis que l'union est ouverte.

Définition 9.58.

Soit A , une partie de l'espace vectoriel normé V . Un point $a \in V$ est dit **adhérent** à A dans V si pour tout $\varepsilon > 0$,

$$B(a, \varepsilon) \cap A \neq \emptyset. \quad (9.130)$$

Nous notons $\bar{A}$ l'ensemble des points adhérents à A et nous disons que $\bar{A}$ est l'adhérence de A . L'ensemble $\bar{A}$ sera aussi souvent nommé **fermeture** de l'ensemble A .

Un point peut être adhérent à A sans faire partie de A , et nous avons toujours $A \subset \bar{A}$.

Exemple 9.59.

La terminologie « fermeture » de A pour désigner $\bar{A}$ provient de deux origines.

- (1) L'ensemble $\bar{A}$ est le plus petit fermé contenant A . Cela signifie que si B est un fermé qui contient A , alors $\bar{A} \subset B$. Cela est fondamentalement le sens de la définition 7.24.
- (2) Pour les intervalles dans $\mathbb{R}$, trouver $\bar{A}$ revient à fermer les extrémités qui sont ouvertes, comme on en a parlé dans l'exemple 9.53.

△

Exemple 9.60.

Dans $\mathbb{R}$, l'infimum et le supremum d'un ensemble sont des points adhérents. En effet si M est le supremum de $A \subset \mathbb{R}$, pour tout ε , il existe un $a \in A$ tel que $a > M - \varepsilon$, tandis que $M > a$. Cela fait que $a \in B(M, \varepsilon)$, et en particulier que pour tout rayon ε , nous avons $B(M, \varepsilon) \cap A \neq \emptyset$.

Le même raisonnement montre que l'infimum est également dans l'adhérence de A . $\triangle$

Exemple 9.61.

Il ne faut pas conclure de l'exemple précédent qu'un point limite ou adhérent est automatiquement un minimum ou un maximum. En effet, si nous regardons l'ensemble formé par les points de la suite $x_n = (-1)^n/n$, le nombre zéro est un point adhérent et une limite, mais pas un infimum ni un maximum. $\triangle$

Lemme 9.62.

Si B est une partie fermée de V , alors $B = \bar{B}$.

Démonstration. Supposons qu'il existe $a \in \bar{B}$ tel que $a \notin B$. Alors il n'y a pas d'ouverts autour de a qui soit contenu dans $\complement B$. Cela prouve que $\complement B$ n'est pas ouvert, et par conséquent que B n'est pas fermé. Cela est une contradiction qui montre que tout point de $\bar{B}$ doit appartenir à B lorsque B est fermé. $\square$

Exemple 9.63.

Au niveau des intervalles dans $\mathbb{R}$, prendre l'adhérence consiste à « fermer là où c'est ouvert ». Attention cependant à ne pas fermer l'intervalle en l'infini.

- (1) $\overline{[0, 2[} = [0, 2]$.
- (2) $\overline{]3, \infty[} = [3, \infty[$.

$\triangle$

Proposition 9.64.

Soit V un espace vectoriel normé et $a \in V$. Les trois conditions suivantes sont équivalentes :

- (1) $a \in \bar{A}$;
- (2) il existe une suite d'éléments x_n dans A qui converge vers a ;
- (3) $d(a, A) = 0$.

Notez que dans cette proposition, nous ne supposons pas que a soit dans A .

Proposition 9.65.

Pour toute partie A d'un espace vectoriel normé nous avons

- (1) $V \setminus \bar{A} = \text{Int}(V \setminus A)$,
- (2) $V \setminus \text{Int}(A) = \overline{V \setminus A}$.

En utilisant les notations du complémentaire (1.1.5), les deux points de la proposition se récrivent

- (1) $\complement \bar{A} = \text{Int}(\complement A)$,
- (2) $\complement \text{Int}(A) = \overline{\complement A}$.

Démonstration. Nous avons $a \in V \setminus \bar{A}$ si et seulement si $a \notin \bar{A}$. Or ne pas être dans $\bar{A}$ signifie qu'il existe un rayon ε tel que la boule $B(a, \varepsilon)$ n'intersecte pas A . Le fait que la boule $B(a, \varepsilon)$ n'intersecte pas A est équivalent à dire que $B(a, \varepsilon) \subset V \setminus A$. Or cela est exactement la définition du fait que a est à l'intérieur de $V \setminus A$. Nous avons donc montré que $a \in V \setminus \bar{A}$ si et seulement si $a \in \text{Int}(V \setminus A)$. Cela prouve la première affirmation.

Pour prouver la seconde affirmation, nous appliquons la première au complémentaire de A : $\complement(\bar{A}) = \text{Int}(\complement A)$. En prenant le complémentaire des deux membres nous trouvons successivement

$$\begin{aligned} \complement \complement(\bar{A}) &= \complement \text{Int}(\complement A), \\ \bar{A} &= \complement \text{Int}(A), \end{aligned} \tag{9.131}$$

ce qu'il fallait démontrer. $\square$

Attention à ne pas confondre $\mathbb{C}\bar{A}$ et $\overline{\mathbb{C}A}$. Ces deux ensembles ne sont pas égaux. En effet, en tant que complément d'un fermé, l'ensemble $\mathbb{C}\bar{A}$ est certainement ouvert, tandis que, en tant que fermeture, l'ensemble $\overline{\mathbb{C}A}$ est fermé. Pouvez-vous trouver des exemples d'ensembles A tels que $\mathbb{C}\bar{A} = \overline{\mathbb{C}A}$?

Proposition 9.66.

Soient A et B deux parties de l'espace vectoriel normé V .

- (1) Pour les inclusions, si $A \subset B$, alors $\text{Int}(A) \subset \text{Int}(B)$ et $\bar{A} \subset \bar{B}$.
- (2) Pour les unions, $\overline{A \cup B} = \bar{A} \cup \bar{B}$ et $\overline{A \cap B} \subset \bar{A} \cap \bar{B}$.
- (3) Pour les intersections, $\text{Int}(A) \cap \text{Int}(B) = \text{Int}(A \cap B)$ et $\text{Int}(A) \cup \text{Int}(B) \subset \text{Int}(A \cup B)$.

Démonstration. (1) Si a est dans l'intérieur de A , il existe une boule autour de a contenue dans A . Cette boule est alors contenue dans B et donc est une boule autour de a contenue dans B , ce qui fait que a est dans l'intérieur de B . Si maintenant a est dans l'adhérence de A , toute boule centrée en a contient un élément de A et donc un élément de B , ce qui prouve que a est dans l'adhérence de B .

- (2) Nous avons $A \subset A \cup B$ et donc, en utilisant le premier point, $\bar{A} \subset \overline{A \cup B}$. De la même manière, $\bar{B} \subset \overline{A \cup B}$. En prenant l'union, $\bar{A} \cup \bar{B} \subset \overline{A \cup B}$.

Réciproquement, soit $a \in \overline{A \cup B}$ et montrons que $a \in \bar{A} \cup \bar{B}$. Supposons par l'absurde que a ne soit ni dans $\bar{A}$ ni dans $\bar{B}$. Il existe donc des rayons ε_1 et ε_2 tels que

$$\begin{aligned} B(a, \varepsilon_1) \cap A &= \emptyset, \\ B(a, \varepsilon_2) \cap B &= \emptyset. \end{aligned} \tag{9.132}$$

En prenant $r = \min\{\varepsilon_1, \varepsilon_2\}$, la boule $B(a, r)$ est incluse aux deux boules citées et donc n'intersecte ni A ni B . Donc $a \notin \overline{A \cup B}$, d'où la contradiction.

- (3) Si nous appliquons le second point à $\mathbb{C}A$ et $\mathbb{C}B$, nous trouvons

$$\overline{\mathbb{C}A \cup \mathbb{C}B} = \overline{\mathbb{C}A} \cup \overline{\mathbb{C}B}. \tag{9.133}$$

En utilisant les propriétés du lemme 1.20, le membre de gauche devient

$$\overline{\mathbb{C}A \cup \mathbb{C}B} = \overline{\mathbb{C}(A \cap B)} = \mathbb{C}\text{Int}(A \cap B), \tag{9.134}$$

tandis que le membre de droite devient

$$\overline{\mathbb{C}A} \cup \overline{\mathbb{C}B} = \mathbb{C}\text{Int}(A) \cup \mathbb{C}\text{Int}(B) = \mathbb{C}\left(\text{Int}(A) \cap \text{Int}(B)\right). \tag{9.135}$$

En égalisant le membre de droite de (9.134) avec celui de (9.135) et en passant au complémentaire nous trouvons

$$\text{Int}(A \cap B) = \text{Int}(A) \cap \text{Int}(B), \tag{9.136}$$

comme annoncé.

La dernière affirmation provient du fait que $\text{Int}(A) \subset \text{Int}(A \cup B)$ et de la propriété équivalente pour B . $\square$

Remarque 9.67.

Nous avons prouvé que $\overline{A \cap B} \subset \bar{A} \cap \bar{B}$. Il arrive que l'inclusion soit stricte, comme dans l'exemple suivant. Si nous prenons $A = [0, 1]$ et $B =]1, 2]$, nous avons $A \cap B = \emptyset$ et donc $\overline{A \cap B} = \emptyset$. Par contre nous avons $\bar{A} \cap \bar{B} = \{1\}$.

Définition 9.68.

La **frontière** d'un sous-ensemble A de l'espace vectoriel normé V est l'ensemble des points $a \in V$ tels que

$$\begin{aligned} B(a, r) \cap A &\neq \emptyset, \\ B(a, r) \cap \complement A &\neq \emptyset, \end{aligned} \quad (9.137)$$

pour tout rayon r . En d'autres termes, toute boule autour de a contient des points de A et des points de $\complement A$. La frontière de A se note ∂A .

Proposition 9.69.

La frontière d'une partie A d'un espace vectoriel normé V s'exprime sous la forme

$$\partial A = \bar{A} \setminus \text{Int}(A). \quad (9.138)$$

Démonstration. Le fait pour un point a de V d'appartenir à $\bar{A}$ signifie que toute boule centrée en a intersecte A . De la même façon, le fait de ne pas appartenir à $\text{Int}(A)$ signifie que toute boule centrée en a intersecte $\complement A$. $\square$

La description de la frontière donnée par la proposition 9.69 est celle qu'en pratique nous utilisons le plus souvent. Dans certains textes, elle est prise comme définition de la frontière.

Lemme 9.70.

La frontière de A peut également s'exprimer des façons suivantes :

$$\partial A = \bar{A} \cap \complement \text{Int}(A) = \bar{A} \cap \overline{\complement A}, \quad (9.139)$$

Démonstration. En partant de $\partial A = \bar{A} \setminus \text{Int}(A)$, la première égalité est une application de la propriété (2) du lemme 1.20. La seconde égalité est alors la proposition 9.65. $\square$

Exemple 9.71.

Dans $\mathbb{R}$, la frontière d'un intervalle est la paire constituée des points extrêmes. En effet

$$\partial[a, b[= \overline{[a, b[} \setminus \text{Int}([a, b[) = [a, b] \setminus]a, b[= \{a, b\}. \quad (9.140)$$

Toujours dans $\mathbb{R}$ nous avons

$$\partial\mathbb{R} = \bar{\mathbb{R}} \setminus \text{Int}(\mathbb{R}) = \mathbb{R} \setminus \mathbb{R} = \emptyset, \quad (9.141)$$

et

$$\partial\mathbb{Q} = \bar{\mathbb{Q}} \setminus \text{Int}(\mathbb{Q}) = \mathbb{R} \setminus \emptyset = \mathbb{R}. \quad (9.142)$$

$\triangle$

Exemple 9.72.

Dans $\mathbb{R}^n$, nous avons

$$\partial B(a, r) = \partial \bar{B}(a, r) = S(a, r). \quad (9.143)$$

Cela est un boulot pour la proposition 9.47. Si $x \in S(a, r)$ alors toute boule autour de x contient des points à distance strictement plus grande et plus petite que $d(a, x)$, c'est-à-dire des points dans $B(a, r)$ et hors de $B(a, r)$. Cela prouve que les points de $S(a, r)$ font partie de $\partial B(a, r)$, c'est-à-dire que $S(a, r) \subset \partial B(a, r)$; et idem pour $\bar{B}(a, r)$.

Pour prouver l'inclusion inverse, soit $x \in \partial B(a, r)$. Vu que toute boule autour de x contient des points intérieurs à $B(a, r)$, pour tout $\epsilon > 0$, $d(a, x) - \epsilon < r$, c'est-à-dire que $d(a, x) \leq r$. De la même manière toute boule autour de x contient des points hors de $B(a, r)$ signifie que pour tout ϵ , $d(a, x) + \epsilon > r$ ou encore que $d(a, x) \geq r$. Nous avons donc $d(a, x) = r$. $\triangle$

Remarque 9.73.

Il serait toutefois faux de croire que $\partial A = \partial \bar{A}$ pour toute partie A de $\mathbb{R}^n$. En effet si $A = \mathbb{R} \setminus \{0\}$ nous avons $\partial A = \{0\}$ et $\bar{A} = \mathbb{R}$, donc $\partial \bar{A} = \emptyset$.

9.4.3 Point isolé, point d'accumulation

Lemme 9.74.

Soit un espace vectoriel normé V ainsi qu'une partie D de V .

(1) Un point $a \in D$ est dit isolé¹⁹ dans D relativement à V s'il existe un $\varepsilon > 0$ tel que

$$B(a, \varepsilon) \cap D = \{a\}. \quad (9.144)$$

(2) Un point $a \in V$ point d'accumulation²⁰ de D si pour tout $\varepsilon > 0$,

$$(B(a, \varepsilon) \setminus \{a\}) \cap D \neq \emptyset. \quad (9.145)$$

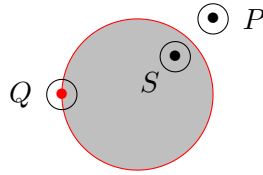


FIGURE 9.3 – L'ensemble décrit par l'équation (9.146). Le point P est un point isolé de D , tandis que les points S et Q sont des points d'accumulation.

Exemple 9.75.

Considérons la partie suivante de $\mathbb{R}^2$:

$$D = \{(x, y) \text{ tel que } x^2 + y^2 < 1\} \cup \{(1, 1)\}. \quad (9.146)$$

Comme on peut le voir sur la figure 9.3, le point $P = (1, 1)$ est un point isolé de D parce qu'on peut tracer une boule autour de P sans inclure d'autres points de D que P lui-même. Le point $Q = (-1, 0)$ est un point d'accumulation de D parce que toute boule autour de Q contient des points de D .

Le point S , étant un point intérieur, est un point d'accumulation : toute boule autour de S intersecte D .

Notez cependant que le point Q lui-même n'est pas dans D parce que l'inégalité qui définit D est stricte. $\triangle$

Remarque 9.76.

À propos de la position des points d'accumulation et des points isolés.

- (1) Les points intérieurs sont tous des points d'accumulation.
- (2) Les points isolés ne sont jamais intérieurs.
- (3) Certains points d'accumulation ne font pas partie de l'ensemble. Par exemple le point 1 est un point d'accumulation de $E =]0, 1[$.
- (4) Les points de la frontière sont soit d'accumulation soit isolés.

Exemple 9.77.

Tous les points de $\mathbb{R}$ sont des points d'accumulation de $\mathbb{Q}$ parce que dans toute boule autour d'un réel, on peut trouver un nombre rationnel. $\triangle$

Remarque 9.78.

L'ensemble des points d'accumulation d'un ensemble n'est pas exactement son adhérence. En effet, un point isolé dans A est dans l'adhérence de A , mais n'est pas un point d'accumulation de A .

19. Définition 7.30.

20. Définition 7.29.

9.4.4 Des exemples

Exemple 9.79.

Nous considérons l'ensemble.

$$A_1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 - 5x + 6 < y \leq 2\}. \quad (9.147)$$

Si un point $(x, y) \in \mathbb{R}^2$ est tel que $x^2 - 5x + 6 < y$, alors dans une boule centrée en (x, y) (de rayon r_1), l'inégalité reste vraie (parce que la fonction $x^2 - 5x + 6 - y$ est une fonction continue). De la même manière, si nous avons $y < 2$ en (x, y) , alors nous avons encore l'inégalité dans une boule de rayon r_2 . En prenant $r = \min\{r_1, r_2\}$, les deux inégalités restent vraies dans la boule de rayon r .

Donc les points (x, y) tels que $x^2 - 5x + 6 < y < 2$ sont dans l'intérieur de A_1 .

Pour les mêmes raisons, autour d'un point (x, y) tel que $x^2 - 5x + 6 > y$, nous pouvons trouver une boule dans laquelle l'inégalité reste stricte. Ces points ne sont donc pas dans l'adhérence de A_1 . Un point qui vérifie $x^2 - 5x + 6 = y = 2$ est par contre dans l'adhérence parce que dans toute boule, on pourra trouver un x tel que $x^2 - 5x + 6 < y$, et un y . L'adhérence est donc donnée par les inéquations

$$\bar{A}_1 \equiv x^2 - 5x + 6 \leq y \leq 2. \quad (9.148)$$

La frontière est donnée par les points de l'adhérence qui ne sont pas dans l'intérieur de A_1 . Attention : **ne pas dire** que la frontière est alors donnée simplement en remplaçant les inégalités par des égalités : $\partial A_1 \equiv x^2 - 5x + 6 = y = 2$. Quel est cet ensemble ?

Trouver la frontière demande un peu plus de travail. Le point marqué sur la figure 9.4 est sur la frontière parce que toute boule intersecte l'intérieur et l'extérieur. Cela est dû au fait que, sur ce point, nous ayons $x^2 - 5x + 6 = y$ en même temps que $y < 2$. Donc si on prend une boule assez petite, on conserve $y < 2$, mais on obtient des points tels que $x^2 - 5x + 6 < y$.

En voyant le dessin, la chose à faire pour écrire la frontière est de trouver les deux points d'intersection entre la parabole et la droite horizontale. Ces points sont les points (x, y) qui satisfont au système

$$\begin{cases} x^2 - 5x + 6 = y \\ y = 2. \end{cases} \quad (9.149a)$$

$$(9.149b)$$

En substituant la seconde équation dans la première, il vient $x^2 - 5x + 6 = 2$, ce qui nous donne à résoudre le polynôme du second degré $x^2 - 5x + 4 = 0$. Les éventuelles solutions entières sont les diviseurs de 4. Par chance²¹, on voit que $x = 1$ et $x = 4$ sont des solutions. Le théorème 3.143 nous assure qu'il n'y a pas d'autres racines. Les deux points d'intersection sont les points $P = (1, 2)$ et $Q = (4, 2)$. Les points de la frontière de A_1 sont donc donnés par

$$\begin{aligned} \partial A_1 = \{ & (x, y) \in \mathbb{R}^2 \text{ tels que } x^2 - 5x + 6 = y \text{ et } 1 \leq x \leq 4 \} \\ & \cup \{ (x, y) \in \mathbb{R}^2 \text{ tels que } y = 2 \text{ et } 1 \leq x \leq 4 \}. \end{aligned} \quad (9.150)$$

Notez que les points de la parabole qui sont sur la frontière ne font pas partie de l'ensemble A_1 lui-même, tandis que ceux de la frontière qui sont sur la droite horizontale en font partie sauf $(4, 2)$ et $(1, 2)$.

L'intérieur de A_1 n'étant pas égal à A_1 , cet ensemble n'est pas ouvert ; de la même manière, vu que $\bar{A}_1 \neq A_1$, l'ensemble n'est pas fermé. L'ensemble A_1 est par contre borné parce qu'il est contenu par exemple dans la boule de centre $(0, 0)$ et de rayon 5. Les points d'accumulation de A_1 sont les points de sa fermeture. $\triangle$

Exemple 9.80.

Nous étudions

$$A_2 = \{(x, y) \in \mathbb{R}^2 \mid x + 1 < y < 2x\}. \quad (9.151)$$

Pour les mêmes raisons que dans l'exemple 9.79 l'intérieur est donné par

$$\text{Int}(A_2) \equiv x + 1 < y < 2x; \quad (9.152)$$

21. Sinon, il aurait fallu utiliser la proposition 10.95.

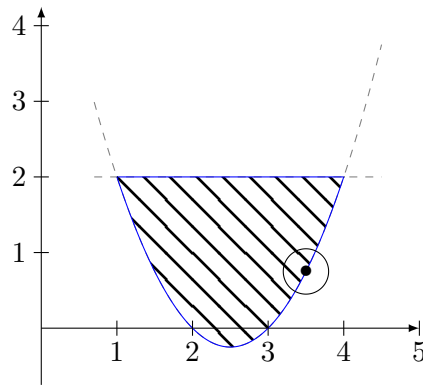


FIGURE 9.4 – En hachuré : l'intérieur ; en trait plein : la frontière. L'adhérence est l'union des deux. Exemple 9.79.

L'adhérence est donnée par

$$\overline{A_2} \equiv x + 1 \leq y \leq 2x, \quad (9.153)$$

Pour la frontière, les deux droites dont il est question dans la définition de A_2 (les droites $y = x + 1$ et $y = 2x$) se coupent en $x = 1$ (refaire soi-même le dessin de la figure 9.5). Lorsque $x < 1$, les conditions $x + 1 < y$ et $y < 2x$ sont incompatibles : aucun point de A_2 n'est dans la partie $x < 1$ du plan. Lorsque $x > 1$, alors les points situés *entre* les deux droites font partie de A_2 . La frontière est donc donnée par ces deux droites pour $x \geq 1$.

Étant donné que $\text{Int}(A_2) = A_2$, cet ensemble est ouvert (et donc pas fermé par la proposition 9.54(4)). Il n'est par contre pas borné parce qu'il contient des points (x, y) avec des x arbitrairement grands. $\triangle$

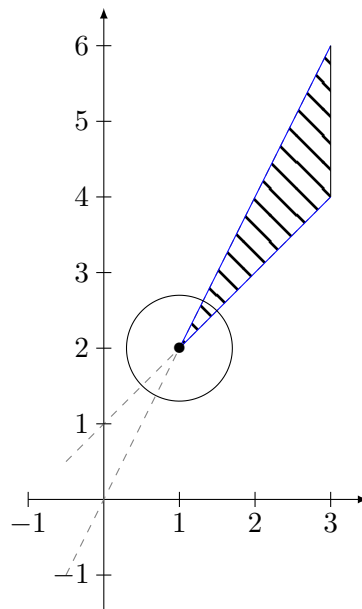


FIGURE 9.5 – Notez que le point d'angle fait partie de la frontière, mais pas de l'ensemble. Exemple 9.80.

Proposition 9.81 ([199]).

Tout partie de $\mathbb{R}$ sans point d'accumulation est dénombrable.

Démonstration. Soit une partie S de $\mathbb{R}$ ne contenant pas de points d'accumulation. Pour chaque $s \in S$, il existe un $\epsilon_s > 0$ tel que

$$B(s, \epsilon_s) \cap S = \{s\}. \quad (9.154)$$

Rien ne garantit cependant que $B(s, \epsilon_s) \cap B(t, \epsilon_t) = \emptyset$, alors que nous en aurons besoin pour la suite.

Le nombre

$$\inf\{|s - v| \text{ tel que } v \in S \setminus \{s\}\} \quad (9.155)$$

est au moins égal à ϵ_s et est donc strictement positif. Nous posons

$$r_s = \frac{\inf\{|s - v| \text{ tel que } v \in S \setminus \{s\}\}}{4}, \quad (9.156)$$

et

$$I_s = B(s, r_s). \quad (9.157)$$

Nous avons maintenant $I_s \cap I_t = \emptyset$. Soit en effet $u \in I_s \cap I_t$. Alors

$$|s - t| \leq |s - u| + |u - t| \quad (9.158a)$$

$$\leq r_s + r_t \quad (9.158b)$$

$$\leq 2r_s \quad (9.158c)$$

où nous avons supposé $r_s \geq r_t$. Si ce n'est pas le cas, changer s et t dans ce qui suit ; les deux points ont des rôles symétriques. Nous avons donc

$$|s - t| \leq 2r_s = \frac{\inf\{|s - v| \text{ tel que } v \in S \setminus \{s\}\}}{2} \leq \frac{|s - t|}{2}. \quad (9.159)$$

Donc $|s - t| = 0$ et $s = t$.

Cela pour dire que I_s ne possède d'intersection avec I_t que si $s = t$.

Nous définissons alors une application

$$\begin{aligned} \varphi: S &\rightarrow \mathbb{Q} \\ s &\mapsto q_s \end{aligned} \quad (9.160)$$

où q_s est un choix de rationnel dans I_s . C'est le lemme 1.307 qui nous permet de choisir un tel rationnel.

La construction des intervalles I_s garantit que φ est une injection. Le fait qu'il existe une injection de $\mathbb{Q}$ vers S et le fait que $\mathbb{Q}$ est dénombrable impliquent que S est au plus dénombrable. $\square$

9.5 Valeur propre et vecteur propre

9.5.1 Généralités

Nous savons qu'une application *linéaire* $A: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ est complètement définie par la donnée de son action sur les trois vecteurs de base, c'est-à-dire par la donnée de

$$Ae_1, Ae_2 \text{ et } Ae_3. \quad (9.161)$$

Nous allons former la matrice de A en mettant simplement les vecteurs Ae_1 , Ae_2 et Ae_3 en colonne. Donc la matrice

$$A = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad (9.162)$$

signifie que l'application linéaire A envoie le vecteur e_1 sur $\begin{pmatrix} 3 \\ 0 \\ 0 \end{pmatrix}$, le vecteur e_2 sur $\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$ et le vecteur e_3 sur $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$. Pour savoir comment A agit sur n'importe quel vecteur, on applique la règle

de produit vecteur $\times$ matrice :

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x + 2y + 3z \\ 4x + 5y + 6z \\ 7x + 8y + 9z \end{pmatrix}. \quad (9.163)$$

Une chose intéressante est de savoir quelles sont les directions invariantes de la transformation linéaire. Par exemple, on peut lire sur la matrice (9.162) que la direction $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ est invariante : elle est simplement multipliée par 3. Dans cette direction, la transformation est juste une dilatation. Afin de savoir si v est un vecteur d'une direction conservée, il faut voir s'il existe un nombre λ tel que $Av = \lambda v$, c'est-à-dire voir si v est simplement dilaté.

L'équation $Av = \lambda v$ se réécrit $(A - \lambda \mathbb{1})v = 0$, c'est-à-dire qu'il faut résoudre l'équation

$$(A - \lambda \mathbb{1}) \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}. \quad (9.164)$$

Nous savons qu'une telle équation ne peut avoir de solutions que si $\det(A - \lambda \mathbb{1}) = 0$. La première étape est donc de trouver les λ qui vérifient cette condition.

9.5.2 Dans le vif du sujet

Définition 9.82.

Soit un $\mathbb{K}$ -espace vectoriel E et un endomorphisme $A: V \rightarrow V$. Un **vecteur propre** de A est un vecteur $v \neq 0$ tel que $Av = \lambda v$ pour un certain $\lambda \in \mathbb{K}$. Dans ce cas, λ est la **valeur propre** de v .

L'espace propre de A pour la valeur λ ²² est l'ensemble des vecteurs propres de A pour la valeur propre λ et zéro.

Définition 9.83.

L'ensemble de valeurs propres de l'endomorphisme u est son **spectre** et est noté $\text{Spec}(u)$.

Remarque 9.84.

Le nombre zéro peut être une valeur propre ; c'est le vecteur zéro qui ne peut pas être vecteur propre. La matrice nulle est une matrice diagonalisable.

Lemme 9.85.

Soient un espace vectoriel E , un endomorphisme $u \in \text{End}(E)$, ainsi que ses sous-espaces propres $\{E_\lambda\}_{\lambda \in \text{Spec}(u)}$. Toute somme finie de la forme

$$E_{\lambda_1} + \dots + E_{\lambda_p} \quad (9.165)$$

est directe²³

Démonstration. Nous utilisons le lemme 4.150. Soient $v_i \in V_{\lambda_i}$ un choix de vecteurs tels que

$$\sum_{i=1}^p v_i = 0. \quad (9.166)$$

Soit un entier j entre 1 et p . Nous allons montrer que $v_j = 0$. Pour cela nous remarquons d'abord que

$$\prod_{k \neq j} (\lambda_i - \lambda_k) = 0 \quad (9.167)$$

22. Nous laissons au lecteur le soin de vérifier que c'est bien un sous-espace vectoriel de E .

23. Définition 4.149.

dès que $i \neq j$. Nous appliquons l'opérateur $\prod_{k \neq j} (A - \lambda_k \mathbb{1})$ à l'égalité (9.166) :

$$0 = \sum_{i=1}^p \prod_{k \neq j} (A - \lambda_k) v_i \quad (9.168a)$$

$$= \sum_{i=1}^p \prod_{k \neq j} (\lambda_i - \lambda_k) v_i \quad (9.168b)$$

$$= \prod_{k \neq j} (\lambda_j - \lambda_k) v_j. \quad (9.168c)$$

Justifications.

- Pour (9.168b). Pour chaque k et i nous avons $(A - \lambda_k)v_i = Av_i - \lambda_k v_i = \lambda_i v_i - \lambda_k v_i$ parce que v_i est un vecteur propre de A pour la valeur propre λ_i .
- Pour (9.168c). Dans la somme, seul le terme $i = j$ est non nul, à cause de (9.167).

Donc $v_j = 0$ parce que le produit $\prod_{k \neq j} (\lambda_j - \lambda_k)$, lui, est non nul. $\square$

Proposition 9.86 ([200]).

Soit E , un espace vectoriel sur un corps infini et $(F_k)_{k=1, \dots, r}$, des sous-espaces vectoriels propres²⁴ de E tels que $\bigcup_{i=1}^r F_i = E$. Alors $E = F_k$ pour un certain k .

Autrement dit, l'union finie de sous-espaces propres ne peut être égal à l'espace complet.

9.6 Polynômes d'endomorphismes

Soit A un anneau commutatif et $\mathbb{K}$, un corps commutatif. L'injection canonique $A \rightarrow A[X]$ se prolonge en une injection

$$\mathbb{M}(A) \rightarrow \mathbb{M}(A[X]). \quad (9.169)$$

9.6.1 Polynômes d'endomorphismes

Soit $u \in \text{End}(E)$ où E est un $\mathbb{K}$ -espace vectoriel. Nous considérons l'application

$$\begin{aligned} \varphi_u: \mathbb{K}[X] &\rightarrow \text{End}(E) \\ P &\mapsto P(u). \end{aligned} \quad (9.170)$$

L'image de φ_u est un sous-espace vectoriel. En effet si $A = \varphi_u(P)$ et $B = \varphi_u(Q)$, alors $A + B = \varphi_u(P + Q)$ et $\lambda A = (\lambda P)(u)$. En particulier c'est un espace fermé.

Soit u un endomorphisme d'un $\mathbb{K}$ -espace vectoriel E et P , un polynôme. Nous disons que P est un polynôme **annulateur** de u si $P(u) = 0$ en tant que endomorphisme de E .

Lemme 9.87.

Si P et Q sont des polynômes dans $\mathbb{K}[X]$ et si u est un endomorphisme d'un $\mathbb{K}$ -espace vectoriel E , nous avons

$$(PQ)(u) = P(u) \circ Q(u). \quad (9.171)$$

Démonstration. Si $P = \sum_i a_i X^i$ et $Q = \sum_j b_j X^j$, alors le coefficient de X^k dans PQ est

$$\sum_l a_l b_{k-l}. \quad (9.172)$$

Par conséquent $(PQ)(u)$ contient $\sum_l a_l b_{k-l} u^k$. Par ailleurs $P(u) \circ Q(u)$ est donné par

$$\sum_i a_i u^i \left(\sum_j b_j u^j \right) (x) = \sum_{ij} a_i b_j u^{i+j}(x). \quad (9.173)$$

Le coefficient du terme en u^k est bien le même que celui donné par (9.172). $\square$

24. Définition 9.82.

Théorème 9.88 (Décomposition des noyaux ou lemme des noyaux).

Soit u un endomorphisme du $\mathbb{K}$ -espace²⁵ vectoriel E . Soit $P \in \mathbb{K}[X]$ un polynôme tel que $P(u) = 0$. Nous supposons que P s'écrit comme le produit $P = P_1 \dots P_n$ de polynômes deux à deux étrangers²⁶. Alors

$$E = \ker P_1(u) \oplus \dots \oplus \ker P_n(u). \quad (9.174)$$

De plus les projecteurs associés à cette décomposition sont des polynômes en u .

Démonstration. Dans ce qui suit, nous allons beaucoup utiliser le fait que $\mathbb{K}[X]$ soit commutatif (lemme 1.244). Nous posons

$$Q_i = \prod_{j \neq i} P_j. \quad (9.175)$$

Par le lemme 6.44 ces polynômes sont étrangers entre eux et le théorème de Bézout (théorème 6.43) donne l'existence de polynômes R_i tels que

$$R_1 Q_1 + \dots + R_n Q_n = 1. \quad (9.176)$$

Si nous appliquons cette égalité à u et ensuite à $x \in E$ nous trouvons

$$\sum_{i=1}^n (R_i Q_i)(u)(x) = x, \quad (9.177)$$

et en particulier si nous posons $E_i = \text{Image}(P_i Q_i(u))$ nous avons

$$E = \sum_{i=1}^n E_i. \quad (9.178)$$

Cette dernière somme n'est éventuellement pas une somme directe. Si $i \neq j$, alors $Q_i Q_j$ est multiple de P ; plus précisément, en utilisant la commutativité de $\mathbb{K}[X]$,

$$Q_i P_j = \prod_{k \neq i} P_k \prod_{l \neq j} P_l = \prod_{\substack{k \neq i \\ k \neq j}} P_k \prod_k P_l = S_{ij} P \quad (9.179)$$

où S_{ij} est un polynôme. Toujours avec $i \neq j$, en utilisant le lemme 9.87 ainsi que la commutativité de $\mathbb{K}[X]$ ²⁷,

$$(R_i Q_i)(u) \circ (R_j Q_j)(u) = (R_i Q_i R_j Q_j)(u) = (R_i R_j \underbrace{Q_i Q_j}_{=S_{ij}P})(u) = (R_i R_j S_{ij})(u) \circ P(u) = 0 \quad (9.180)$$

Nous pouvons voir E comme un $\mathbb{K}$ -module et appliquer le théorème 1.225. Les opérateurs $R_i Q_i(u)$ ont l'identité comme somme et sont orthogonaux, et nous avons donc la décomposition en somme directe :

$$E = \bigoplus_{i=1}^n R_i Q_i(u) E. \quad (9.181)$$

Afin de terminer la preuve, nous devons montrer que $R_i Q_i(u) E = \ker P_i(u)$. D'abord nous avons

$$P_i R_i Q_i(u) = (R_i P)(u) = R_i(u) \circ P(u) = 0, \quad (9.182)$$

par conséquent $\text{Image}(R_i Q_i(u)) \subset \ker P_i(u)$. Pour obtenir l'inclusion inverse, nous reprenons l'équation (9.177) avec $x \in \ker P_i(u)$. Elle se réduit à

$$(R_i Q_i)(u)x = x. \quad (9.183)$$

Par conséquent $x \in \text{Image}(R_i Q_i(u))$. □

25. Le corps $\mathbb{K}$ est commutatif comme tous les corps dans le Frido.

26. Définition 3.128.

27. Lemme 1.244.

9.89.

Ce résultat est utilisé pour prouver que toute représentation est décomposable en représentations irréductibles, proposition 16.9 ainsi que pour le théorème 9.129 qui dit que si le polynôme minimal d'un endomorphisme est scindé à racine simple alors il est diagonalisable.

Corolaire 9.90.

Soit E , un $\mathbb{K}$ -espace vectoriel de dimension finie et f , un endomorphisme semi-simple dont la décomposition du polynôme minimal μ_f en facteurs irréductibles sur $\mathbb{K}[X]$ est $\mu_f = M_1^{\alpha_1} \cdots M_r^{\alpha_r}$. Si F est un sous-espace stable par f , alors

$$F = \bigoplus_{i=1}^r \ker M_i^{\alpha_i}(f) \cap F \quad (9.184)$$

Démonstration. Nous posons $E_i = \ker M_i^{\alpha_i}(f)$ et $F_i = E_i \cap F$. Les polynômes $M_i^{\alpha_i}$ sont deux à deux étrangers et $\mu_f(f) = 0$, donc le lemme des noyaux (9.88) s'applique et

$$E = E_1 \oplus \cdots \oplus E_r. \quad (9.185)$$

Nous pouvons décomposer $x \in F$ en termes de cette somme :

$$x = x_1 + \cdots + x_r \quad (9.186)$$

avec $x_i \in E_i$. Toujours selon le lemme des noyaux, les projections sur les espaces E_i sont des polynômes en f . Par conséquent F est stable sous toutes ces projections $\text{proj}_i: E \rightarrow E_i$, et en appliquant proj_i à (9.186), $\text{proj}_i(x) = x_i$. Vu que $x \in F$, le membre de gauche est encore dans F et $x_i \in E_i \cap F$. Nous avons donc

$$F \subset \bigoplus_{i=1}^r F_i. \quad (9.187)$$

L'inclusion inverse est immédiate parce que $F_i \subset F$ pour chaque i . □

Lemme 9.91.

Si x est un vecteur propre de valeur propre λ pour l'endomorphisme u et si P est un polynôme, alors x est vecteur propre de u pour la valeur propre $P(\lambda)$.

Démonstration. C'est un simple calcul de $P(u)x$ en ayant noté $P(X) = \sum_{k=0}^n c_k X^k$:

$$P(u)x = \sum_{k=0}^n c_k u^k(x) = \sum_{k=0}^n c_k \lambda^k u = P(\lambda)x. \quad (9.188)$$

□

9.6.2 Polynôme minimal et minimal ponctuel**Lemme 9.92.**

Soit un endomorphisme $f: E \rightarrow E$ d'un $\mathbb{K}$ -espace vectoriel de dimension finie. Il existe un unique polynôme annulateur normalisé de degré minimum.

Tout endomorphisme de $\mathbb{K}$ -espace vectoriel de dimension finie possède un polynôme minimal²⁸.

Démonstration. Pour l'unicité, soient P et Q deux polynômes annulateur de f de même degré N et ayant tous deux 1 comme coefficient de x^N . Alors $P - Q$ est de degré $N - 1$ tout en étant encore annulateur.

Pour l'existence, les endomorphismes Id , f , f^2 , $\dots$ ne peuvent pas être tous linéairement indépendants parce que la dimension de $\text{End}(E)$ est finie. Il existe donc un nombre N et des coefficients a_k tels que $\sum_{k=0}^N a_k f^k = 0$. Le polynôme $P(X) = \sum_{k=0}^N a_k X^k$ est donc annulateur de f .

28. Définition 6.59.

Une autre façon de le dire est que l'application linéaire $\varphi: \mathbb{K}[X] \rightarrow \text{End}(E)$ donnée par $\varphi(P) = P(f)$ est un endomorphisme d'un espace vectoriel de dimension infinie vers un espace vectoriel de dimension finie. Il ne peut donc pas être injectif et possède donc un noyau non réduit à zéro.

L'existence d'un polynôme minimal est maintenant seulement le fait que, avec les notations de la définition 6.59, l'idéal I_f n'est pas réduit à $\{0\}$. $\square$

Remarque 9.93.

La preuve donnée ci-dessus montre que $\deg(\mu) \leq \dim(E)^2$. Comme conséquence du théorème de Caley-Hamilton 9.116 nous verrons qu'en réalité le degré du polynôme minimal est majoré par la dimension de l'espace.

Exemple 9.94 (Pas en dimension infinie).

L'endomorphisme de dérivation $\triangle$

Dans la suite, l'endomorphisme f du $\mathbb{K}$ -espace vectoriel E de dimension n est fixé. Pour $x \in E$ nous notons

$$E_x = \{P(f)x \text{ tel que } P \in \mathbb{K}[X]\}. \quad (9.189)$$

Nous considérons le morphisme d'algèbres

$$\begin{aligned} \varphi: \mathbb{K}[X] &\rightarrow \text{End}(E) \\ P &\mapsto P(f) \end{aligned} \quad (9.190)$$

et si $x \in E$ est donné nous considérons le morphisme de $\mathbb{K}$ -espaces vectoriels

$$\begin{aligned} \varphi_x: \mathbb{K}[X] &\rightarrow E \\ P &\mapsto P(f)x. \end{aligned} \quad (9.191)$$

Les noyaux de ces applications sont des idéaux, entre autres par le lemme 9.87. Ils ont donc un unique générateur unitaire (chacun) par le théorème 6.39. En termes de vocabulaire, l'ensemble

$$\ker(\phi) = \{Q \in \mathbb{K}[X] \text{ tel que } Q(f) = 0\} \quad (9.192)$$

est l'**idéal annulateur** de f et un polynôme Q tel que $Q(f) = 0$ est un polynôme annulateur de f .

Définition 9.95.

Le générateur unitaire de $\ker(\varphi_x)$ est le **polynôme minimal ponctuel** de f en x . Il sera noté $\mu_{f,x}$ ou μ_x lorsque la dépendance en f est claire dans le contexte.

Nous notons μ le générateur unitaire du noyau de φ et μ_x celui de φ_x . Vu que $\mu \in \ker(\varphi_x)$ pour tout x nous avons $\mu_x \mid \mu$ pour tout x .

Exemple 9.96 (Pas en dimension infinie).

En dimension infinie, il n'y a pas toujours de polynôme annulateur. Si E est un espace vectoriel de dimension infinie ayant une base dénombrable $\{e_i\}_{i \in \mathbb{N}}$ alors l'opérateur donné par $f(e_i) = e_{i+1}$ n'a pas de polynôme annulateur. Même pas ponctuel en quel que point que ce soit.

De même l'opérateur donné par $g(e_1) = 0$ et $g(e_i) = e_{i-1}$ si $i \neq 1$ n'a pas de polynôme annulateur, mais il a un polynôme annulateur ponctuel évident en $x = e_1$. L'exemple 15.79 donnera un habillage à peine subtil à cet exemple. $\triangle$

Proposition 9.97.

Si P est un polynôme tel que $P(f) = 0$, alors le polynôme minimal μ_f divise P . Autrement dit, le polynôme minimal engendre l'idéal des polynômes annulateurs.

Démonstration. L'ensemble $\ker(\varphi) = \{Q \in \mathbb{K}[X] \text{ tel que } Q(f) = 0\}$ est un idéal par le lemme 9.87. Le polynôme minimal de u est un élément de degré plus bas dans I et par conséquent $I = (\mu_u)$ par le théorème 6.39. Nous concluons que μ_u divise tous les éléments de I . $\square$

La proposition suivante permet de caractériser le polynôme minimal.

Proposition 9.98 ([101]).

Soit une application linéaire f sur un $\mathbb{K}$ -espace vectoriel. Il existe un unique polynôme unitaire²⁹ $P \in \mathbb{K}[X]$ tel que

- (1) $P(f) = 0$;
- (2) l'application

$$\begin{aligned} \varphi: \frac{\mathbb{K}[X]}{(P)} &\rightarrow \text{End}(E) \\ \bar{Q} &\mapsto Q(f) \end{aligned} \quad (9.193)$$

est injective.

Démonstration. En ce qui concerne l'existence, il existe le polynôme minimal de f qui satisfait les conditions. Pour l'unicité nous travaillons maintenant.

Supposons que l'application (9.193) soit injective. Alors pour tout $Q \in \mathbb{K}[X]$ tel que $Q(f) = 0$ nous avons $\bar{Q} = 0$, c'est-à-dire $Q = PR$ pour un certain $R \in \mathbb{K}[X]$. Autrement dit : P est un générateur unitaire de l'idéal annulateur de f . Le théorème 6.39(3) nous dit alors que $P = \mu$ parce que μ est également générateur unitaire. $\square$

Lemme 9.99 ([201]).

Soit $f: E \rightarrow E$ un endomorphisme de l'espace vectoriel E . Il existe un élément $x \in E$ tel que $\mu_{f,x} = \mu_f$.

Démonstration. Soit une décomposition en irréductibles du polynôme minimal $\mu = P_1^{\alpha_1} \dots P_r^{\alpha_r}$. Nous notons $E_i = \ker(P_i^{\alpha_i}(f))$. Les polynômes P_i sont étrangers deux à deux (un diviseur commun aurait a fortiori été un diviseur et aurait contredit l'irréductibilité). Le lemme des noyaux 9.88 nous donne la somme directe

$$E = \bigoplus_{i=1}^r \ker(P_i^{\alpha_i}(f)). \quad (9.194)$$

Si $x_i \in E_i$ alors μ_{x_i} est une puissance de P_i . En effet $\mu_{x_i} \mid \mu$ et est donc un produit des puissances des P_j . Or si $(QP_j)(f)x_i = 0$ alors $(P_jQ)(f)x_i = 0$, ce qui donne $Q(f)x_i \in E_j \cap E_i = \{0\}$. Donc μ_{x_i} n'est pas de la forme QP_j pour $j \neq i$. Nous en déduisons que μ_{x_i} est une puissance de P_i dès que $x_i \in E_i$. Nous choisissons $x_i \in E_i$ tel que $\mu_{x_i} = P_i^{\alpha_i}$.

Nous posons enfin $a = x_1 + \dots + x_r$; par définition du polynôme annulateur μ_a , nous avons

$$0 = \mu_a(f)a = \mu_a(f)x_1 + \dots + \mu_a(f)x_r. \quad (9.195)$$

Mais $\mu_a(f)x_j \in E_j$, et la somme des E_j est directe, donc l'annulation de la somme (9.195) implique l'annulation de chacun des termes : $\mu_a(f)x_i = 0$ pour tout i . Cela prouve que $\mu_{x_i} \mid \mu_a$. Mais comme les μ_{x_i} sont premiers deux à deux (parce que ce sont les $P_i^{\alpha_i}$), nous avons que le produit divise encore μ_a :

$$\prod_{i=1}^r \mu_{x_i} \mid \mu_a, \quad (9.196)$$

c'est-à-dire $\mu \mid \mu_a$. Comme nous avons aussi $\mu_a \mid \mu$, nous déduisons $\mu_a = \mu$. $\square$

Définition 9.100 (Matrices, endomorphismes et vecteurs cycliques).

Une matrice est **cyclique** si elle est semblable à une matrice compagnon. Un endomorphisme $f: E \rightarrow E$ est **cyclique** s'il existe un vecteur $x \in E$ tel que $\{f^k(x)\}_{k=0, \dots, n-1}$ est une base de E . Un vecteur ayant cette propriété est un **vecteur cyclique** pour f .

Lemme 9.101.

Soit E un espace vectoriel de dimension finie et un endomorphisme cyclique³⁰ f de E . Soit un

29. À mon avis, « unitaire » manque dans [101].

30. Voir la définition 9.100.

vecteur cyclique v de f , alors le polynôme minimal de f est égal au polynôme minimal de f au point $v : \mu_f = \mu_{f,v}$.

Démonstration. Montrons que $\mu_{f,v}$ est un polynôme annulateur de f , ce qui prouvera que μ_f divise $\mu_{f,v}$ par la proposition 9.97. Étant donné que v est cyclique, tout élément de E s'écrit sous la forme $x = Q(f)v$. Prenons un polynôme P annulateur de f en $v : P(f)v = 0$. Nous montrons que P est alors un polynôme annulateur de f . En effet, nous avons

$$P(f)x = (P(f) \circ Q(f))v = (Q(f) \circ P(f))v = 0 \quad (9.197)$$

où nous avons utilisé le lemme 9.87. $\square$

Lemme 9.102 ([201]).

Soit $a \in E$ tel que $\mu_a = \mu$. Alors E_a est un sous-espace stable pour f pour lequel il existe un supplémentaire stable.

Démonstration. Soit $l = \deg(\mu) = \deg(\mu_a)$. L'espace E_a étant engendré par les $f^k(a)$ nous savons que $e_1 = a, e_2 = f(a), \dots, e_l = f^{l-1}(a)$ forment une base de E_a . Nous pouvons la compléter en une base $\{e_1, \dots, e_n\}$ de E . Et nous posons³¹

$$G = \{x \in E \text{ tel que } e_l^*(f^k(x)) = 0 \forall k \geq 0\} \quad (9.198a)$$

$$= \bigcap_{k \geq 0} \ker\{e_l^* \circ f^k\} \quad (9.198b)$$

$$= \bigcap_{k=0}^{l-1} \ker(e_l^* \circ f^k). \quad (9.198c)$$

La dernière égalité est due au fait que l soit le degré de μ . Du coup f^l est une combinaison linéaire des f^i avec $i \leq l-1$.

Nous avons $f(G) \subset G$ et de plus $E_a \cap G = \{0\}$ parce qu'un élément de E_a est une combinaison linéaire d'éléments de la forme $f^j(a)$ ($j \leq l$). Après application de f^{l-j} , ces éléments obtiennent une composante $f^l(a) = e_l$. De plus G est un sous-espace vectoriel du fait que $e_l^* \circ f^i$ est une application linéaire.

Montrons enfin que $\dim(G) = n - l$. Pour cela nous remarquons que G est une intersection d'hyperplans, et nous montrons que les équations définissant ces hyperplans sont linéairement indépendantes. Soit donc

$$\sum_{j=0}^{l-1} \lambda_j (e_l^* \circ f^j) = 0 \quad (9.199)$$

et montrons que $\lambda_j = 0$ pour tout j est l'unique solution. Soit $x \in E$ et appliquons l'opération (9.199) au vecteur $f^i(x)$; le résultat est zéro :

$$0 = \sum_{j=0}^{l-1} \lambda_j (e_l^* \circ f^i \circ f^j) = (e_l^* \circ f^i)P(u) \quad (9.200)$$

où nous avons posé $P(X) = \sum_{j=0}^{l-1} \lambda_j X^j$. Appliquons cela à a : pour tout i nous avons

$$(e_l^* \circ f^i)(P(f)a) = 0. \quad (9.201)$$

Mais par définition de E_a , l'élément $P(f)a$ est dans E_a . Nous en déduisons que

$$P(f)a \in G \cap E_a = \{0\}, \quad (9.202)$$

c'est-à-dire que P est un polynôme annulateur de a . Mais P est de degré $l-1$ alors que le polynôme minimal de a est de degré l . Par conséquent $P = 0$ et $\lambda_j = 0$ pour tout j . $\square$

31. ici, comme presque partout, e_l^* est le dual de e_l , c'est-à-dire l'application linéaire sur E donnée par $e_l^*(e_i) = \delta_{li}$.

Définition 9.103.

Un endomorphisme d'un espace vectoriel est **semi-simple** si tout sous-espace stable par u possède un supplémentaire stable.

Lemme 9.104.

Si le polynôme minimal d'un endomorphisme est irréductible, alors il est semi-simple³².

Démonstration. Soit f , un endomorphisme dont le polynôme minimal est irréductible et F , un sous-espace stable par f . Nous devons en trouver un supplémentaire stable. Si $F = E$, il n'y a pas de problèmes. Sinon nous considérons $u_1 \in E \setminus F$ et

$$E_{u_1} = \{P(f)u_1 \text{ tel que } P \in \mathbb{K}[X]\}, \quad (9.203)$$

qui est un espace stable par f .

Montrons que $E_{u_1} \cap F = \{0\}$. Pour cela nous regardons l'idéal

$$I_{u_1} = \{P \in \mathbb{K}[X] \text{ tel que } P(f)u_1 = 0\}. \quad (9.204)$$

Cela est un idéal non réduit à $\{0\}$ parce que le polynôme minimal de f par exemple est dans I_{u_1} . Soit P_{u_1} un générateur unitaire de I_{u_1} . Étant donné que $\mu_f \in I_{u_1}$, nous avons que P_{u_1} divise μ_f et donc $P_{u_1} = \mu_f$ parce que μ_f est irréductible par hypothèse.

Soit $y \in E_{u_1} \cap F$. Par définition il existe $P \in \mathbb{K}[X]$ tel que $y = P(f)u_1$ et si $y \neq 0$, ce la signifie que $P \notin I_{u_1}$, c'est-à-dire que P_{u_1} ne divise pas P . Étant donné que P_{u_1} est irréductible cela implique que P_{u_1} et P sont premiers entre eux (ils n'ont pas d'autre pgcd que 1).

Nous utilisons maintenant Bézout (théorème 6.43) qui nous donne $A, B \in \mathbb{K}[X]$ tels que

$$AP + BP_{u_1} = 1. \quad (9.205)$$

Nous appliquons cette égalité à f et puis à u_1 :

$$u_1 = A(f) \circ \underbrace{P(f)u_1}_{=y} + B(f) \circ \underbrace{P_{u_1}(u_1)}_{=0} = A(f)y. \quad (9.206)$$

Mais $y \in F$, donc $A(f)y \in F$. Nous aurions donc $u_1 \in F$, ce qui est impossible par choix. Nous avons maintenant que l'espace $E_{u_1} \oplus F$ est stable sous f . Si cet espace est E alors nous arrêtons. Sinon nous reprenons le raisonnement avec $E_{u_1} \oplus F$ en guise de F et en prenant $u_2 \in E \setminus (E_{u_1} \oplus F)$. Étant donné que E est de dimension finie, ce procédé s'arrête à un certain moment et nous aurons

$$E = F \oplus E_{u_1} \oplus \dots \oplus E_{u_k} \quad (9.207)$$

où chacun des E_{u_i} sont stables. □

Théorème 9.105.

Un endomorphisme est semi-simple si et seulement si son polynôme minimal est produit de polynômes irréductibles distincts deux à deux.

Démonstration. Supposons que f soit semi-simple et que son polynôme minimal soit donné par $\mu_f = M_1^{\alpha_1} \dots M_r^{\alpha_r}$ où les M_i sont des polynômes irréductibles deux à deux distincts. Nous devons montrer que $\alpha_i = 1$ pour tout i . Soit i tel que $\alpha_i \geq 1$ et $N \in \mathbb{K}[X]$ tel que $\mu_f = M^2 N$ où l'on a noté $M = M_i$. Nous étudions l'espace

$$F = \ker M(f) \quad (9.208)$$

qui est stable par f , et qui possède donc un supplémentaire S également stable par f . Nous allons montrer que MN est un polynôme annulateur de f .

32. Définition 9.103.

D'abord nous prenons $x \in S$. Étant donné que F est le noyau de $M(f)$,

$$M(f)(MN(f)x) = \mu_f(f)x = 0, \quad (9.209)$$

ce qui signifie que $MN(f)x \in F$. Mais vu que S est stable par f nous avons aussi que $MN(f)x \in S$. Finalement $MN(f)x \in F \cap S = \{0\}$. Autrement dit, $MN(f)$ s'annule sur S .

Prenons maintenant $y \in F$. Nous avons

$$MN(f) = N(f)(M(f)y) = 0 \quad (9.210)$$

parce que $y \in F = \ker M(f)$.

Nous avons prouvé que $MN(f)$ s'annule partout et donc que $MN(f)$ est un polynôme annulateur de f , ce qui contredit la minimalité de $\mu_f = M^2N$.

Nous passons au sens inverse. Soit $m_f = M_1 \dots M_r$ une décomposition du polynôme minimal de l'endomorphisme f en irréductibles distincts deux à deux. Soit F un sous-espace vectoriel stable par f . Nous notons

$$E_i = \ker(M_i(f)) \quad (9.211)$$

et $f_i = f|_{E_i}$. Par le lemme 9.90 nous avons

$$F = \bigoplus_{i=1}^r (F \cap E_i). \quad (9.212)$$

Les espaces E_i sont stables par f et étant donné que M_i est irréductible, il est le polynôme minimal de f_i . En effet, M_i est annulateur de f_i , ce qui montre que le minimal de f_i divise M_i . Mais M_i étant irréductible, M_i est le polynôme minimal. Étant donné que $\mu_{f_i} = M_i$, l'endomorphisme f_i est semi-simple par le lemme 9.104.

L'espace $F \cap E_i$ étant stable par l'endomorphisme semi-simple f_i , il possède un supplémentaire stable que nous notons S_i :

$$E_i = S_i \oplus (F \cap E_i). \quad (9.213)$$

Étant donné que sur chaque S_i nous avons $f|_{S_i} = f_i$, l'espace $S = S_1 \oplus \dots \oplus S_r$ est stable par f . Du coup nous avons

$$E = E_1 \oplus \dots \oplus E_r \quad (9.214a)$$

$$= (S_1 \oplus (F \cap E_1)) \oplus \dots \oplus (S_r \oplus (F \cap E_r)) \quad (9.214b)$$

$$= \left(\bigoplus_{i=1}^r S_i \right) \oplus \left(\bigoplus_{i=1}^r F \cap E_i \right) \quad (9.214c)$$

$$= S \oplus F, \quad (9.214d)$$

ce qui montre que F a bien un supplémentaire stable par f et donc que f est semi-simple. $\square$

Exemple 9.106 (L'espace engendré par $\mathbb{1}, A, A^2, \dots$).

Soit A une matrice, et

$$V = \text{Span}\{A^k \text{ tel que } k \in \mathbb{N}\}. \quad (9.215)$$

Nous montrons que $\dim(V)$ est le degré du polynôme minimal de A .

D'abord l'idéal annulateur de A est engendré par le polynôme minimal³³ que nous notons $\mu = \sum_{k=0}^p a_k X^k$. La partie $\{\mathbb{1}, \dots, A^{p-1}\}$ est libre parce qu'une combinaison linéaire nulle de cela serait un polynôme annulateur en A de degré plus petit que p . Donc $\dim(V) \geq p$.

La partie $\{\mathbb{1}, A, \dots, A^p\}$ est liée à cause du polynôme minimal. Isoler A^p dans $\mu(A) = 0$ donne un polynôme f de degré $p-1$ tel que $A^p = f(A)$.

Nous allons montrer à présent que la famille $\{\mathbb{1}, A, \dots, A^{p-1}\}$ est génératrice (alors $\dim(V) \leq p$). Soit un entier $q \geq p$ de division euclidienne³⁴ $np + r = q$ avec $r < p$. Nous avons $A^q = A^{np} A^r$. D'une part

$$A^{np} = (A^p)^n = f(A)^n \quad (9.216)$$

33. Proposition 9.97.

34. Théorème 1.177.

est de degré $n(p-1)$. Par conséquent

$$A^q = f(A)^n A^r \quad (9.217)$$

qui est de degré $n(p-1) + r = q - n$. Autrement dit il existe un polynôme g_1 de degré $q - n$ tel que $A^q = g_1(A)$. Si $q - n > p - 1$ alors nous pouvons recommencer et obtenir un polynôme g_2 de degré strictement inférieur à celui de g_1 tel que $A^q = g_2(A)$. Au bout du compte, il existe un polynôme g de degré au maximum $p - 1$ tel que $A^q = g(A)$. Cela prouve que la partie $\{1, A, \dots, A^{p-1}\}$ est génératrice de V .

La dimension de V est donc p , le degré du polynôme minimal. $\triangle$

Proposition 9.107.

Soit f un endomorphisme d'un espace vectoriel de dimension finie. Nous avons l'isomorphisme d'espace vectoriel

$$\mathbb{K}[f] \simeq \frac{\mathbb{K}[X]}{(\mu_f)} \quad (9.218)$$

La dimension en est $\deg(\mu_f)$.

Démonstration. Notons avant de commencer que (μ) est l'idéal engendré par μ . Les classes dont il est question dans le quotient $\mathbb{K}[X]/(\mu)$ sont

$$\bar{P} = \{P + S\mu\}_{S \in \mathbb{K}[X]}. \quad (9.219)$$

Nous allons montrer que l'application suivante fournit l'isomorphisme :

$$\begin{aligned} \psi: \frac{\mathbb{K}[X]}{(\mu)} &\rightarrow \mathbb{K}[f] \\ \bar{P} &\mapsto P(f). \end{aligned} \quad (9.220)$$

ψ est bien définie Si $Q \in \bar{P}$ alors $Q = P + S\mu$ pour un certain $S \in \mathbb{K}[X]$. Du coup nous avons

$$\psi(\bar{Q}) = P(f) + (S\mu)(f). \quad (9.221)$$

Mais $\mu(f) = 0$ donc le deuxième terme est nul. Donc $\psi(\bar{P})$ est bien défini.

Injectif Si $\psi(\bar{P}) = 0$ nous avons $P(f) = 0$, ce qui signifie que $P = S\mu$ pour un polynôme S . Par conséquent $P \in (\mu)$ et donc $\bar{P} = 0$.

Surjectif Soit $P \in \mathbb{K}[X]$. L'élément $P(f)$ de $\mathbb{K}[f]$ est dans l'image de ψ parce que c'est $\psi(\bar{P})$.

En ce qui concerne la dimension, le corolaire 6.40 en parle déjà : une base est donné par les projections de $1, X, \dots, X^{\deg(\mu_a)-1}$. $\square$

9.6.3 Polynôme caractéristique

Définition 9.108.

*Soit un anneau commutatif A . Si $u \in \mathbb{M}(n, A)$, nous définissons le **polynôme caractéristique** de u :*

$$\chi_u(X) = \det(u - X\mathbb{1}_n). \quad (9.222)$$

Nous définissons de même le polynôme caractéristique d'un endomorphisme $u: E \rightarrow E$.

Remarque 9.109.

Quelques remarques à propos du signe³⁵.

- Certains auteurs définissent le polynôme caractéristique par $\det(X - u)$ au lieu de $\det(u - X)$.
- Wikipédia francophone prend la définition $\det(X - u)$ (donc inverse de la notre). Allez lire la page de discussion.

35. Attention : je crois qu'il y a des incohérences dans le Frido à propos de ce choix

- Sur les wikipédias d'autre langues, ça varie.
- Un avantage de $\det(u - X)$ est que $\det(u) = \chi_u(0)$.
- Un avantage de $\det(X - u)$ est qu'il est unitaire.

Lemme 9.110.

Le polynôme caractéristique χ_u est unitaire en dimension paire et a pour degré la dimension de l'espace vectoriel E .

Théorème 9.111.

Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie n et un endomorphisme $u \in \text{End}(E)$. Alors

- (1) Le polynôme caractéristique divise $(\mu_u)^n$ dans $\mathbb{K}[X]$.
- (2) Les polynômes caractéristiques et minimaux ont mêmes facteurs irréductibles dans $\mathbb{K}[X]$.
- (3) Les polynômes caractéristiques et minimaux ont mêmes racines dans $\mathbb{K}[X]$.
- (4) Le polynôme caractéristique est scindé si et seulement si le polynôme minimal est scindé.

Théorème 9.112.

Soit $u \in \text{End}(E)$ et $\lambda \in \mathbb{K}$. Les conditions suivantes sont équivalentes

- (1) $\lambda \in \text{Spec}(u)$
- (2) $\chi_u(\lambda) = 0$
- (3) $\mu_u(\lambda) = 0$.

Démonstration. (1) $\Leftrightarrow$ (2). Dire que λ est dans le spectre de u signifie que l'opérateur $u - \lambda \mathbb{1}$ n'est pas inversible, ce qui est équivalent à dire que $\det(u - \lambda \mathbb{1})$ est nul par la proposition 9.9(1) ou encore que λ est une racine du polynôme caractéristique de u .

(2) $\Leftrightarrow$ (3). Cela est une application directe du théorème 9.111 qui précise que le polynôme caractéristique a les mêmes racines dans $\mathbb{K}$ que le polynôme minimal. $\square$

Exemple 9.113.

Sur $\mathbb{R}^2$, nous considérons la matrice $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ qui a pour polynôme caractéristique³⁶ le polynôme $\chi_A = (X - 1)^2$. Le nombre $\lambda = 1$ est une racine double de ce polynôme, et pourtant il n'y a qu'une seule dimension d'espace propre :

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \quad (9.223)$$

entraîne $x = 0$.

Ici la multiplicité algébrique est différente de la multiplicité géométrique. $\triangle$

La proposition suivante donne une utilisation amusante de la notion de polynôme caractéristique³⁷.

Proposition 9.114 ([202]).

Soit un espace vectoriel V de dimension finie pour lequel il existe un endomorphisme $f: V \rightarrow V$ tel que $(f \circ f)(v) = -v$ pour tout $v \in V$. Alors la dimension de V est paire.

Démonstration. Cherchons les valeurs propres de f en résolvant l'équation $f(v) = \lambda v$. Nous appliquons f à cette égalité :

$$-v = \lambda f(v) = \lambda^2 v. \quad (9.224)$$

Donc λ ne peut pas être réel. Nous avons montré que f n'a pas de valeurs propres réelles. Or le polynôme caractéristique de f est de degré égal à la dimension. Si la dimension est impaire, le polynôme caractéristique est de degré impair, et possède donc une racine réelle. Autrement dit, l'absence de racines réelles au polynôme caractéristique indique une dimension paire. $\square$

36. Définition 9.108.

37. Définition 9.108.

Une autre preuve possible est d'utiliser le déterminant : si la dimension de V est n nous avons :

$$\det(f^2) = \det(-\text{Id}) = (-1)^n. \quad (9.225)$$

Donc $(-1)^n$ est positif, ce qui montre que n est pair.

Proposition 9.115 ([200]).

Soit f , un endomorphisme de E et $x \in E$. Alors

(1) L'espace $E_{f,x}$ est stable par f .

(2) L'espace $E_{f,x}$ est de dimension

$$p_{f,x} = \dim E_{f,x} = \deg(\mu_{f,x}) \quad (9.226)$$

où $\mu_{f,x}$ est le générateur unitaire de $I_{f,x}$.

(3) Le polynôme caractéristique de $f|_{E_{f,x}}$ est $\mu_{f,x}$.

(4) Nous avons

$$\chi_{f|_{E_{f,x}}}(f)x = \mu_{f,x}(f)x = 0. \quad (9.227)$$

Démonstration. Le fait que $E_{f,x}$ soit stable par f est classique. Le point (4) est une application du point (3). Les deux gros morceaux sont donc les points (2) et (3).

Étant donné que $\mu_{f,x}$ est de degré minimal dans $I_{f,x}$, l'ensemble

$$B = \{f^k(x) \text{ tel que } 0 \leq k \leq p_{f,x} - 1\} \quad (9.228)$$

est libre. En effet une combinaison nulle des vecteurs de B donnerait un polynôme en f de degré inférieur à $p_{f,x}$ annulant x . Nous écrivons

$$\mu_{f,x}(X) = X^{p_{f,x}} - \sum_{i=0}^{p_{f,x}-1} a_i X^i. \quad (9.229)$$

Étant donné que $\mu_{f,x}(f)x = 0$ et que la somme du membre de droite est dans $\text{Span}(B)$, nous avons $f^{p_{f,x}}(x) \in \text{Span}(B)$. Nous prouvons par récurrence que $f^{p_{f,x}+k}(x) \in \text{Span}(B)$. En effet en appliquant f^k à l'égalité

$$0 = f^{p_{f,x}}(x) - \sum_{i=0}^{p_{f,x}-1} a_i f^i(x) \quad (9.230)$$

nous trouvons

$$f^{p_{f,x}+k}(x) = \sum_{i=0}^{p_{f,x}-1} a_i f^{i+k}(x), \quad (9.231)$$

alors que par hypothèse de récurrence le membre de droite est dans $\text{Span}(B)$. L'ensemble B est alors générateur de $E_{f,x}$ et donc une base d'icelui. Nous avons donc bien $\dim(E_{f,x}) = p_{f,x}$.

Nous montrons maintenant que $\mu_{f,x}$ est annulateur de f au point x . Nous savons que

$$\mu_{f,x}(f)x = 0. \quad (9.232)$$

En y appliquant f^k et en profitant de la commutativité des polynômes sur les endomorphismes (proposition 9.87), nous avons

$$0 = f^k(\mu_{f,x}(f)x) = \mu_{f,x}(f)f^k(x), \quad (9.233)$$

de telle sorte que $\mu_{f,x}(f)$ est nul sur B et donc est nul sur $E_{f,x}$. Autrement dit,

$$\mu_{f,x}(f|_{E_{f,x}}) = 0. \quad (9.234)$$

Montrons que $\mu_{f,x}$ est même minimal pour $f|_{E_{f,x}}$. Soit Q , un polynôme non nul de degré $p_{f,x} - 1$ annulant $f|_{E_{f,x}}$. En particulier $Q(f)x = 0$, alors qu'une telle relation signifierait que B est un système lié, alors que nous avons montré que c'était un système libre. Nous concluons que $\mu_{f,x}$ est le polynôme minimal de $f|_{E_{f,x}}$. $\square$

Cette histoire de densité permet de donner une démonstration alternative du théorème de Cayley-Hamilton.

Théorème 9.116 (Cayley-Hamilton).

Le polynôme caractéristique est un polynôme annulateur.

Une démonstration plus simple via la densité des diagonalisables est donnée en théorème 13.24.

Démonstration. Nous devons prouver que $\chi_f(f)x = 0$ pour tout $x \in E$. Pour cela nous nous fixons un $x \in E$, nous considérons l'espace $E_{f,x}$ et $\chi_{f,x}$, le polynôme caractéristique de $f|_{E_{f,x}}$. Étant donné que $E_{f,x}$ est stable par f , le polynôme caractéristique de $f|_{E_{f,x}}$ divise χ_f , c'est-à-dire qu'il existe un polynôme Q_x tel que

$$\chi_f = Q_x \chi_{f,x}, \quad (9.235)$$

et donc aussi

$$\chi_f(f)x = Q_x(f)(\chi_{f,x}(f)x) = 0 \quad (9.236)$$

parce que la proposition 9.115 nous indique que $\chi_{f,x}$ est un polynôme annulateur de $f|_{E_{f,x}}$. $\square$

Corolaire 9.117.

Le degré du polynôme minimal est majoré par la dimension de l'espace.

Démonstration. Le polynôme minimal divise le polynôme caractéristique parce qu'il engendre l'idéal des polynômes annulateurs par la proposition 9.97. Or le degré du polynôme caractéristique est la dimension de l'espace par le lemme 9.110. $\square$

Exemple 9.118 (Calcul de l'inverse d'un endomorphisme).

Le polynôme de Cayley-Hamilton donne un moyen de calculer l'inverse d'un endomorphisme inversible pourvu que l'on sache son polynôme caractéristique. En effet, supposons que

$$\chi_f(X) = \sum_{k=0}^n a_k X^k. \quad (9.237)$$

Nous aurons alors

$$0 = \chi_f(f) = \sum_{k=0}^n a_k f^k. \quad (9.238)$$

Nous appliquons f^{-1} à cette dernière égalité en sachant que $f^{-1}(0) = 0$:

$$0 = a_0 f^{-1} + \sum_{k=1}^n a_k f^{k-1}, \quad (9.239)$$

et donc

$$u^{-1} = -\frac{1}{\det(f)} \sum_{k=1}^n a_k f^{k-1} \quad (9.240)$$

où nous avons utilisé le fait que $a_0 = \chi_f(0) = \det(f)$. $\triangle$

Proposition 9.119.

Si $(X - z)^l$ ($l \geq 1$) est la plus grande puissance de $(X - z)$ dans le polynôme caractéristique d'un endomorphisme u alors

$$1 \leq \dim(E_e) \leq l. \quad (9.241)$$

C'est-à-dire que nous avons au moins un vecteur propre pour chaque racine du polynôme caractéristique.

Démonstration. Si $(X - z)$ divise χ_u alors en posant $\chi_u = (X - z)P(X)$ nous avons

$$\det(u - X\mathbb{1}) = (X - z)P(X), \quad (9.242)$$

ce qui, évalué en $X = z$, donne $\det(u - z\mathbb{1}) = 0$. L'annulation du déterminant étant équivalente à l'existence d'un noyau non trivial, nous avons $v \neq 0$ dans E tel que $(u - z\mathbb{1})v = 0$. Cela donne $u(v) = zv$ et donc que v est vecteur propre de u pour la valeur propre z . Donc aussi $\dim(E_z) \geq 1$.

Si $\dim(E_z) = k$ alors le théorème de la base incomplète 4.11 nous permet d'écrire une base de E dont les k premiers vecteurs forment une base de E_z . Dans cette base, la matrice de u est de la forme

$$\begin{pmatrix} z & & * \\ & \ddots & \vdots \\ & & z & * \\ & & & * \end{pmatrix} \quad (9.243)$$

où les étoiles représentent des blocs à priori non nuls. En tout cas il est vu sous cette forme que $(X - z\mathbb{1})^k$ divise χ_u . $\square$

9.7 Diagonalisation et trigonalisation

Ici encore $\mathbb{K}$ est un corps commutatif.

9.7.1 Matrices semblables

Définition 9.120 (matrices semblables).

Sur l'ensemble $\mathbb{M}_n(\mathbb{K})$ des matrices $n \times n$ à coefficients dans $\mathbb{K}$ nous introduisons la relation d'équivalence $A \sim B$ si et seulement s'il existe une matrice $P \in \text{GL}(n, \mathbb{K})$ telle que $B = P^{-1}AP$. Deux matrices équivalentes en ce sens sont dites **semblables**.

Le polynôme caractéristique³⁸ est un invariant sous les similitudes. En effet si P est une matrice inversible,

$$\chi_{PAP^{-1}} = \det(PAP^{-1} - \lambda X) \quad (9.244a)$$

$$= \det(P^{-1}(PAP^{-1} - \lambda X)P) \quad (9.244b)$$

$$= \det(A - \lambda X). \quad (9.244c)$$

La permutation de lignes ou de colonnes ne sont pas de similitudes, comme le montrent les exemples suivants :

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \quad B = \begin{pmatrix} 2 & 1 \\ 4 & 3 \end{pmatrix}. \quad (9.245)$$

Nous avons $\chi_A = x^2 - 5x - 2$ tandis que $\chi_B = x^2 - 5x + 2$ alors que le polynôme caractéristique est un invariant de similitude.

9.7.2 Endomorphismes nilpotents

La **trace** d'une matrice $A \in \mathbb{M}(n, \mathbb{K})$ est la somme de ses éléments diagonaux :

$$\text{Tr}(A) = \sum_{i=1}^n A_{ii}. \quad (9.246)$$

Une propriété importante est son invariance cyclique.

Lemme 9.121.

Quelques propriétés de la trace.

38. Définition 9.108.

Proposition 9.123 ([203]).

Soit un $\mathbb{K}$ -espace vectoriel E . Un endomorphisme $u \in \text{End}(E)$ est nilpotent si et seulement s'il existe une base de E dans laquelle la matrice de u est strictement triangulaire supérieure.

Démonstration. $\Rightarrow$ Nous faisons la démonstration par récurrence sur la dimension de E . Lorsque $n = 1$ nous avons $u = (a)$ avec $a \in \mathbb{K}$. Vu que $a^k = 0$ pour un certain k nous avons $a = 0$ parce qu'un corps est toujours un anneau intègre⁴⁰.

Lorsque $\dim(E) = n$ nous savons que u a un noyau non réduit au vecteur nul (parce qu'il est nilpotent). Soit donc un vecteur non nul $x \in \ker(u)$ et une base

$$\{x, e_2, \dots, e_n\} \quad (9.253)$$

donnée par le théorème de la base incomplète 4.11. La matrice de u dans cette base s'écrit

$$\left(\begin{array}{c|ccc} 0 & * & * & * \\ \hline 0 & & & \\ 0 & & A & \\ 0 & & & \end{array} \right). \quad (9.254)$$

Un tout petit peu de calcul de produit de matrice montre que la matrice de u^k est de la forme

$$\left(\begin{array}{c|ccc} 0 & * & * & * \\ \hline 0 & & & \\ 0 & & A^k & \\ 0 & & & \end{array} \right). \quad (9.255)$$

Étant donné que u est nilpotente, la matrice A l'est aussi. L'hypothèse de récurrence dit alors que A est strictement triangulaire supérieure (ou en tout cas peut le devenir par un changement de base adéquat).

$\Leftarrow$ Lorsqu'une matrice est triangulaire supérieure stricte, elle applique

$$\text{Span}\{e_1, \dots, e_k\} \rightarrow \text{Span}\{e_1, \dots, e_{k-1}\}. \quad (9.256)$$

Donc tout vecteur finit sur zéro si on lui applique u assez souvent. □

Proposition 9.124 (Thème 47).

Soit E un espace de Banach (espace vectoriel normé complet). Si $A \in \mathcal{L}(E, E)$ est nilpotente, alors $(\mathbb{1} - A)$ est inversible et son inverse est donné par

$$(\mathbb{1} - A)^{-1} = \sum_{k=0}^{\infty} A^k, \quad (9.257)$$

où l'infini peut évidemment être remplacé par l'ordre de nilpotence de A .

Démonstration. En ce qui concerne la convergence de la somme, elle ne fait pas de doute parce que A étant nilpotente, la somme contient seulement une quantité finie de termes non nuls.

Montrons à présent que la somme est l'inverse de $\mathbb{1} - A$ en multipliant terme à terme :

$$\sum_{k=0}^n A^k (\mathbb{1} - A) = \sum_{k=0}^n (A^k - A^{k+1}) = \mathbb{1} - A^{n+1}. \quad (9.258)$$

Par conséquent

$$\|\mathbb{1} - \sum_{k=0}^n A^k (\mathbb{1} - A)\| = \|A^{n+1}\| \rightarrow 0. \quad (9.259)$$

La dernière limite est en réalité une égalité pour n assez grand. □

40. Lemme 1.194.

Proposition 9.125.

Soit $A \in \text{GL}(n, \mathbb{C})$. La suite $(A^k)_{k \in \mathbb{Z}}$ est bornée si et seulement si A est diagonalisable et $\text{Spec}(A) \subset \mathbb{S}^1$.

Démonstration. Si A est diagonalisable avec les valeurs propres λ_i de norme 1 dans $\mathbb{C}$, alors A^k est la matrice diagonale avec les λ_i^k sur la diagonale. Cela reste borné pour toute valeur entière de k .

En ce qui concerne l'autre sens, nous supposons encore que

$$A = \begin{pmatrix} \lambda_1 \mathbb{1} + N_1 & & \\ & \ddots & \\ & & \lambda_s \mathbb{1} + N_s \end{pmatrix}, \quad (9.260)$$

et nous regardons un des blocs. Nous voulons prouver que $N = 0$ et que $|\lambda| = 1$.

Nous commençons par regarder ce qu'implique le fait que $(\lambda \mathbb{1} + N)^n$ reste borné pour $n > 0$. En notant r l'ordre de nilpotence de N , nous avons le développement

$$(\lambda \mathbb{1} + N)^n = \sum_{k=0}^{r-1} \binom{n}{k} N^k \lambda^{n-k}. \quad (9.261)$$

Par la proposition 9.123, une matrice nilpotente s'écrit dans une base sous la forme

$$N = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ & & & & 0 \end{pmatrix} \quad (9.262)$$

et effectuer A^k revient à décaler la diagonale de 1. Donc la famille

$$\{\mathbb{1}, N, \dots, N^{r-1}\} \quad (9.263)$$

est libre. Par conséquent la suite $(\lambda \mathbb{1} + N)^n$ restera bornée si et seulement si chacun des termes

$$\binom{n}{k} N^k \lambda^{n-k} \quad (9.264)$$

reste borné. Le premier terme étant $\lambda^n \mathbb{1}$, nous avons obligatoirement $|\lambda| \leq 1$. Si $|\lambda| < 1$, alors le coefficient $\binom{n}{k} \lambda^{n-k}$ tend vers zéro. Si $|\lambda| = 1$ par contre ce coefficient tend vers l'infini et la seule façon pour que (9.264) reste borné est que $N = 0$. Nous avons donc deux possibilités :

- $|\lambda| < 1$
- $|\lambda| = 1$ et $N = 0$.

Nous nous tournons maintenant sur la contrainte que $(\lambda \mathbb{1} + N)^n$ doive rester borné pour $n < 0$. Nous avons

$$\lambda \mathbb{1} + N = \lambda(\mathbb{1} + \lambda^{-1} N), \quad (9.265)$$

et nous pouvons appliquer la proposition 9.124 à l'opérateur nilpotent $-\lambda^{-1} N$ pour avoir

$$(\mathbb{1} + \lambda^{-1} N)^{-1} = \mathbb{1} + \sum_{k=1}^{\infty} (-\lambda)^{-1} N^k. \quad (9.266)$$

Ceci pour dire que $(\lambda \mathbb{1} + N)^{-1} = \lambda^{-1}(\mathbb{1} + \lambda^{-1} N')$ pour une autre matrice nilpotente N' . Le travail déjà fait, appliqué à λ^{-1} et N' , nous donne deux possibilités :

- $|\lambda^{-1}| < 1$
- $|\lambda^{-1}| = 1$ et $N' = 0$.

La possibilité $|\lambda^{-1}| < 1$ est exclue parce qu'elle impliquerait $|\lambda| > 1$ qui avait déjà été exclu. Il ne reste donc que la possibilité $|\lambda| = 1$ et $N = N' = 0$. $\square$

9.7.3 Endomorphismes diagonalisables

Définition 9.126.

Une matrice est **diagonalisable** si elle est semblable⁴¹ à une matrice diagonale.

Lemme 9.127.

Une matrice triangulaire supérieure avec des 1 sur la diagonale n'est diagonalisable que si elle est diagonale (c'est-à-dire si elle est la matrice unité).

Démonstration. Si A est une matrice triangulaire supérieure de taille n telle que $A_{ii} = 1$, alors $\det(A - \lambda \mathbb{1}) = (1 - \lambda)^n$, ce qui signifie que $\text{Spec}(A) = \{1\}$. Pour la diagonaliser, il faudrait une matrice $P \in \text{GL}(n, \mathbb{K})$ telle que $\mathbb{1} = P^{-1}AP$, ce qui est uniquement possible si $A = \mathbb{1}$. $\square$

Lemme 9.128.

Soit F un sous-espace stable par u . Soit une décomposition du polynôme minimal

$$\mu_u = P_1^{n_1} \dots P_r^{n_r} \quad (9.267)$$

où les P_i sont des polynômes irréductibles unitaires distincts. Si nous posons $E_i = \ker P_i^{n_i}$, alors

$$F = (F \cap E_1) \oplus \dots \oplus (F \cap E_r). \quad (9.268)$$

Théorème 9.129.

Soit E , un espace vectoriel de dimension n sur le corps commutatif $\mathbb{K}$ et $u \in \text{End}(E)$. Les propriétés suivantes sont équivalentes.

- (1) L'endomorphisme u est diagonalisable.
- (2) Il existe un polynôme $P \in \mathbb{K}[X]$ non constant, scindé sur $\mathbb{K}$ dont toutes les racines sont simples tel que $P(u) = 0$.
- (3) Le polynôme minimal μ_u est scindé sur $\mathbb{K}$ et toutes ses racines sont simples⁴².
- (4) Tout sous-espace de E possède un supplémentaire stable par u .
- (5) Dans une base adaptée, la matrice de u est diagonale et les éléments diagonaux sont ses valeurs propres.

Démonstration. Plein d'implications à prouver.

(2) implique (3) Étant donné que $P(u) = 0$, il est dans l'idéal des polynômes annulateurs de u , et le polynôme minimal μ_u le divise parce que l'idéal des polynômes annulateurs est généré par μ_u par le théorème 6.39.

(3) implique (1) Étant donné que le polynôme minimal est scindé à racines simples, il s'écrit sous forme de produits de monômes tous distincts, c'est-à-dire

$$\mu_u(X) = (X - \lambda_1) \dots (X - \lambda_r) \quad (9.270)$$

où les λ_i sont des éléments distincts de $\mathbb{K}$. Étant donné que $\mu_u(u) = 0$, le théorème de décomposition des noyaux (théorème 9.88) nous enseigne que

$$E = \ker(u - \lambda_1) \oplus \dots \oplus \ker(u - \lambda_r). \quad (9.271)$$

Mais $\ker(u - \lambda_i)$ est l'espace propre $E_{\lambda_i}(u)$. Donc u est diagonalisable.

41. Définition 9.120.

42. Le polynôme caractéristique, lui, n'a pas spécialement ses racines simples ; il peut encore être de la forme

$$\chi_u(X) = \prod_{i=1}^r (X - \lambda_i)^{\alpha_i}, \quad (9.269)$$

mais alors $\dim(E_{\lambda_i}) = \alpha_i$.

(1) implique (4) Soit $\{e_1, \dots, e_n\}$ une base qui diagonalise u , soit F un sous-espace de E un $\{f_1, \dots, f_r\}$ une base de F . Par le théorème 4.15(2), nous pouvons compléter la base de F par des éléments de la base $\{e_i\}$. Le complément ainsi construit est invariant par u .

(4) implique (1) En dimension un, tout endomorphisme est diagonalisable, nous supposons donc que $\dim E = n \geq 2$. Nous procédons par récurrence sur le nombre de vecteurs propres connus de u . Supposons avoir déjà trouvé p vecteurs propres $e_1, \dots, e_p$ de u . Considérons H , un hyperplan qui contient les vecteurs $e_1, \dots, e_p$. Soit F un supplémentaire de H stable par u ; par construction $\dim F = 1$ et si $e_{p+1} \in F$, il doit être vecteur propre de u .

(1) implique (2) Nous supposons maintenant que u est diagonalisable. Soient $\lambda_1, \dots, \lambda_r$ les valeurs propres deux à deux distinctes, et considérons le polynôme

$$P(x) = (X - \lambda_1) \dots (X - \lambda_r). \quad (9.272)$$

Alors $P(u) = 0$. En effet si e_i est un vecteur propre pour la valeur propre λ_i ,

$$P(u)e_i = \prod_{j \neq i} (u - \lambda_j) \circ (u - \lambda_i)e_i = 0 \quad (9.273)$$

par le lemme 9.87. Par conséquent $P(u)$ s'annule sur une base.

(5) implique (2) Si la matrice A est diagonale alors le polynôme $P = \prod_{i=1}^n (A - A_{ii} \mathbb{1})$ est annulateur de A .

(3) implique (5) le polynôme minimal de u s'écrit

$$\mu = (X - \lambda_1) \dots (X - \lambda_r), \quad (9.274)$$

et les espaces E_i du lemme 9.128 sont les espaces propres $E_i = \ker(u - \lambda_i)$. Nous avons donc une somme directe

$$E = E_1 \oplus \dots \oplus E_r. \quad (9.275)$$

Dans chacun des espaces propres, u a une matrice diagonale avec la valeur propre correspondante sur la diagonale. Une base de E constituée d'une base de chacun des espaces propres est donc une base comme nous en cherchons. □

Corolaire 9.130.

Si u est diagonalisable et si F est une sous-espace stable par u , alors

$$F = \bigoplus_{\lambda} E_{\lambda}(u) \cap F \quad (9.276)$$

où $E_{\lambda}(u)$ est l'espace propre de u pour la valeur propre λ . En particulier la restriction de u à F , $u|_F$ est diagonalisable.

Démonstration. Par le théorème 9.129, le polynôme μ_u est scindé et ne possède que des racines simples. Notons le

$$\mu_u(X) = (X - \lambda_1) \dots (X - \lambda_r). \quad (9.277)$$

Les espaces E_i du lemme 9.128 sont maintenant les espaces propres.

En ce qui concerne la diagonalisabilité de $u|_F$, notons que nous avons une base de F composée de vecteurs dans les espaces $E_{\lambda}(u)$. Cette base de F est une base de vecteurs propres de u . □

Lemme 9.131.

Soit E un $\mathbb{K}$ -espace vectoriel et $u \in \text{End}(E)$. Si $\text{Card}(\text{Spec}(u)) = \dim(E)$ alors u est diagonalisable.

Démonstration. Soient $\lambda_1, \dots, \lambda_n$ les valeurs propres distinctes de u . Nous savons que les espaces propres correspondants sont en somme directe (lemme 9.85). Par conséquent $\text{Span}\{E_{\lambda_i}(u)\}$ est de dimension n et u est diagonalisable. □

Voici un résultat de diagonalisation simultanée. Nous donnerons un résultat de trigonalisation simultanée dans le lemme 9.211.

Proposition 9.132 (Diagonalisation simultanée).

Soit $(u_i)_{i \in I}$ une famille d'endomorphismes qui commutent deux à deux.

- (1) Si $i, j \in I$ alors tout sous-espace propre de u_i est stable par u_j . Autrement dit $u_j(E_\lambda(u_i)) \subset E_\lambda(u_i)$.
- (2) Si les u_i sont diagonalisables, alors ils le sont simultanément.

Démonstration. Supposons que u_i et u_j commutent et soit x un vecteur propre de u_i : $u_i x = \lambda x$. Nous montrons que $u_j x \in E_\lambda(u_i)$. Nous avons

$$u_i(u_j(x)) = u_j(u_i(x)) = \lambda u_j(x). \quad (9.278)$$

Par conséquent $u_j(x)$ est vecteur propre de u_i de valeur propre λ .

Montrons maintenant l'affirmation à propos des endomorphismes simultanément diagonalisables. Si $\dim E = 1$, le résultat est évident. Nous supposons également qu'aucun des u_i n'est multiple de l'identité. Nous effectuons une récurrence sur la dimension.

Soit u_0 un des u_i et considérons ses valeurs propres deux à deux distinctes $\lambda_1, \dots, \lambda_r$. Pour chaque k nous avons

$$E_{\lambda_k}(u_0) \neq E, \quad (9.279)$$

sinon u_0 serait un multiple de l'identité. Par contre le fait que u_0 soit diagonalisable permet de décomposer E en espaces propres de u_0 :

$$E = \bigoplus_k E_{\lambda_k}(u_0). \quad (9.280)$$

Ce que nous allons faire est de simultanément diagonaliser les $(u_i)_{i \in I}$ sur chacun des E_{λ_k} séparément. Par le point (1), nous avons $u_i : E_{\lambda_k}(u_0) \rightarrow E_{\lambda_k}(u_0)$, et nous pouvons considérer la famille d'opérateurs

$$\left(u_i|_{E_{\lambda_k}(u_0)} \right)_{i \in I}. \quad (9.281)$$

Ce sont tous des opérateurs qui commutent et qui agissent sur un espace de dimension plus petite. Par hypothèse de récurrence nous avons une base de $E_{\lambda_k}(u_0)$ qui diagonalise tous les u_i . $\square$

Exemple 9.133.

Soit un espace vectoriel sur un corps $\mathbb{K}$. Un opérateur **involutif** est un opérateur différent de l'identité dont le carré est l'identité. Typiquement une symétrie orthogonale dans $\mathbb{R}^3$. Le polynôme caractéristique d'une involution est $X^2 - 1 = (X + 1)(X - 1)$.

Tant que $1 \neq -1$, $X^2 - 1$ est donc scindé à racines simples et les involutions sont diagonalisables (9.129). Cependant si le corps est de caractéristique 2, alors $X^2 - 1 = (X + 1)^2$ et l'involution n'est plus diagonalisable.

Par exemple si le corps est de caractéristique 2, nous avons

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad (9.282a)$$

$$A^1 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \quad (9.282b)$$

Ce A est donc une involution mais n'est pas diagonalisable. $\triangle$

9.7.4 Diagonalisation : cas complexe, pas toujours

Il n'est pas vrai qu'une matrice de $\mathbb{M}(n, \mathbb{C})$ soit toujours diagonalisable. En effet le théorème 9.129(3) dit qu'une matrice est diagonalisable si et seulement si son polynôme minimal est scindé à racines simples. Certes sur $\mathbb{C}$ le polynôme minimal sera scindé, mais il ne sera pas spécialement à racines simples.

Exemple 9.134.

La matrice

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad (9.283)$$

a pour polynôme caractéristique $\chi_A(X) = X^2$. Cela est également son polynôme minimal, et ce n'est pas à racine simple.

Il est par ailleurs facile de voir que le seul espace propre de A est $\text{Span}\{(1, 0)\}$ (ici le span est sur $\mathbb{C}$). Donc l'espace $\mathbb{C}^2$ ne possède pas de base de vecteurs propres de A . $\triangle$

Ce qui est vrai, c'est que le polynôme caractéristique a des racines, et que ces racines correspondent à des vecteurs propres. Mais il n'y a pas toujours autant de vecteurs propres que la multiplicité des racines.

9.7.5 Trigonalisation : généralités

Définition 9.135 ([204]).

Une matrice dans $\mathbb{M}(n, \mathbb{K})$ est **trigonalisable** lorsqu'elle est semblable⁴³ à une matrice triangulaire supérieure.

Proposition 9.136 (Trigonalisation et polynôme caractéristique scindé).

Soit u un endomorphisme d'un espace vectoriel E sur le corps $\mathbb{K}$. Les faits suivants sont équivalents.

- (1) L'endomorphisme u est trigonalisable (auquel cas les valeurs propres sont sur la diagonale).
- (2) Le polynôme caractéristique de u est scindé⁴⁴.

Démonstration. (2) $\Rightarrow$ (1) Nous avons par hypothèse que

$$\chi_u(X) = \prod_{i=1}^r (X - \lambda_i)^{\alpha_i} \quad (9.284)$$

où les λ_i sont les valeurs propres de u . Le théorème de Cayley-Hamilton 9.116 dit que $\chi_u(u) = 0$, ce qui permet d'utiliser le théorème de décomposition des noyaux 9.88 :

$$E = \ker(X - \lambda_1)^{\alpha_1} \oplus \dots \oplus \ker(X - \lambda_r)^{\alpha_r}. \quad (9.285)$$

Les espaces $F_{\lambda_i}(u) = \ker(X - \lambda_i)^{\alpha_i}$ sont les espaces caractéristiques de u , ce qui fait que $u - \lambda_i \mathbb{1}$ est nilpotent sur $F_{\lambda_i}(u)$. L'endomorphisme $u - \lambda_i \mathbb{1}$ est donc strictement trigonalisable supérieur sur son bloc⁴⁵. Cela signifie que u est triangulaire supérieure avec les valeurs propres sur la diagonale.

(1) $\Rightarrow$ (2) C'est immédiat parce que le déterminant d'une matrice triangulaire est le produit des éléments de sa diagonale. □

Remarque 9.137.

La méthode des pivots de Gauss⁴⁶ certes permet de trigonaliser n'importe quoi, mais elle ne

43. Définition 9.120.

44. Définition 6.34.

45. Proposition 9.123.

46. Le lemme 4.107.

correspond pas à un changement de base. Autrement dit, les pivots de Gauss ne sont pas de similitudes.

C'est là qu'il faut bien avoir en tête la différence entre *équivalence* et *similarité*⁴⁷. Lorsqu'on parle de changement de base, de matrice trigonalisable ou diagonalisable, nous parlons de similarité et non d'équivalence.

9.7.6 Trigonalisation : cas complexe

La proposition 9.136 dit déjà que tous les endomorphismes sont trigonalisables sur $\mathbb{C}$. Nous allons aller plus loin et montrer que la trigonalisation peut être effectuée à l'aide d'une matrice unitaire.

Une démonstration alternative passant par le polynôme caractéristique sera présentée dans la remarque 9.141 utilisant la proposition 9.136.

Lemme 9.138 (Lemme de Schur complexe, trigonalisation[205]).

Si $A \in \mathbb{M}(n, \mathbb{C})$, il existe une matrice unitaire U telle que UAU^{-1} soit triangulaire supérieure⁴⁸.

Démonstration. Étant donné que $\mathbb{C}$ est algébriquement clos, nous pouvons toujours considérer un vecteur propre v_1 de A , de valeur propre λ_1 . Nous pouvons utiliser un procédé de Gram-Schmidt pour construire une base orthonormée $\{v, u_2, \dots, u_n\}$ de $\mathbb{R}^n$, et la matrice (unitaire)

$$Q = \begin{pmatrix} \uparrow & \uparrow & \cdots & \uparrow \\ v & u_2 & \cdots & u_n \\ \downarrow & \downarrow & & \downarrow \end{pmatrix}. \quad (9.286)$$

Nous avons $Q^{-1}AQe_1 = Q^{-1}Av = \lambda Q^{-1}v = \lambda e_1$, par conséquent la matrice $Q^{-1}AQ$ est de la forme

$$Q^{-1}AQ = \begin{pmatrix} \lambda_1 & * \\ 0 & A_1 \end{pmatrix} \quad (9.287)$$

où $*$ représente une ligne quelconque et A_1 est une matrice de $\mathbb{M}(n-1, \mathbb{C})$. Nous pouvons donc répéter le processus sur A_1 et obtenir une matrice triangulaire supérieure (nous utilisons le fait qu'un produit de matrices orthogonales est une matrice orthogonale). $\square$

En particulier les matrices hermitiennes, anti-hermitiennes et unitaires sont trigonalisables par une matrice unitaire, qui peut être choisie de déterminant 1.

Lemme 9.139.

Soit $A \in \mathbb{M}(n, \mathbb{C})$ et une matrice unitaire U telle que $A = UTU^{-1}$ où T est triangulaire.

- (1) En ce qui concerne les polynômes caractéristiques, $\chi_A = \chi_T$.
- (2) Pour les spectres, $\text{Spec}(A) = \text{Spec}(T)$.
- (3) Les valeurs propres de A sont les éléments diagonaux de T .

Démonstration. Vu que U commute évidemment avec $\mathbb{1}$ nous avons

$$\chi_A(\lambda) = \det(A - \lambda\mathbb{1}) = \det(UTU^{-1} - \lambda\mathbb{1}) = \det(U(T - \lambda\mathbb{1})U^{-1}). \quad (9.288)$$

À ce niveau nous utilisons le fait que le déterminant soit multiplicatif 9.9 pour conclure :

$$\chi_A(\lambda) = \det(U(T - \lambda\mathbb{1})U^{-1}) = \det(U) \det(T - \lambda\mathbb{1}) \det(U^{-1}) = \det(T - \lambda\mathbb{1}) = \chi_T(\lambda). \quad (9.289)$$

Pour les spectres, l'égalité des polynômes caractéristique implique l'égalité des spectres parce que les valeurs propres sont les racines du polynôme caractéristique par le théorème 9.112.

Les valeurs propres d'une matrice triangulaire sont les valeurs sur la diagonale. $\square$

47. Définition 4.106.

48. « triangulaire supérieure » ne signifie pas « strictement triangulaire supérieure ». Ici, il est possible que la diagonale soit non nulle ; non seulement possible, mais même très probable en pratique.

Remarque 9.140.

Le lemme mentionne le fait que les valeurs propres de A sont les éléments diagonaux de T . Mais attention : ceci ne dit rien au niveau des multiplicités géométriques. Un nombre peut être cinq fois sur la diagonale de T alors que l'espace propre correspondant pour A n'est que de dimension 1. Exemple : la matrice

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad (9.290)$$

a deux 1 sur la diagonale. Le nombre 1 est bien une valeur propre de A , mais le système

$$A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \quad (9.291)$$

donne $y = 0$ et donc un espace propre de dimension seulement 1.

Remarque 9.141.

Si $\mathbb{K}$ est algébriquement clos (comme $\mathbb{C}$ par exemple), alors tous les polynômes sont scindés et toutes les matrices sont trigonalisables⁴⁹. Un exemple un peu simple de cela est la matrice

$$u = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \quad (9.292)$$

Le polynôme caractéristique est $\chi_u(X) = X^2 + 1$ et les valeurs propres sont $\pm i$. Il est vite vu que dans la base

$$\left\{ \begin{pmatrix} i \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ i \end{pmatrix} \right\} \quad (9.293)$$

de $\mathbb{C}^2$, la matrice u se note $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$.

Remarque 9.142.

Cela nous donne une autre façon de prouver qu'une matrice nilpotente de $M(n, \mathbb{C})$ ou $M(n, \mathbb{R})$ est trigonalisable[206]. D'abord dans $M(n, \mathbb{C})$, toutes les matrices sont trigonalisables⁵⁰, et les valeurs propres arrivent sur la diagonale. Mais comme les valeurs propres d'une matrice nilpotente sont zéro, elle est triangulaire stricte. Par ailleurs son polynôme caractéristique est alors X^n .

Ensuite si $u \in M(n, \mathbb{R})$ nous pouvons voir u comme une matrice dans $M(n, \mathbb{C})$ et y calculer son polynôme caractéristique qui sera tout de même X^n . Ce polynôme étant scindé, la proposition 9.136 nous assure que u est trigonalisable. Une fois de plus, les valeurs propres étant sur la diagonale, elle est triangulaire supérieure stricte.

Corolaire 9.143.

Le polynôme caractéristique⁵¹ sur $\mathbb{C}$ d'une matrice s'écrit sous la forme

$$\chi_A(X) = \prod_{i=1}^r (X - \lambda_i)^{m_i} \quad (9.294)$$

où les λ_i sont les valeurs propres distinctes de A et m_i sont les multiplicités correspondantes.

Démonstration. Le lemme 9.138 nous donne l'existence d'une base de trigonalisation ; dans cette base les valeurs propres de A sont sur la diagonale et nous avons

$$\chi_A(X) = \det(A - X\mathbb{1}) = \det \begin{pmatrix} X - \lambda_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & X - \lambda_r \end{pmatrix}, \quad (9.295)$$

qui vaut bien le produit annoncé. □

49. La proposition 9.136 montre cela, et le lemme de Schur complexe 9.138 va un peu plus loin et précise que la trigonalisation peut être faite par une matrice unitaire.

50. Parce que le polynôme caractéristique est scindé, voir la proposition 9.136..

51. Définition 9.108.

Corolaire 9.144.

Si $A \in \mathbb{M}(n, \mathbb{C})$ et $k \in \mathbb{N}$ alors

$$\text{Spec}(A^k) = \{\lambda^k \text{ tel que } \lambda \in \text{Spec}(A)\}. \quad (9.296)$$

Démonstration. Par le lemme 9.138 nous avons une matrice unitaire U et une triangulaire T telles que $A = UTU^{-1}$. En passant à la puissance k nous avons aussi

$$A^k = UT^kU^{-1}. \quad (9.297)$$

Donc le spectre de A^k est celui de T^k (lemme 9.139 et le fait qu'une puissance d'une matrice triangulaire est encore triangulaire). Or les éléments diagonaux de T^k sont les puissances k^{e} des éléments diagonaux de T , qui sont les valeurs propres de A . $\square$

Pour le cas complexe, c'est le lemme 11.20 et le théorème 11.23.

9.7.7 Diagonalisation : cas réel**Lemme 9.145** (Lemme de Schur réel).

Soit $A \in \mathbb{M}(n, \mathbb{R})$. Il existe une matrice orthogonale Q telle que $Q^{-1}AQ$ soit de la forme

$$Q^{-1}AQ = \begin{pmatrix} \lambda_1 & * & * & * & * \\ 0 & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \lambda_r & * & * \\ 0 & 0 & 0 & \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} & * \\ 0 & 0 & 0 & 0 & \begin{pmatrix} a_s & b_s \\ c_s & d_s \end{pmatrix} \end{pmatrix}. \quad (9.298)$$

Le déterminant de A est le produit des déterminants des blocs diagonaux et les valeurs propres de A sont les $\lambda_1, \dots, \lambda_r$ et celles de ces blocs.

Démonstration. Si la matrice A a des valeurs propres réelles, nous procédons comme dans le cas complexe. Cela nous fournit la partie véritablement triangulaire avec les valeurs propres $\lambda_1, \dots, \lambda_r$ sur la diagonale. Supposons donc que A n'a pas de valeurs propres réelles. Soit donc $\alpha + i\beta$ une valeur propre ($\beta \neq 0$) et $u + iv$ un vecteur propre correspondant où u et v sont des vecteurs réels. Nous avons

$$Au + iAv = A(u + iv) = (\alpha + i\beta)(u + iv) = \alpha u - \beta v + i(\alpha v + \beta u), \quad (9.299)$$

et en égalisant les parties réelles et imaginaires,

$$Au = \alpha u - \beta v \quad (9.300a)$$

$$Av = \alpha v + \beta u. \quad (9.300b)$$

Sur ces relations nous voyons que ni u ni v ne sont nuls. De plus u et v sont linéairement indépendants (sur $\mathbb{R}$), en effet si $v = \lambda u$ nous aurions $Au = \alpha u - \beta \lambda u = (\alpha - \beta \lambda)u$, ce qui serait une valeur propre réelle alors que nous avons supposé avoir déjà épuisé toutes les valeurs propres réelles.

Étant donné que u et v sont deux vecteurs réels non nuls et linéairement indépendants, nous pouvons trouver une base orthonormée $\{q_1, q_2\}$ de $\text{Span}\{u, v\}$. Nous pouvons étendre ces deux vecteurs en une base orthonormée $\{q_1, q_2, q_3, \dots, q_n\}$ de $\mathbb{R}^n$. Nous considérons à présent la matrice orthogonale dont les colonnes sont formées de ces vecteurs : $Q = [q_1 \ q_2 \ \dots \ q_n]$.

L'espace $\text{Span}\{e_1, e_2\}$ est stable par $Q^{-1}AQ$, en effet nous avons

$$Q^{-1}AQe_1 = Q^{-1}Aq_1 = Q^{-1}(aq_1 + bq_2) = ae_1 + be_2. \quad (9.301)$$

La matrice $Q^{-1}AQ$ est donc de la forme

$$Q^{-1}AQ = \begin{pmatrix} \begin{pmatrix} \cdot & \cdot \\ \cdot & \cdot \end{pmatrix} & C_1 \\ 0 & A_1 \end{pmatrix} \quad (9.302)$$

où C_1 est une matrice réelle $2 \times (n-1)$ quelconque et A_1 est une matrice réelle $(n-2) \times (n-2)$. Nous pouvons appliquer une récurrence sur la dimension pour poursuivre.

Notons que si A n'a pas de valeurs propres réelles, elle est automatiquement d'ordre pair parce que les valeurs propres complexes viennent par couple complexes conjuguées.

En ce qui concerne les valeurs propres, il est facile de voir en regardant (9.298) que les valeurs propres sont celles des blocs diagonaux. Étant donné que $Q^{-1}AQ$ et A ont même polynôme caractéristique, ce sont les valeurs propres de A . $\square$

Théorème 9.146 (Théorème spectral, matrice symétrique[79]).

Une matrice symétrique réelle,

(1) a un spectre contenu dans $\mathbb{R}$

(2) est diagonalisable par une matrice orthogonale.

Si M est une matrice symétrique réelle alors $\mathbb{R}^n$ possède une base orthonormée de vecteurs propres de M .

Démonstration. Soit A une matrice réelle symétrique. Si λ est une valeur propre complexe pour le vecteur propre complexe v , alors d'une part $\langle Av, v \rangle = \lambda \langle v, v \rangle$ et d'autre part $\langle Av, v \rangle = \langle v, Av \rangle = \bar{\lambda} \langle v, v \rangle$. Par conséquent $\lambda = \bar{\lambda}$.

Le lemme de Schur réel 9.145 donne une matrice orthogonale qui trigonalise A . Les valeurs propres étant toutes réelles, la matrice $Q^{-1}AQ$ est même triangulaire (il n'y a pas de blocs dans la forme (9.298)). Prouvons que $Q^{-1}AQ$ est symétrique :

$$(Q^{-1}AQ)^t = (Q^{-1})^t A^t Q^t = Q^t A^t Q^{-1} = Q^t A Q^{-1} = Q^{-1}AQ \quad (9.303)$$

où nous avons utilisé le fait que Q était orthogonale ($Q^{-1} = Q^t$) et que A était symétrique ($A^t = A$). Une matrice triangulaire supérieure symétrique est obligatoirement une matrice diagonale.

En ce qui concerne la base de vecteurs propres, soit $\{e_i\}_{i=1,\dots,n}$ la base canonique de $\mathbb{R}^n$ et Q une matrice orthogonale telle que $A = Q^t D Q$ avec D diagonale. Nous posons $f_i = Q^t e_i$ et en tenant compte du fait que $Q^t = Q^{-1}$ nous avons $A f_i = Q^t D Q Q^t e_i = Q^t D e_i = \lambda_i Q^t e_i = \lambda_i f_i$. Donc les f_i sont des vecteurs propres de A . De plus ils sont orthonormés parce que

$$\langle f_i, f_j \rangle = \langle Q^t e_i, Q^t e_j \rangle = \langle e_i, Q Q^t e_j \rangle = \langle e_i, e_j \rangle = \delta_{ij}. \quad (9.304)$$

$\square$

Le théorème spectral pour les opérateurs autoadjoints sera traité plus bas parce qu'il a besoin de choses sur les formes bilinéaires, théorème 11.5.

Remarque 9.147.

Une matrice symétrique est diagonalisable par une matrice orthogonale. Nous pouvons en réalité nous arranger pour diagonaliser par une matrice de $SO(n)$. Plus généralement si A est une matrice diagonalisable par une matrice $P \in GL^+(n, \mathbb{R})$ alors elle est diagonalisable par une matrice de $GL^-(n, \mathbb{R})$ en changeant le signe de la première ligne de P . Et inversement.

En effet, si nous avons $P^t D P = A$, alors en notant * les quantités qui ne dépendent pas de a , b ou c ,

$$\begin{aligned} \begin{pmatrix} a & * & * \\ b & * & * \\ c & * & * \end{pmatrix} \begin{pmatrix} \lambda_1 & & \\ & \lambda_2 & \\ & & \lambda_3 \end{pmatrix} \begin{pmatrix} a & b & c \\ * & * & * \\ * & * & * \end{pmatrix} &= \begin{pmatrix} a & * & * \\ b & * & * \\ c & * & * \end{pmatrix} \begin{pmatrix} \lambda_1 a & \lambda_1 b & \lambda_1 c \\ * & * & * \\ * & * & * \end{pmatrix} \\ &= \begin{pmatrix} \lambda_1 a^2 + * & \lambda_1 ab + * & \lambda_1 ac + * \\ \dots & \dots & \dots \\ \dots & \dots & \dots \end{pmatrix}. \end{aligned} \quad (9.305)$$

Nous voyons donc que si nous changeons les signes de a , b et c en même temps, le résultat ne change pas.

Définition 9.148 (Matrice définie positive, opérateur défini positif).

Un opérateur sur un espace vectoriel sur $\mathbb{C}$ ou $\mathbb{R}$ est **défini positif** si toutes ses valeurs propres sont réelles et strictement positives. Il est **semi-défini positif** si ses valeurs propres sont réelles positives ou nulles.

Même définitions pour une matrice.

Afin d'éviter l'une ou l'autre confusion, nous disons souvent *strictement* définie positive pour positive.

9.149.

Nous nommons $S^+(n, \mathbb{R})$ l'ensemble des matrices réelles symétriques $n \times n$ et $S^{++}(n, \mathbb{R})$ le sous-ensemble de $S^+(n, \mathbb{R})$ des matrices strictement définies positives.

Remarque 9.150.

Nous ne définissons pas la notion de matrice définie positive pour une matrice non symétrique.

Proposition 9.151.

Soit M , une matrice symétrique. Nous avons

- (1) $\det(M) > 0$ et $\text{Tr}(M) > 0$ implique M définie positive⁵²,
- (2) $\det(M) > 0$ et $\text{Tr}(M) < 0$ implique M définie négative,
- (3) $\det(M) < 0$ implique ni semi-définie positive, ni définie négative
- (4) $\det(M) = 0$ implique M semi-définie positive ou semi-définie négative.

Lorsqu'un énoncé parle d'une matrice symétrique, le premier réflexe est de la diagonaliser : considérer une matrice orthogonale T telle que $T^t M T = D$ avec D diagonale. Et les valeurs propres sur la diagonale : $D_{kl} = \delta_{kl} \lambda_k$. Les matrices symétriques définies positives ont cependant des propriétés même en dehors de leur base de diagonalisation.

Lemme 9.152.

Soit une matrice symétrique M .

- (1) Elle est strictement définie positive si et seulement si $\langle x, Mx \rangle > 0$ pour tout x non nul dans $\mathbb{R}^n$.
- (2) Elle est semi-définie positive si et seulement si $\langle x, Mx \rangle \geq 0$ pour tout x non nul dans $\mathbb{R}^n$.
- (3) Si elle est seulement définie positive, alors $\langle x, Mx \rangle \geq \lambda \|x\|^2$ dès que $\lambda \geq 0$ minore toutes les valeurs propres.

Démonstration. Démonstration en trois parties.

(1) Soit $\{e_i\}_{i=1,\dots,n}$ une base orthonormée de vecteurs propres de M dont l'existence est assurée par le théorème spectral 9.146. Nous nommons x_i les coordonnées de x dans cette base. Alors,

$$\langle x, Mx \rangle = \sum_{i,j} x_i \langle e_i, x_j M e_j \rangle = \sum_{i,j} x_i x_j \langle e_i, \lambda_j e_j \rangle = \sum_{i,j} x_i x_j \lambda_j \delta_{ij} = \sum_i \lambda_i x_i^2 \quad (9.306)$$

où les λ_i sont les valeurs propres de M . Cela est strictement positif pour tout x si et seulement si tous les λ_i sont strictement positifs.

(2) Nous avons encore

$$\langle x, Mx \rangle = \sum_i \lambda_i x_i^2. \quad (9.307)$$

Cela est plus grand ou égal à zéro si et seulement si tous les λ_i sont plus grands ou égaux à zéro.

52. Définition 9.148.

(3) Soit une matrice orthogonale T diagonalisant M , c'est-à-dire telle que $T^t M T = D$ avec D diagonale. Nous allons vérifier que

$$\langle Tx, MTx \rangle \geq \lambda \|Tx\|^2 \quad (9.308)$$

pour tout x . Vu que T est une bijection⁵³, cela impliquera le résultat pour tout x . Si nous considérons la base de diagonalisation $\{e_k\}$ pour les valeurs propres λ_k , nous avons le calcul

$$\langle Tx, MTx \rangle = \langle x, T^t M T x \rangle \quad (9.309a)$$

$$= \langle x, D x \rangle \quad (9.309b)$$

$$= \sum_k \langle x, x_k D e_k \rangle \quad (9.309c)$$

$$= \sum_k \lambda_k x_k \underbrace{\langle x, e_k \rangle}_{=x_k} \quad (9.309d)$$

$$\geq \sum_k \lambda |x_k|^2 \quad (9.309e)$$

$$= \lambda \|x\|^2 \quad (9.309f)$$

$$= \lambda \|Tx\|^2. \quad (9.309g)$$

Au dernier passage nous avons utilisé le fait que T est une isométrie (proposition 9.41). □

Les personnes qui aiment les vecteurs lignes et colonnes écriront des inégalités comme

$$x^t M x \geq x^t x. \quad (9.310)$$

Tout à l'autre bout du spectre des personnes névrosées des notations, on trouvera des inégalités comme

$$M(x \otimes x) \geq x \cdot x. \quad (9.311)$$

Le penchant personnel de l'auteur de ces lignes est la notation avec le produit tensoriel. Si vous aimez ça, vous pouvez lire la section 11.10.5 et en particulier ce qui suit (11.477).

La notation adoptée ici avec le produit scalaire $\langle x, Mx \rangle$, qui peut aussi être écrite $x \cdot Mx$ est entre les deux. Elle a l'avantage de n'être pas technologique comme le produit tensoriel (si vous y mettez les pieds, vous devez savoir ce que vous faites), tout en évitant de se casser la tête à savoir qui est un vecteur ligne ou un vecteur colonne.

Corolaire 9.153.

Une matrice symétrique strictement définie positive est inversible.

Démonstration. Si $Ax = 0$ alors $\langle Ax, x \rangle = 0$. Mais dans le cas d'une matrice strictement définie positive, cela implique $x = 0$ par le lemme 9.152. □

Lemme 9.154.

Pour une base quelconque, les éléments diagonaux d'une matrice symétrique semi-définie positive sont positifs. Si la matrice est strictement définie positive, alors les éléments diagonaux sont strictement positifs.

Démonstration. Il s'agit d'une application du lemme 9.152. Si A est définie positive et que $\{e_i\}$ est une base, alors

$$A_{ii} = \langle Ae_i, e_i \rangle \geq \lambda \|e_i\|^2 = \lambda \geq 0. \quad (9.312)$$

Si A est strictement définie positive, alors λ peut être choisi strictement positif. □

53. Une matrice orthogonale a un déterminant ± 1 .

9.8 Fonctions

Soient $(V, \|\cdot\|_V)$ et $(W, \|\cdot\|_W)$ deux espaces vectoriels normés, et une fonction f de V dans W . Il est maintenant facile de définir les notions de limites et de continuité pour de telles fonctions en copiant les définitions données pour les fonctions de $\mathbb{R}$ dans $\mathbb{R}$ en changeant simplement les valeurs absolues par les normes sur V et W .

La proposition suivante explicite la définition 7.70 dans le cas où la topologie est donnée par des boules.

Proposition 9.155 (Caractérisation de la limite).

Soient des espaces vectoriels normés. Soit $f: V \rightarrow W$ une fonction de domaine $\text{Dom}(f) \subset V$ et soit a un point d'accumulation de $\text{Dom}(f)$.

- (1) Si W est séparé⁵⁴ et si f admet une limite en a , alors cette limite est unique.
- (2) La fonction f admet une limite en $a \in V$ si et seulement s'il existe un élément $\ell \in W$ tel que pour tout $\varepsilon > 0$, il existe un $\delta > 0$ tel que pour tout $x \in \text{Dom}(f)$,

$$0 < \|x - a\|_V < \delta \Rightarrow \|f(x) - \ell\|_W < \varepsilon. \quad (9.313)$$

Si la limite existe et est unique, nous écrivons $\lim_{x \rightarrow a} f(x) = \ell$ et nous disons que ℓ est la **limite** de f lorsque x tend vers a .

Démonstration. L'unicité est la proposition 7.73.

$\Rightarrow$ La définition 7.70 nous assure de l'existence d'un élément ℓ tel que pour tout voisinage S de ℓ , il existe un ouvert U autour de a tel que $f(U \cap D \setminus \{a\}) \subset S$.

Soit $\epsilon > 0$. Nous posons $S = B(\ell, \epsilon)$. Il existe un voisinage U de a tel que $f(U \cap D \setminus \{a\}) \subset B(\ell, \epsilon)$. Vu que S est un voisinage de a , il contient une boule centrée en a (c'est dans la définition 7.99 de la topologie métrique). Soit donc $\delta > 0$ tel que $B(a, \delta) \subset U$.

Un élément de D qui est dans $B(0, \delta) \setminus \{a\}$ est un élément de D qui vérifie $0 < \|x - a\| < \delta$. Nous avons donc, pour $x \in D$ que

$$0 < \|x - a\| < \delta \Rightarrow \|f(x) - \ell\| < \epsilon. \quad (9.314)$$

$\Leftarrow$ C'est le même raisonnement.

□

Remarque 9.156.

Le fait que nous limitons la formule (9.313) aux x dans le domaine de f n'est pas anodin. Considérons la fonction $f(x) = \sqrt{x^2 - 4}$, de domaine $|x| \geq 2$. Nous avons

$$\lim_{x \rightarrow 2} \sqrt{x^2 - 4} = 0. \quad (9.315)$$

Nous ne pouvons pas dire que cette limite n'existe pas en justifiant que la limite à gauche n'existe pas. Les points $x < 2$ sont hors du domaine de f et ne comptent donc pas dans l'appréciation de l'existence de la limite.

Vous verrez plus tard que ceci provient de la **topologie induite** de $\mathbb{R}$ sur l'ensemble $[2, \infty[$.

9.9 Sous espaces caractéristiques

Lorsqu'un opérateur n'est pas diagonalisable, les valeurs propres jouent quand même un rôle important.

54. C'est le cas en dimension finie et en particulier pour $\mathbb{R}^n$. En dimension infinie, il faut être très prudent.

Définition 9.157.

Soit E un $\mathbb{K}$ -espace vectoriel $f \in \text{End}(E)$. Pour $\lambda \in \mathbb{K}$ nous définissons

$$F_\lambda(f) = \{v \in E \text{ tel que } (f - \lambda \mathbb{1})^n v = 0, n \in \mathbb{N}\} \quad (9.316)$$

et nous appelons ça un **sous-espace caractéristique** de f .

L'espace $F_\lambda(f)$ est l'ensemble de nilpotence de l'opérateur $f - \lambda \mathbb{1}$ et

Lemme 9.158.

L'ensemble $F_\lambda(f)$ est non vide si et seulement si λ est une valeur propre de f . L'espace $F_\lambda(f)$ est invariant sous f .

Démonstration. Si $F_\lambda(f)$ est non vide, nous considérons $v \in F_\lambda(f)$ et n le plus petit entier non nul tel que $(f - \lambda)^n v = 0$. Alors $(f - \lambda)^{n-1} v$ est un vecteur propre de f pour la valeur propre λ . Inversement si v est une valeur propre de f pour la valeur propre λ , alors $v \in F_\lambda(f)$.

En ce qui concerne l'invariance, remarquons que f commute avec $f - \lambda \mathbb{1}$. Si $x \in F_\lambda(f)$ il existe n tel que $(f - \lambda \mathbb{1})^n x = 0$. Nous avons aussi

$$(f - \lambda \mathbb{1})^n f(x) = f((f - \lambda \mathbb{1})^n x) = 0, \quad (9.317)$$

par conséquent $f(x) \in F_\lambda(f)$. □

Remarque 9.159.

Toute matrice sur $\mathbb{C}$ n'est pas diagonalisable : nous en avons déjà donné un exemple simple en 9.210. Nous en voyons maintenant un moins simple. Considérons en effet l'endomorphisme f donné par la matrice

$$\begin{pmatrix} a & \alpha & \beta \\ 0 & a & \gamma \\ 0 & 0 & b \end{pmatrix} \quad (9.318)$$

où $a \neq b$, $\alpha \neq 0$, β et γ sont des nombres complexes quelconques. Son polynôme caractéristique est

$$\chi_f(\lambda) = (a - \lambda)^2(b - \lambda), \quad (9.319)$$

et les valeurs propres sont donc a et b . Nous trouvons les vecteurs propres pour la valeur a en résolvant

$$\begin{pmatrix} a & \alpha & \beta \\ 0 & a & \gamma \\ 0 & 0 & b \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} ax \\ ay \\ az \end{pmatrix}. \quad (9.320)$$

L'espace propre $E_a(f)$ est réduit à une seule dimension générée par $(1, 0, 0)$. De la même façon l'espace propre correspondant à la valeur propre b est donné par

$$\begin{pmatrix} \frac{1}{b-a} \left(\beta + \frac{\alpha\gamma}{b-a} \right) \\ \frac{\gamma}{b-a} \\ 1 \end{pmatrix}. \quad (9.321)$$

Il n'y a donc pas trois vecteurs propres linéairement indépendants, et l'opérateur f n'est pas diagonalisable.

Par contre nous pouvons voir que

$$(f - a \mathbb{1})^2 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a & \alpha & \beta \\ 0 & a & \gamma \\ 0 & 0 & b \end{pmatrix} \begin{pmatrix} \alpha \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} a\alpha \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \quad (9.322)$$

de telle sorte que le vecteur $(0, 1, 0)$ soit également dans l'espace caractéristique $F_a(f)$.

Dans cet exemple, la multiplicité algébrique de la racine a du polynôme caractéristique vaut 2 tandis que sa multiplicité géométrique vaut seulement 1.

9.9.1 Théorèmes de décomposition

Théorème 9.160 (Théorème spectral, décomposition primaire).

Soit E espace vectoriel de dimension finie sur le corps algébriquement clos $\mathbb{K}$ et $f \in \text{End}(E)$. Alors

$$E = F_{\lambda_1}(f) \oplus \dots \oplus F_{\lambda_r}(f) \quad (9.323)$$

où la somme est sur les valeurs propres distinctes de f .

Les projecteurs sur les espaces caractéristique forment un système complet et orthogonal.

Démonstration. Soit P le polynôme caractéristique de f et une décomposition

$$P = (f - \lambda_1)^{\alpha_1} \dots (f - \lambda_r)^{\alpha_r} \quad (9.324)$$

en facteurs irréductibles. La le théorème de noyaux (9.88) nous avons

$$E = \ker(f - \lambda_1)^{\alpha_1} \oplus \dots \oplus \ker(f - \lambda_r)^{\alpha_r}. \quad (9.325)$$

Les projecteurs sont des polynômes en f et forment un système orthogonal. Il nous reste à prouver que $\ker(f - \lambda_i)^{\alpha_i} = F_{\lambda_i}(f)$. L'inclusion

$$\ker(f - \lambda_i)^{\alpha_i} \subset F_{\lambda_i}(f) \quad (9.326)$$

est évidente. Nous devons montrer l'inclusion inverse. Prouvons que la somme des $F_{\lambda_i}(f)$ est directe. Si $v \in F_{\lambda_i}(f) \cap F_{\lambda_j}(f)$, alors il existe $v_1 = (f - \lambda_i)^n v \neq 0$ avec $(f - \lambda_i)v_1 = 0$. Étant donné que $(f - \lambda_i)$ commute avec $(f - \lambda_j)$, ce v_1 est encore dans $F_{\lambda_j}(f)$ et par conséquent il existe $w = (f - \lambda_j)^m v_1$ non nul tel que

$$\begin{cases} (f - \lambda_i)w = 0 \\ (f - \lambda_j)w = 0. \end{cases} \quad (9.327a)$$

$$\quad (9.327b)$$

Ce w serait donc un vecteur propre simultanément pour les valeurs propres λ_i et λ_j , ce qui est impossible parce que les espaces propres sont linéairement indépendants. Les espaces F_{λ_i} sont donc en somme directe et

$$\sum_i \dim F_{\lambda_i}(f) \leq \dim E. \quad (9.328)$$

En tenant compte de l'inclusion (9.326) nous avons même

$$\dim E = \sum_i \dim \ker(f - \lambda_i)^{\alpha_i} \leq \sum_i \dim F_{\lambda_i}(f) \leq \dim E. \quad (9.329)$$

Par conséquent nous avons $\dim \ker(f - \lambda_i)^{\alpha_i} = \dim F_{\lambda_i}(f)$ et l'égalité des deux espaces. $\square$

⚠ Avertissement/question à la lectrice !! 9.161

Dans le cas où le corps n'est pas algébriquement clos, il paraît qu'il faut remplacer « diagonalisable » par « semi-simple ».

Si l'espace vectoriel est sur un corps algébriquement clos, alors les endomorphismes semi-simples⁵⁵ sont les endomorphismes diagonaux.

Théorème 9.162 (Décomposition de Dunford).

Soit E un espace vectoriel sur le corps algébriquement clos $\mathbb{K}$ et $u \in \text{End}(E)$ un endomorphisme de E .

(1) L'endomorphisme u se décompose de façon unique sous la forme

$$u = s + n \quad (9.330)$$

où s est diagonalisable, n est nilpotent et $[s, n] = 0$.

55. Définition 9.103.

(2) Les endomorphismes s et n sont des polynômes en u et commutent avec u .

(3) Les parties s et n sont données par

$$s = \sum_i \lambda_i p_i \quad (9.331a)$$

$$n = \sum_i (s - \lambda_i \mathbb{1}) p_i \quad (9.331b)$$

où les sommes sont sur les valeurs propres distinctes⁵⁶ de f et où $p_i: E \rightarrow F_{\lambda_i}(u)$ est la projection de E sur $F_{\lambda_i}(u)$.

Démonstration. Le théorème spectral 9.160 nous indique que

$$E = \bigoplus_i F_{\lambda_i}(f). \quad (9.332)$$

Nous considérons l'endomorphisme s de E qui consiste à dilater d'un facteur λ l'espace caractéristique $F_{\lambda}(f)$:

$$s = \sum_i \lambda_i p_i \quad (9.333)$$

où $p_i: E \rightarrow F_{\lambda_i}(u)$ est la projection de E sur $F_{\lambda_i}(u)$.

Nous allons prouver que $[s, f] = 0$ et $n = f - s$ est nilpotent. Cela impliquera que $[s, n] = 0$.

Si $x \in F_{\lambda}(f)$, alors nous avons $sf(x) = \lambda f(x)$ parce que $f(x) \in F_{\lambda}(f)$ tandis que $fs(x) = f(\lambda x) = \lambda f(x)$. Par conséquent f commute avec s .

Pour montrer que $f - s$ est nilpotent, nous en considérons la restriction

$$f - s: F_{\lambda}(f) \rightarrow F_{\lambda}(f). \quad (9.334)$$

Cet opérateur est égal à $f - \lambda \mathbb{1}$ et est par conséquent nilpotent.

Prouvons à présent l'unicité. Soit $u = s' + n'$ une autre décomposition qui satisfait aux conditions : s' est diagonalisable, n' est nilpotent et $[n', s'] = 0$. Commençons par prouver que s' et n' commutent avec u . En multipliant $u = s' + n'$ par s' nous avons

$$s'u = s'^2 + s'n' = s'^2 + n's' = (s' + n')s' = us', \quad (9.335)$$

par conséquent $[u, s'] = 0$. Nous faisons la même chose avec n' pour trouver $[u, n'] = 0$. Notons que pour obtenir ce résultat nous avons utilisé le fait que n' et s' commutent, mais pas leur propriétés de nilpotence et de diagonalisabilité.

Si $s' + n' = s + n$ est une autre décomposition, s' et n' commutent avec u , et par conséquent avec tous les polynômes en u . Ils commutent en particulier avec n et s . Les endomorphismes s et s' sont alors deux endomorphismes diagonalisables qui commutent. Par la proposition 9.132, ils sont simultanément diagonalisables. Dans la base de simultanée diagonalisation, la matrice de l'opérateur $s' - s = n - n'$ est donc diagonale. Mais $n - n'$ est également nilpotent, en effet si A et B sont deux opérateurs nilpotents,

$$(A + B)^n = \sum_{k=0}^n \binom{n}{k} A^k B^{n-k}. \quad (9.336)$$

Si n est assez grand, au moins un parmi A^k ou B^{n-k} est nul.

Maintenant que $n - n'$ est diagonal et nilpotent, il est nul et $n = n'$. Nous avons alors immédiatement aussi $s = s'$.

□

56. C'est-à-dire sur les sous-espaces caractéristiques.

9.9.2 Diverses conséquences

Théorème 9.163.

Soit une matrice $A \in \mathbb{M}(n, \mathbb{C})$. On a que la suite $(A^k x)$ tend vers zéro pour tout x si et seulement si $\rho(A) < 1$ où $\rho(A)$ est le rayon spectral de A .

Démonstration. Dans le sens direct, il suffit de prendre comme x , un vecteur propre de A . Dans ce cas nous avons $A^k x = \lambda^k x$. Mais $\lambda^k x$ ne tend vers zéro que si $|\lambda| < 1$. Donc toutes les valeurs propres de A doivent être plus petite que 1 et $\rho(A) < 1$.

Pour l'autre sens nous utilisons la décomposition de Dunford (théorème 9.162) : il existe une matrice inversible P telle que

$$A = P^{-1}(D + N)P \quad (9.337)$$

où D est diagonale, N est nilpotente et $[D, N] = 0$. Étant donné que $D + N$ est triangulaire, son polynôme caractéristique que

$$\chi_{D+N}(\lambda) = \prod_i (D_{ii} - \lambda). \quad (9.338)$$

Par similitude, c'est le même polynôme caractéristique que celui de A et nous savons alors que la diagonale de D contient les valeurs propres de A .

Par ailleurs nous avons

$$A^k = P^{-1}(D + N)^k P \quad (9.339a)$$

$$= P^{-1} \sum_{j=0}^k \binom{k}{j} D^{k-j} N^j P \quad (9.339b)$$

$$= P^{-1} \sum_{j=0}^{n-1} \binom{k}{j} D^{k-j} N^j P \quad (9.339c)$$

où nous avons utilisé le fait que D et N commutent ainsi que $N^{n-1} = 0$ parce que N est nilpotente. Nous utilisons la norme matricielle usuelle, pour laquelle $\|D\| = \rho(D) = \rho(A)$. Nous avons alors

$$\|(D + N)^k\| \leq \sum_{j=0}^k \binom{k}{j} \rho(D)^{k-j} \|N\|^j. \quad (9.340)$$

Du coup si $\rho(D) < 1$ alors $\|(D + N)^k\| \rightarrow 0$ (et c'est même un si et seulement si). $\square$

Une application de la décomposition de Jordan est l'existence d'un logarithme pour les matrices. La proposition suivant va d'une certaine manière donner un logarithme pour les matrices inversibles complexes. Dans le cas des matrices réelles m telles que $\|m - \mathbb{1}\| < 1$, nous donnerons au lemme 15.135 une formule pour le logarithme sous forme d'une série ; ce logarithme sera réel.

9.9.3 Valeurs singulières

Définition 9.164.

Soit M une matrice $m \times n$ sur $\mathbb{K}$ ($\mathbb{K}$ est $\mathbb{R}$ ou $\mathbb{C}$). Un nombre réel σ est une **valeur singulière** de M s'il existent des vecteurs unitaires $u \in \mathbb{K}^m$, $v \in \mathbb{K}^n$ tels que

$$Mv = \sigma u \quad (9.341a)$$

$$M^* u = \sigma v. \quad (9.341b)$$

Théorème 9.165 (Décomposition en valeurs singulières).

Soit $M \in \mathbb{M}(m \times n, \mathbb{K})$ où $\mathbb{K} = \mathbb{R}, \mathbb{C}$. Alors M se décompose en

$$M = ADB \quad (9.342)$$

où il existe deux matrices unitaires $A \in \mathbb{U}(m \times m)$, $B \in \mathbb{U}(n \times n)$ et une matrice (pseudo)diagonale $D \in \mathbb{M}(m \times n)$ tels que

- (1) $A \in \mathcal{U}(m \times m)$, $B \in \mathcal{U}(n \times n)$ sont deux matrices unitaires ;,
- (2) D est (pseudo)diagonale,
- (3) les éléments diagonaux de D sont les valeurs singulières de M ,
- (4) le nombre d'éléments non nuls sur la diagonale de D est le rang⁵⁷ de M .

Corolaire 9.166.

Soit $M \in \mathcal{M}(n, \mathbb{C})$. Il existe un isomorphisme $f: \mathbb{C}^n \rightarrow \mathbb{C}^n$ tel que fM soit autoadjoint.

Démonstration. Si $M = ADB$ est la décomposition de M en valeurs singulières, alors nous pouvons prendre $f = \overline{B}^t A^{-1}$ qui est une matrice inversible. Pour la vérification que ce f répond bien à la question, ne pas oublier que D est réelle, même si M ne l'est pas. $\square$

9.10 Extension du corps de base

Nous avons discuté dans la section 6.4 de ce qui arrive au corps lorsqu'on l'étend. Dans cette section nous allons étudier ce qui arrive aux applications linéaires entre deux $\mathbb{K}$ -espaces vectoriels lorsque nous étendons le corps $\mathbb{K}$ en un corps $\mathbb{L}$.

Soit donc un corps $\mathbb{K}$ et deux $\mathbb{K}$ -espaces vectoriels E et F , et entrons dans le vif du sujet⁵⁸. Soit $\mathbb{K}$ un corps (commutatif) et une extension $\mathbb{L}$ de $\mathbb{K}$. Soient E et F , des $\mathbb{K}$ -espaces vectoriels de dimension finie.

9.10.1 Extension des applications linéaires

Définition 9.167 ([207]).

L'espace vectoriel obtenu par *extension du corps de base* de E est l'espace vectoriel

$$E_{\mathbb{L}} = \mathbb{L} \otimes_{\mathbb{K}} E. \quad (9.343)$$

Ce dernier est le quotient $\mathbb{L} \otimes_{\mathbb{K}} E = (\mathbb{L} \times E) / \sim$ par la relation d'équivalence

$$(\lambda, v) \sim (a\lambda, \frac{1}{a}v) \quad (9.344)$$

pour tout $a \in \mathbb{K}$. Nous noterons $[\lambda, v]$ ou $\lambda \otimes v$ ou encore $\lambda \otimes_{\mathbb{K}} v$ la classe de (λ, v) .

Un élément de $E_{\mathbb{L}}$ est de la forme $\sum_k [\lambda_k, v_k]$ avec $\lambda_k \in \mathbb{L}$ et $v_k \in E$. Si $f: E \rightarrow F$ est une applications linéaire nous définissons

$$\begin{aligned} f_{\mathbb{L}}: E_{\mathbb{L}} &\rightarrow F_{\mathbb{L}} \\ [\lambda, v] &\mapsto [\lambda, f(v)]. \end{aligned} \quad (9.345)$$

Remarque 9.168.

Si deux vecteurs de $E_{\mathbb{L}}$ sont linéairement indépendants pour $\mathbb{K}$, ils ne le sont pas spécialement pour $\mathbb{L}$. Par exemple si $\mathbb{C}$ est vu comme $\mathbb{R}$ -espace vectoriel, alors $\{1, i\}$ est une partie libre. Mais dans $\mathbb{C}$ vu comme $\mathbb{C}$ -espace vectoriel, la partie $\{1, i\}$ n'est pas libre.

Nous définissons aussi l'injection canonique

$$\begin{aligned} \iota: E &\rightarrow E_{\mathbb{L}} \\ v &\mapsto [1, v]. \end{aligned} \quad (9.346)$$

Proposition 9.169 ([101]).

Injectivité et surjectivité respectées.

- (1) L'application $f_{\mathbb{L}}$ est injective si et seulement si f est injective.

⁵⁷. Définition 4.41.

⁵⁸. Le sujet étant le corps étendu.

(2) L'application $f_{\mathbb{L}}$ est surjective si et seulement si f est surjective.

Démonstration. Supposons pour commencer que $f_{\mathbb{L}}$ est injective. Le diagramme

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ \tau \downarrow & & \downarrow \tau \\ E_{\mathbb{L}} & \xrightarrow{f_{\mathbb{L}}} & F_{\mathbb{L}} \end{array} \quad (9.347)$$

est un diagramme commutatif. En effet

$$(\tau \circ f)(v) = [1, f(v)] \quad (9.348)$$

tandis que

$$(f_{\mathbb{L} \circ \tau})(v) = f_{\mathbb{L}}[1, v] = [1, f(v)]. \quad (9.349)$$

Donc si $f(v) = 0$ avec $v \neq 0$ nous aurions $(\tau \circ f)(v) = 0$ et donc aussi $(f_{\mathbb{L}} \circ \tau)(v) = 0$, alors que $\tau(v) \neq 0$ dans $E_{\mathbb{L}}$.

Réciproquement, nous supposons que f est injective et nous prouvons que $f_{\mathbb{L}}$ est injective. Par le lemme 4.51(1), nous savons qu'il existe $g: F \rightarrow E$ telle que $f \circ g = \text{Id}|_F$. Nous en déduisons que $f_{\mathbb{L}} \circ g_{\mathbb{L}} = \text{Id}|_{F_{\mathbb{L}}}$ parce que si $[\lambda, v] \in F_{\mathbb{L}}$ alors

$$(f_{\mathbb{L}} \circ g_{\mathbb{L}})[\lambda, v] = f_{\mathbb{L}}[\lambda, g(v)] = [\lambda, (f \circ g)(v)] = [\lambda, v]. \quad (9.350)$$

Notons que g est injective, donc $g_{\mathbb{L}}$ est injective et l'égalité $f_{\mathbb{L}} \circ g_{\mathbb{L}} = \text{Id}|_{F_{\mathbb{L}}}$ implique que $f_{\mathbb{L}}$ est également injective. $\square$

Proposition 9.170 ([1, 208]).

Soit $\{e_i\}_{i=1, \dots, p}$ une base de E . Alors $\{1 \otimes e_i\}_i$ est une base de $E_{\mathbb{L}} = \mathbb{L} \otimes_{\mathbb{K}} E$.

Démonstration. L'espace vectoriel E peut être écrit comme somme directe $E = \bigoplus_i \mathbb{K}e_i$. Si $\lambda \in \mathbb{L}$ et $k \in \mathbb{K}$ nous avons

$$\lambda \otimes ke_i = \frac{\lambda}{k} \otimes e_i = \frac{\lambda}{k} (1 \otimes e_i). \quad (9.351)$$

Cela pour introduire que l'application

$$\begin{aligned} \psi: \mathbb{L} \otimes_{\mathbb{K}} E &\rightarrow \bigoplus_i \mathbb{L}(1 \otimes e_i) \\ \sum_k \lambda_k \otimes v_k &\mapsto \bigoplus_i \sum_k (\lambda_k v_{ik})(1 \otimes e_i) \end{aligned} \quad (9.352)$$

où $v_k = \sum_i v_{ik} e_i$ avec $v_{ik} \in \mathbb{K}$ est un isomorphisme de $\mathbb{L}$ -espaces vectoriels. La surjectivité est facile. En ce qui concerne l'injectivité, si

$$\sum_i \sum_k (\lambda_k v_{ik})(1 \otimes e_i) = 0 \quad (9.353)$$

alors les choses suivantes sont nulles également :

$$\sum_i \sum_k (\lambda_k v_{ik})(1 \otimes e_i) = \sum_{ik} (\lambda_k \otimes v_{ik} e_i) = \sum_k (\lambda_k \otimes \sum_i v_{ik} e_i) = \sum_k (\lambda_k \otimes v_k). \quad (9.354)$$

Le dernier est l'argument de ψ . Le fait que ce soit nul implique que ψ est injective. $\square$

Remarque 9.171.

Nous n'avons pas dû prouver que chacun des $\lambda_k \otimes v_k$ était nul. Et encore heureux, parce que cela pouvait très bien être faux, vu qu'il y a plusieurs façons de noter un élément de $E_{\mathbb{L}}$ sous la forme de tels termes.

Corolaire 9.172.

La $\mathbb{L}$ -dimension de $E_{\mathbb{L}}$ est égale à la $\mathbb{K}$ -dimension de E .

9.10.2 Projections

⚠ Avertissement/question à la lectrice !! 9.173

Nous allons définir $\mathbf{proj}: \mathcal{L}(E_{\mathbb{L}}, F_{\mathbb{L}}) \rightarrow \mathcal{L}(E, F)$ en faisant appel à des bases et en prouvant que les choses définies ne dépendent pas des bases choisies. Il y a sûrement une façon plus « intrinsèque » de faire.

Nous savons que $\mathbb{L}$ est un $\mathbb{K}$ -espace vectoriel dans lequel nous pouvons voir $\mathbb{K}$ comme un sous-espace (lemme 6.55). Dans cette optique nous choisissons dans $\mathbb{L}$ un supplémentaire de $\mathbb{K}$, c'est-à-dire un sous-espace vectoriel de $\mathbb{L}$ tel que

$$\mathbb{L} = \mathbb{K} \oplus V. \quad (9.355)$$

Nous avons alors naturellement une projection $\mathbf{proj}: \mathbb{L} \rightarrow \mathbb{K}$.

Soit $\{e_i\}$ une base de E et $\{e_a\}$ une de F . Nous noterons également e_i et e_a les éléments τe_i et τe_a correspondants. Grâce à la proposition 9.170, ce sont des bases de $E_{\mathbb{L}}$ et $F_{\mathbb{L}}$. Si la fonction $f: E_{\mathbb{L}} \rightarrow F_{\mathbb{L}}$ s'écrit dans ces bases comme

$$f(e_i) = \sum_a f_{ai} e_a \quad (9.356)$$

alors nous définissons $\mathbf{proj}(f)$ par

$$(\mathbf{proj} f)e_i = \sum_a \mathbf{proj}(f_{ai})e_a. \quad (9.357)$$

Proposition 9.174 ([1]).

L'application $\mathbf{proj}$ définie en (9.357) est indépendante du choix des bases.

Démonstration. Notons que dans ce qui suit, les sommes sur a ou b et celles sur i ou j ne vont pas jusqu'au même indice (dimensions de E et F). De plus nous manipulons deux choses qui se notent $\mathbf{proj}$. La première est la projection $\mathbf{proj}: \mathbb{L} \rightarrow \mathbb{K}$ qui ne dépend que d'un choix de supplémentaire et que nous supposons fixée ici. D'autre part il y a $\mathbf{proj}: E_{\mathbb{L}} \rightarrow E$ qui dépend à priori des bases choisies.

Nous choisissons de nouvelles bases qui sont liées aux anciennes bases par

$$\left\{ \begin{array}{l} e'_b = \sum_a B_{ab} e_a \\ e'_i = \sum_j A_{ji} e_j. \end{array} \right. \quad (9.358a)$$

$$\left\{ \begin{array}{l} e'_b = \sum_a B_{ab} e_a \\ e'_i = \sum_j A_{ji} e_j. \end{array} \right. \quad (9.358b)$$

Les matrices A et B sont dans $\mathrm{GL}(\mathbb{K})$. Nous allons écrire l'opérateur $\mathbf{proj}'$ qui correspond à ces bases et montrer que pour toute application linéaire $f: E_{\mathbb{L}} \rightarrow F_{\mathbb{L}}$ nous avons $\mathbf{proj}(f) = \mathbf{proj}'(f)$. Nous avons :

$$f(e'_j) = \sum_i A_{ji} f(e_i) \quad (9.359a)$$

$$= \sum_a \sum_b \sum_i A_{ji} f_{ai} (B^{-1})_{ba} e'_b \quad (9.359b)$$

$$= \sum_b \left(\sum_{ai} A_{ji} f_{ai} (B^{-1})_{ba} \right) e'_b, \quad (9.359c)$$

ce qui fait que

$$(\mathbf{proj}' f)e'_j = \sum_b \left(\mathbf{proj} (A_{ji} f_{ai} (B^{-1})_{ba}) \right) e'_b. \quad (9.360)$$

Nous calculons maintenant $(\text{proj}' f)e_j$ en substituant $e_j = \sum_l (A^{-1})_{lj} e'_l$ et en utilisant (9.360) et la linéarité de proj' et la $\mathbb{K}$ -linéarité de $\text{proj}: \mathbb{L} \rightarrow \mathbb{K}$:

$$(\text{proj}' f) \left(\sum_l (A^{-1})_{lj} e'_l \right) = \sum_l (A^{-1})_{lj} \sum_b \sum_{ai} \text{proj} (A_{li} f_{ai} (B^{-1})_{ba}) e_b \quad (9.361a)$$

$$= \sum_a \text{proj} (f_{aj}) e_a \quad (9.361b)$$

$$= (\text{proj} f) e_j. \quad (9.361c)$$

Donc $\text{proj} = \text{proj}'$. □

Note au passage comme toujours : il y a un abus systématique de notation entre $e_i \in E$ et $\tau(e_i) = 1 \otimes e_i \in E_{\mathbb{L}}$.

Remarque 9.175 ([1]).

L'opération $\text{proj}: \mathcal{L}(E_{\mathbb{L}}, F_{\mathbb{L}}) \rightarrow \mathcal{L}(E, F)$ ne dépend pas des bases choisies un peu partout. Mais elle dépend de l'application $pr: \mathbb{L} \rightarrow \mathbb{K}$ déjà construite. Et celle-là dépend du choix d'un supplémentaire V qui fournit $\mathbb{L} = \mathbb{K} \oplus V$.

Si $\text{proj}(\lambda) = 0$ pour un de ces choix, cela n'implique nullement que $\lambda = 0$. Penser à $i \in \mathbb{C}$ si la projection $\text{proj}: \mathbb{C} \rightarrow \mathbb{R}$ est l'application $(x + iy) \mapsto x$ parallèle à l'axe des imaginaires.

Par contre si $\text{proj}(\lambda) = 0$ pour tout choix de V , alors nous avons bien $\lambda = 0$. Dans la suite nous « fixons » un choix de V générique, et lorsque nous rencontrerons l'égalité $\text{proj}(\lambda) = 0$ nous en déduirons $\lambda = 0$.

Proposition 9.176.

Si $f: E \rightarrow F$ et si $f_{\mathbb{L}} e_j = \sum_a (f_{\mathbb{L}})_{aj} e_a$ et si $f(e_j) = \sum_a f_{aj} e_a$ alors

$$(1) \text{proj} f_{\mathbb{L}} = f,$$

$$(2) (f_{\mathbb{L}})_{ja} = f_{ja} \in \mathbb{K}.$$

Démonstration. Nous avons

$$f_{\mathbb{L}}(e_i) = \sum_a f_{ai} (1 \otimes e_a) = \sum_a f_{ai} \tau(e_a), \quad (9.362)$$

donc

$$(\text{proj} f_{\mathbb{L}}) e_i = \sum_a \text{proj} (f_{ai}) e_a = \sum_a f_{ai} e_a = f(e_i). \quad (9.363)$$

Cela prouve que $\text{proj} f_{\mathbb{L}} = f$.

Par ailleurs,

$$f_{\mathbb{L}}(\tau e_i) = f_{\mathbb{L}}(1 \otimes e_i) = 1 \otimes f(e_i) = \tau(f(e_i)) = \sum_a f_{ai} \tau(e_a) \quad (9.364)$$

alors que par définition,

$$f_{\mathbb{L}}(\tau e_i) = \sum_a (f_{\mathbb{L}})_{ai} \tau(e_a). \quad (9.365)$$

Les éléments $\tau(e_a)$ formant une base⁵⁹, la comparaison de (9.364) avec (9.365) donne $(f_{\mathbb{L}})_{ai} = f_{ai} \in \mathbb{K}$. □

Lemme 9.177.

Soient

- (1) Une base $\{e_i\}$ de E et une application linéaire $f: E \rightarrow F$;
- (2) une base $\{e_a\}$ de F et une application linéaire $g: G \rightarrow F$;
- (3) une base $\{e_{\alpha}\}$ de G et une application linéaire $\tilde{h}: G_{\mathbb{L}} \rightarrow E_{\mathbb{L}}$.

59. Encore la proposition 9.170.

Alors nous avons

$$\text{proj}(f_{\mathbb{L}} \circ \tilde{h}) = \text{proj}(f_{\mathbb{L}}) \circ \text{proj}(\tilde{h}). \quad (9.366)$$

Démonstration. Pour écrire $\text{proj}(f_{\mathbb{L}} \circ \tilde{h})$ à partir de la définition (9.357) nous commençons par écrire

$$(f_{\mathbb{L}} \circ \tilde{h})e_{\alpha} = \sum_a (f_{\mathbb{L}} \circ \tilde{h})_{a\alpha} e_a = \sum_{ai} (f_{\mathbb{L}})_{ai} (\tilde{h})_{i\alpha} e_a = \sum_a \left(\sum_i f_{ai} (\tilde{h})_{i\alpha} \right) e_a \quad (9.367)$$

où nous avons utilisé le fait que $(f_{\mathbb{L}})_{ai} = f_{ai}$. Donc, en utilisant la $\mathbb{K}$ -linéarité de proj ,

$$\text{proj}(f_{\mathbb{L}} \circ \tilde{h})e_{\alpha} = \sum_a \sum_i \text{proj} \left(f_{ai} (\tilde{h})_{i\alpha} \right) e_a = \sum_a \sum_i f_{ai} \text{proj} \left((\tilde{h})_{i\alpha} \right) e_a. \quad (9.368)$$

D'autre part,

$$\begin{aligned} \text{proj}(f_{\mathbb{L}}) \circ \text{proj}(\tilde{h})e_{\alpha} &= \text{proj}(f_{\mathbb{L}}) \sum_i \text{proj} \left((\tilde{h})_{i\alpha} \right) e_i \\ &= \sum_i \text{proj} \left((\tilde{h})_{i\alpha} \right) \sum_a f_{ai} e_a \\ &= \sum_{ai} \text{proj} \left((\tilde{h})_{i\alpha} \right) f_{ai} e_a, \end{aligned} \quad (9.369)$$

et c'est égal à (9.368). $\square$

Remarque 9.178.

Nous n'avons en général pas $\text{proj}(xy) = \text{proj}(x) \text{proj}(y)$ pour tout $x, y \in \mathbb{L}$. Par exemple si $\mathbb{K} = \mathbb{R}$ et $\mathbb{L} = \mathbb{C}$ avec la projection canonique,

$$\text{proj}(i \cdot i) = \text{proj}(-1) = -1 \quad (9.370)$$

alors que $\text{proj}(i) = 0$.

Proposition 9.179.

Soient $f \in \mathcal{L}(E, F)$ et $g \in \mathcal{L}(F, E)$. Alors il existe $h: G \rightarrow E$ tel que $f \circ h = g$ si et seulement s'il existe $\tilde{g}: G_{\mathbb{L}} \rightarrow E_{\mathbb{L}}$ tel que $f_{\mathbb{L}} \circ \tilde{g} = g_{\mathbb{L}}$.

Démonstration. Dans le sens direct, il suffit de poser $\tilde{h} = h_{\mathbb{L}}$.

Dans le sens inverse, si nous avons $\tilde{h}: G_{\mathbb{L}} \rightarrow E_{\mathbb{L}}$ tel que $f_{\mathbb{L}} \circ \tilde{h} = g_{\mathbb{L}}$ alors en appliquant proj des deux côtés et en utilisant le lemme 9.177,

$$\text{proj}(f_{\mathbb{L}}) \circ \text{proj}(\tilde{h}) = \text{proj}(g_{\mathbb{L}}) \quad (9.371)$$

c'est-à-dire

$$f \circ \text{proj}(\tilde{h}) = g, \quad (9.372)$$

c'est-à-dire que l'application $\text{proj} \tilde{h}: G \rightarrow E$ est la réponse à la proposition. $\square$

9.10.3 Rang, polynôme minimal, polynôme caractéristique

Proposition 9.180 (Stabilité du rang par extension des scalaires[101]).

Si $f: E \rightarrow F$ est linéaire alors nous avons

$$\text{rang}(f) = \text{rang}(f_{\mathbb{L}}). \quad (9.373)$$

où à droite nous considérons le rang de l'application $\mathbb{L}$ -linéaire $f_{\mathbb{L}}: E_{\mathbb{L}} \rightarrow F_{\mathbb{L}}$.

Démonstration. Il existe un supplémentaire V tel que $E = \ker(f) \oplus V$ avec $\dim(V) = \text{rang}(f)$. Nous pouvons factoriser f en

$$f = f_2 \circ f_1 \quad (9.374)$$

avec $f_1: E \rightarrow V$ est la projection parallèle à $\ker(f)$ et est surjective (vers V) parce que $\dim(V) = \text{rang}(f) = \dim(\text{Image}(f))$. De plus $f_2: V \rightarrow F$ est injective parce que si $v \in V$ est tel que $f_2(v) = 0$ alors on aurait

$$f(v) = (f_2 \circ f_1)(v) = f_2(v) = 0. \quad (9.375)$$

Cela donne $v \in \ker(f) \cap V = \{0\}$. Par la proposition 9.169, les applications $(f_1)_{\mathbb{L}}$ et $(f_2)_{\mathbb{L}}$ sont respectivement surjective et injective.

L'application $(f_2)_{\mathbb{L}}: V_{\mathbb{L}} \rightarrow F_{\mathbb{L}}$ est forcément surjective sur son image, donc

$$(f_2)_{\mathbb{L}}: V_{\mathbb{L}} \rightarrow \text{Image}(f_{\mathbb{L}}) \quad (9.376)$$

est un isomorphisme de $\mathbb{L}$ -espaces vectoriels. Nous avons alors les égalités

$$\dim_{\mathbb{L}}(V_{\mathbb{L}}) = \dim_{\mathbb{L}}(\text{Image}(f_{\mathbb{L}})) = \text{rang}(f_{\mathbb{L}}). \quad (9.377)$$

Mais aussi, par les définitions posées plus haut,

$$\dim(V) = \text{rang}(f) = \dim(\text{Image}(f)). \quad (9.378)$$

Mais le corolaire 9.172 nous dit que $\dim_{\mathbb{L}}(V_{\mathbb{L}}) = \dim_{\mathbb{K}}(V)$. Donc il y a égalité des deux lignes (9.377) et (9.378) donne $\text{rang}(f) = \text{rang}(f_{\mathbb{L}})$. $\square$

Proposition 9.181.

Nous avons

$$(1) \det(f) = \det(f_{\mathbb{L}})$$

$$(2) \chi_f = \chi_{f_{\mathbb{L}}}.$$

Démonstration. Dès que l'on a des bases nous avons $(f_{\mathbb{L}})_{ai} = f_{ai}$ par la proposition 9.176(2). Le nombre $\det(f) \in \mathbb{K}$ est un polynôme en les f_{ai} . Entendons nous : il existe un polynôme indépendant de f et de $\mathbb{K}$ et de $\mathbb{L}$ donnant le déterminant de n'importe quelle matrice. Donc $\det(f) = \det(f_{\mathbb{L}})$.

Même chose pour le polynôme caractéristique (définition 9.108) : les coefficients de ce polynôme sont des polynômes en les f_{ai} qui sont indépendants de $\mathbb{L}$, de $\mathbb{K}$ et de f .

Notons que $\chi_{f_{\mathbb{L}}}$ est un polynôme à coefficients dans $\mathbb{K}$. $\square$

La situation est très différente avec le polynôme minimal⁶⁰. Autant il existe une « recette » pour créer le polynôme caractéristique, il n'en n'existe pas pour le polynôme minimal (ou en tout cas, il ne suffit pas d'appliquer des polynômes en les coefficients de la matrice). La proposition suivante montre que le polynôme minimal est conservé par extension de corps, mais que pour le voir, il faut travailler plus.

Proposition 9.182 ([101, 1]).

Soit $\mathbb{L}$ une extension du corps $\mathbb{K}$ et une application linéaire $f: E \rightarrow F$ entre deux $\mathbb{K}$ -espaces vectoriels. Alors $\mu_f = \mu_{f_{\mathbb{L}}}$.

Démonstration. Nous allons montrer que l'application

$$\begin{aligned} \tilde{g}: \frac{\mathbb{L}[X]}{(\mu)} &\rightarrow \text{End}(E_{\mathbb{L}}) \\ \bar{P} &\mapsto P(f_{\mathbb{L}}) \end{aligned} \quad (9.379)$$

est bien définie et injective. La proposition 9.98 nous dira alors que μ est le polynôme minimal de $f_{\mathbb{L}}$.

60. Définition 6.59.

Pour prouver que l'application $\tilde{g}$ est bien définie, nous commençons par prouver que $P(f_{\mathbb{L}}) = P(f)_{\mathbb{L}}$:

$$P(f_{\mathbb{L}})\lambda \otimes v = \sum_k a_k f_{\mathbb{L}}^k \lambda \otimes v \quad (9.380a)$$

$$= \lambda \otimes \sum_k a_k f^k(v) \quad (9.380b)$$

$$= \lambda \otimes P(f)v \quad (9.380c)$$

$$= P(f)_{\mathbb{L}}\lambda \otimes v. \quad (9.380d)$$

Par conséquent $\mu(f_{\mathbb{L}}) = 0$ et l'application est bien définie.

Sur $\mathbb{L}[X]/(\mu)$ nous considérons la base $\{1, \bar{X}, \dots, \bar{X}^{\deg(\mu)-1}\}$, et $\text{End}(E_{\mathbb{L}})$ nous considérons une base qui commence⁶¹ par $\{f_{\mathbb{L}}^k\}_{k=0, \dots, \deg(\mu)-1}$. Montrons tout de même que cette partie est libre (sinon le théorème de la base incomplète ne s'applique pas) : si $\sum_k \lambda_k f_{\mathbb{L}}^k = 0$ alors

$$\sum_k \text{proj}(\lambda_k f_{\mathbb{L}}^k) = 0. \quad (9.381)$$

Pour détailler ce que cela implique, nous calculons ceci :

$$(\lambda f_{\mathbb{L}})(\tau e_i) = \lambda f_{\mathbb{L}}(\tau e_i) = \sum_a \lambda f_{ia} e_a, \quad (9.382)$$

par conséquent $\text{proj}(\lambda f_{\mathbb{L}})e_i = \sum_a \text{proj}(\lambda f_{ia})e_a$, et comme proj est $\mathbb{K}$ -linéaire et que $f_{ai} \in \mathbb{K}$,

$$\text{proj}(\lambda f_{\mathbb{L}})e_i = \text{proj}(\lambda) \sum_a f_{ai} e_a = \text{proj}(\lambda) \text{proj}(f_{\mathbb{L}})e_i = \text{proj}(\lambda) f(e_i). \quad (9.383)$$

Appliquer la projection proj à l'équation (9.381) donne alors $\sum_k \text{proj}(\lambda_k) f^k = 0$. Mais comme les f^k sont linéairement indépendantes sur $\mathbb{K}$ nous avons pour tout k : $\text{proj}(\lambda_k) = 0$ (égalité dans $\mathbb{K}$). En nous souvenant de la remarque 9.175 nous en déduisons $\lambda_k = 0$ dans $\mathbb{L}$.

Dans les choix de bases faits, l'application $\tilde{g}$ a la forme

$$\tilde{g} = \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ * & * & * & & \\ * & * & * & & \\ * & * & * & & \end{pmatrix}, \quad (9.384)$$

qui est injective.

Vu que $\tilde{g}$ est injective, μ est le polynôme minimal de $f_{\mathbb{L}}$ et donc $\mu = \mu_{\mathbb{L}}$. □

9.11 Frobenius et Jordan

9.11.1 Matrice compagnon

Définition 9.183.

Soit le polynôme $P = X^n - a_{n-1}X^{n-1} - \dots - a_1X - a_0$ dans $\mathbb{K}[X]$. La **matrice compagnon** de P est la matrice donnée par

$$C(P) = \begin{pmatrix} 0 & \cdots & \cdots & 0 & a_0 \\ 1 & 0 & & \vdots & a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & a_{n-2} \\ 0 & \cdots & 0 & 1 & a_{n-1} \end{pmatrix} \quad (9.385)$$

61. Théorème de la base incomplète 4.11(2).

si $n \geq 2$ et par (a_0) si $n = 1$.

Une matrice est dite *compagnon* si elle a cette forme.

Proposition 9.184.

Si f est l'endomorphisme associé à la matrice $C(P)$ nous avons

$$f(e_i) = \begin{cases} e_{i+1} & \text{si } i < n \\ (a_0, \dots, a_{n-1}) & \text{si } i = n. \end{cases} \quad (9.386)$$

De plus l'endomorphisme f vérifie $P(f)e_1 = 0$.

Lemme 9.185 ([209]).

Un polynôme sur un corps commutatif est le polynôme caractéristique de sa matrice compagnon. En d'autres termes nous avons $\chi_{C(P)} = P$.

Démonstration. Nous notons f l'endomorphisme associé à $C(P)$. La propriété $P(f)e_1 = 0$ nous indique que le polynôme minimal ponctuel de f en e_1 divise P . L'ensemble des puissances de f appliquées à e_1 , $(f^i(e_1))_{i=1, \dots, n-1}$ est libre, donc le polynôme minimal ponctuel en e_1 est de degré n au minimum. En reprenant les notations du théorème 6.39, nous avons $I_{e_1} = (P)$ parce que P est de degré minimum dans I_{e_1} et $\chi_f \in I_{e_1}$.

Donc P divise χ_f et est de degré égal à celui de χ_f . Étant donné qu'ils sont tous deux unitaires, ils sont égaux. $\square$

Remarque 9.186.

Les matrices compagnons ne sont pas les seules dont le polynôme caractéristique est égal au polynôme minimal. En fait les matrices dont le polynôme caractéristique est égale au polynôme minimal sont denses dans les matrices. En effet une matrice dont le polynôme minimal n'est pas égal au polynôme caractéristique a un polynôme caractéristique avec une racine double. Il est possible, en modifiant arbitrairement peu la matrice de séparer la racine double en deux racines distinctes.

9.11.2 Réduction de Frobenius

Lemme 9.187.

Soit un endomorphisme $f: E \rightarrow E$ sur l'espace vectoriel de dimension finie n . Nous notons μ et χ les polynômes minimal et caractéristique. Si f est cyclique, alors $\mu = \chi$.

Le théorème 9.200 donnera une version plus complète de ce lemme.

Démonstration. Soit v un vecteur cyclique de f , c'est-à-dire que $\{f^k(v)\}_{k=0, \dots, n-1}$ est libre. Donc si P est un polynôme de degré jusqu'à $n - 1$ nous ne pouvons pas avoir $P(f) = 0$ parce que, appliqué à v , ce serait une combinaison nulle non triviale des $f^k(v)$. Donc le polynôme minimal est au minimum de degré n . Mais le polynôme caractéristique est annulateur de degré n (Cayley-Hamilton 9.116), donc il est le polynôme minimal. $\square$

Théorème 9.188 (Réduction de Frobenius [210, 211, 212]).

Soit E , un $\mathbb{K}$ -espace vectoriel, et $f \in \text{End}(E)$. Alors il existe une suite de sous-espaces $E_1, \dots, E_r$ stables par f tels que

- (1) $E = \bigoplus_{i=1}^r E_i$;
- (2) pour chaque E_i , l'endomorphisme restreint $f_i = f|_{E_i}$ est cyclique ;
- (3) si μ_i est le polynôme minimal de f_i alors μ_{i+1} divise μ_i ;

Une telle décomposition vérifie automatiquement $\mu_1 = \mu_f$ et $\mu_1 \cdots \mu_r = \chi_f$, et la suite $(\mu_i)_{i=1, \dots, r}$ ne dépend que de f et non du choix de la décomposition du point (1).

Les polynômes μ_i sont les **invariants de similitude** de l'endomorphisme f .

Démonstration. Nous commençons par montrer que si une telle décomposition existe, alors

$$\chi_f = \prod_{i=1}^r \mu_i \quad (9.387a)$$

$$\mu_f = \mu_1 \quad (9.387b)$$

où χ_f est le polynôme caractéristique de f et μ_f est le polynôme minimal. D'abord le polynôme caractéristique de f devra être égal au produit des polynômes caractéristique des $f|_{E_i}$, mais ces derniers endomorphismes étant cycliques⁶², leurs polynôme caractéristique sont égaux à leurs polynômes minimaux (lemme 9.187). Cela prouve l'égalité (9.387a). Ensuite tous les μ_i doivent diviser le polynôme minimal, donc $\text{ppcm}(\mu_1, \dots, \mu_r)$ divise μ_f . Cependant le polynôme minimal doit contenir une et une seule fois chacun des facteurs irréductibles du polynôme caractéristique, et chacun de ces facteurs sont dans les polynômes μ_i . Par conséquent $\text{ppcm}(\mu_1, \dots, \mu_r) = \mu_f$. Mais par ailleurs $\mu_1 = \text{ppcm}(\mu_1, \dots, \mu_r)$ parce qu'on a supposé $\mu_{i+1} \mid \mu_i$, donc $\mu_1 = \mu_f$.

Soit d , le degré du polynôme minimal de f et $y \in E$ tel que $\mu_f = \mu_{f,y}$ (voir lemme 9.99). Le plus petit espace stable sous f contenant y est

$$E_y = \text{Span}\{y, f(y), \dots, f^{d-1}(y)\}. \quad (9.388)$$

Nous notons $e_i = f^{i-1}(y)$. Notons que les vecteurs donnés forment bien une base de E_y parce que si les e_i n'étaient pas linéairement indépendants, alors nous aurions des a_k tels que $\sum_k a_k e_k = 0$ et avec lesquels

$$\left(\sum_k a_k X^k\right)(f)y = 0, \quad (9.389)$$

ce qui contredirait la minimalité de $\mu_{f,y}$.

La difficulté du théorème est de trouver un complément de E_y qui soit également stable sous f . Nous commençons par étendre⁶³ $\{e_1, \dots, e_d\}$ en une base $\{e_1, \dots, e_n\}$ de E . Ensuite nous allons montrer que

$$E = E_y \oplus F \quad (9.390)$$

avec

$$F = \{x \in E \text{ tel que } e_d^*(f^k(x)) = 0 \forall k \in \mathbb{N}\}. \quad (9.391)$$

Par construction, F est invariant sous f . Montrons pour commencer que $E_y \cap F = \{0\}$. Un élément de E_y s'écrit

$$z = a_1 e_1 + \dots + a_k e_k \quad (9.392)$$

avec $k \leq d$. Étant donné que f décale les vecteurs de base, nous avons $e_d^*(f^{d-k}(z)) = a_k$. Du coup $z \in F$ si et seulement si $a_1 = \dots = a_d = 0$, c'est-à-dire que $E_y \cap F = \{0\}$.

Nous montrons maintenant que $\dim F = n - d$. Pour cela nous considérons l'application

$$\begin{aligned} T: \mathbb{K}[F] &\rightarrow E^* \\ g &\mapsto e_d^* \circ g. \end{aligned} \quad (9.393)$$

Cette application est injective. En effet un élément général de $\mathbb{K}[f]$ est

$$g = a_1 \text{Id} + a_2 f + \dots + a_p f^{p-1} \quad (9.394)$$

avec $p \leq d$. Si $T(g) = 0$, alors nous avons en particulier

$$0 = T(g)e_{d-p+1} = e_d^*(a_1 e_{d-p+1} + a_2 e_{d-p+2} + \dots + a_p e_d) = a_p. \quad (9.395)$$

Donc $a_p = 0$ et en appliquant maintenant $T(g)$ à e_{d-p} nous obtenons $a_{p-1} = 0$. Au final nous trouvons que $g = 0$ et donc que T est injective.

62. Définition 9.100.

63. Pour autant que j'aie compris, cette extension manque dans [210]. Corrigez-moi si je me trompe.

Étant donné que $\dim \mathbb{K}[f] = d$ et que T est injective, $\dim \text{Image}(T) = d$. Nous regardons l'orthogonal de l'image :

$$(\text{Image}(T))^\perp = \{x \in E \text{ tel que } T(g)x = 0 \forall g \in \mathbb{K}[f]\} \quad (9.396a)$$

$$= \{x \in E \text{ tel que } e_d^*(g(x)) = 0 \forall g \in \mathbb{K}[f]\} \quad (9.396b)$$

$$= F. \quad (9.396c)$$

Par conséquent $F^\perp = \text{Image}(T)$. Vu que $\dim \text{Image}(T) = d$, nous avons donc $\dim F = n - d$ et il est établi que $E = E_y \oplus F$.

Nous avons donc trouvé F , stable par f et tel que $E = E_y \oplus F$. Nous devons maintenant nous assurer que cette décomposition tombe bien pour les polynômes minimaux. Si P_1 est le polynôme minimal de $f|_{E_y}$, alors par le lemme 9.101 nous avons $P_1 = \mu_{f,y} = \mu_f$ parce que $f|_{E_y}$ est cyclique sur E_y . Mettons P_2 , le polynôme minimal de $f|_F$. Étant attendu que F est stable par f , le polynôme P_2 divise P_1 . En recommençant la construction sur F , nous construisons un nouvel espace F' stable sous F et vérifiant $\mu_{f|_{F'}} = P_2$, etc.

Nous passons maintenant à la partie unicité du théorème. Soient deux suites $F_1, \dots, F_r$ et $G_1, \dots, G_s$ de sous-espaces stables par f et vérifiant

$$(1) \quad E = \bigoplus_{i=1}^r F_i,$$

$$(2) \quad f|_{F_i} \text{ est cyclique,}$$

$$(3) \quad \mu_{f|_{F_{i+1}}} \text{ divise } \mu_{f|_{F_i}},$$

et, *mutatis mutandis*, les mêmes conditions pour la famille $\{G_i\}$. Nous posons $P_i = \mu_{f|_{F_i}}$ et $Q_i = \mu_{f|_{G_i}}$. Nous allons montrer par récurrence que $P_i = Q_i$ et $\dim F_i = \dim G_i$. Il ne sera cependant pas garanti que $F_i = G_i$. D'abord, $P_1 = Q_1$ parce qu'ils sont tous deux égaux à μ_f par les relations (9.387). Nous supposons que $P_i = Q_i$ pour $i \leq j-1$ et nous tentons de montrer que $P_j = Q_j$.

Nous avons

$$P_j(f) = P_j(f)|_{F_1} \oplus \dots \oplus P_j(f)|_{F_{j-1}}. \quad (9.397)$$

En effet étant donné que P_{j+k} divise P_j , nous avons⁶⁴ $P_j(f) = A(f) \circ P_{j+k}(f)$, mais $P_{j+k}(f)F_{j+k} = 0$, donc $P_j(f)F_{j+k} = 0$. Les espaces G_i n'ayant à priori aucun rapport avec les polynômes P_i , nous écrivons

$$P_j(f) = P_j(f)|_{G_1} \oplus \dots \oplus P_j(f)|_{G_{j-1}} \oplus P_j(f)|_{G_j} \oplus \dots \oplus P_j(f)|_{G_s}. \quad (9.398)$$

Pour $1 \leq i \leq j-1$, nous avons supposé $P_i = Q_i$. Étant donné que $f|_{F_i}$ est semblable à C_i et $f|_{G_i}$ est semblable à C_{Q_i} , la matrice de $f|_{E_i}$ est semblable à la matrice de $f|_{G_i}$. En particulier,

$$\dim P_j(f)F_i = \dim P_j(f)G_i. \quad (9.399)$$

En prenant les dimensions des images dans les égalités (9.397) et (9.398), nous trouvons que

$$P_j(f)|_{G_j} = \dots = P_j(f)|_{G_s} = 0. \quad (9.400)$$

Par conséquent $P_j \in I_{f|_{G_j}}$ et donc P_j divise Q_j , qui est générateur de $I_{f|_{G_j}}$. La situation étant symétrique entre P et Q , nous montrons de même que Q_j divise P_j et donc que $P_j = Q_j$.

Ceci achève la démonstration du théorème de réduction de Frobenius.

□

Remarque 9.189.

Sous forme matricielle, ce théorème dit que toute matrice est semblable à une matrice de la forme bloc-diagonale

$$f = \begin{pmatrix} C_{\mu_1} & & \\ & \ddots & \\ & & C_{\mu_r} \end{pmatrix} \quad (9.401)$$

où les C_{μ_i} sont les matrices compagnon (définition 9.183).

En particulier, et ceci est très important, deux applications sont semblables si et seulement si elles ont même suite d'invariants de similitude.

64. En vertu du lemme 9.87.

Remarque 9.190.

Si nous travaillons sur $\mathbb{R}$, la réduite de Frobenius restera une matrice réelle, même si les valeurs propres sont complexes. En effet le procédé de Frobenius ne regarde absolument pas les valeurs propres, mais seulement les facteurs irréductibles du polynôme caractéristique. La réduite de Frobenius ne tente pas de résoudre ces polynômes, mais se contente d'en utiliser les matrices compagnon.

La situation sera différente dans le cas de la forme normale de Jordan.

9.11.3 Forme normale de Jordan

Il existe une preuve directe de la réduction de Jordan ne nécessitant pas la réduction de Frobenius[213]. Cette dernière passe par les espaces caractéristiques⁶⁵ et est à mon avis plus compliquée que la démonstration de Frobenius elle-même. Nous allons donc nous contenter de donner la réduction de Jordan comme un cas particulier de Frobenius.

Théorème 9.191 (Réduction de Jordan).

Soit E un espace vectoriel sur $\mathbb{K}$, et $f \in \text{End}(E)$ un endomorphisme dont le polynôme caractéristique χ_f est scindé⁶⁶. Il existe une base de E dans laquelle la matrice de f s'écrit sous la forme

$$M = \begin{pmatrix} J_{n_1}(\lambda_1) & & \\ & \ddots & \\ & & J_{n_k}(\lambda_k) \end{pmatrix} \quad (9.402)$$

où les λ_i sont les valeurs propres de f (avec éventuelle répétitions) et $J_n(\lambda)$ représente le bloc $n \times n$

$$J_n(\lambda) = \begin{pmatrix} \lambda & 1 & & \\ & \lambda & 1 & \\ & & \ddots & \ddots \\ & & & \lambda \end{pmatrix}. \quad (9.403)$$

En d'autres termes, $J_n(\lambda)_{ii} = \lambda$ et $J_n(\lambda)_{i-1,i} = 1$.

Démonstration. Nous commençons par le cas où f est nilpotente ; nous notons M sa matrice. Dans ce cas la seule valeur propre est zéro et le polynôme caractéristique est X^m pour un certain m . Nous savons par le lemme 9.185 que (la matrice de) f est semblable à sa matrice compagnon. En l'occurrence pour f nous avons

$$C_{X^m} = \begin{pmatrix} 0 & & & 0 \\ 1 & \ddots & & \vdots \\ & \ddots & \ddots & \vdots \\ & & 1 & 0 \end{pmatrix}. \quad (9.404)$$

Ensuite le changement de base (qui est une similitude) $(e_1, \dots, e_n) \mapsto (e_n, \dots, e_1)$ montre que C_{X^m} est semblable à un bloc de Jordan $J_m(0)$.

Supposons à présent que f ne soit pas nilpotente. Par l'hypothèse de polynôme caractéristique scindé, nous supposons que f a m valeurs propres distinctes et que son polynôme caractéristique est

$$\chi_f = (X - \lambda_1)^{l_1} \dots (X - \lambda_m)^{l_m}. \quad (9.405)$$

Le lemme des noyaux (théorème 9.88) nous enseigne que

$$E = \bigoplus_{i=1}^m \underbrace{\ker(f - \mu_i \mathbb{1})^{l_i}}_{F_i}. \quad (9.406)$$

65. Aussi appelés « espaces propres généralisés ».

66. C'est pour cette hypothèse que $\mathbb{K} = \mathbb{R}$ n'est pas le bon cadre.

La restriction de $f - \lambda_i \mathbb{1}$ à F_i est par construction un endomorphisme nilpotent, et donc peut s'écrire comme un bloc de Jordan avec des zéros sur la diagonale. En utilisant la décomposition

$$f|_{F_i} = (f - \lambda_i \mathbb{1})|_{F_i} + \lambda_i \mathbb{1}_{F_i}, \quad (9.407)$$

nous voyons que $f|_{F_i}$ s'écrit comme un bloc de Jordan avec λ_i sur la diagonale. $\square$

Remarque 9.192.

Nous pouvons calculer la forme normale de Jordan pour une matrice complexe ou réelle, mais dans les deux cas nous devons nous attendre à obtenir une matrice complexe parce que les valeurs propres d'une matrice réelle peuvent être complexes. Cependant nous demandons que le polynôme caractéristique de f soit scindé sur $\mathbb{K}$. En pratique, la décomposition de Jordan n'est garantie que sur les corps algébriquement clos, c'est-à-dire sur $\mathbb{C}$.

La suite des invariants de similitude sur laquelle repose Frobenius, elle, est disponible sur tout corps, y compris $\mathbb{R}$.

9.12 Commutant et endomorphismes cycliques

9.12.1 Endomorphisme cyclique

Lemme 9.193.

Si A est la matrice de l'endomorphisme f alors nous avons équivalence des propriétés suivantes :

- (1) La matrice A est cyclique.
- (2) L'endomorphisme f est cyclique.

Si f est un endomorphisme de l'espace vectoriel E et si $x \in E$, nous notons

$$E_{f,x} = \text{Span}\{f^k(x) \text{ tel que } k \in \mathbb{N}\}. \quad (9.408)$$

Définition 9.194.

Soit E un espace vectoriel de dimension finie sur un corps $\mathbb{K}$ et un endomorphisme $f: E \rightarrow E$. Le **commutant** de f est l'ensemble des endomorphismes de E qui commutent avec f :

$$\mathcal{C}(f) = \{g \in \mathcal{L}(E, E) \text{ tel que } g \circ f = f \circ g\}. \quad (9.409)$$

Il n'est pas très compliqué de vérifier que $\mathcal{C}(f)$ est un sous-espace vectoriel de $\mathcal{L}(E, E)$.

Notons l'inclusion évidente $\mathbb{K}[f] \subset \mathcal{C}(f)$. L'inclusion inverse va un peu nous occuper durant les prochaines pages.

9.12.2 Commutant : cas diagonalisable

Proposition 9.195 ([214]).

Si f est diagonalisable, alors

$$\dim(\mathcal{C}(f)) = \sum_{\lambda \in \text{Spec}(f)} \dim(E_\lambda)^2. \quad (9.410)$$

où les E_λ sont les espaces propres de f .

Démonstration. D'abord si $g \in \mathcal{C}(f)$ alors E_λ est stable par g . En effet si $v \in E_\lambda$ alors $f(g(v)) = g(f(v)) = g(\lambda v) = \lambda g(v)$, ce qui montre que $g(v)$ est un vecteur propre de f pour la valeur propre λ , et donc que $g(v) \in E_\lambda$.

Nous considérons ensuite l'application

$$\begin{aligned} \psi: \mathcal{C}(f) &\rightarrow \text{End}(E_1) \times \dots \times \text{End}(E_r) \\ g &\mapsto g|_{E_1} \times \dots \times g|_{E_r} \end{aligned} \quad (9.411)$$

qui est bien définie parce que g se restreint aux espaces propres de f . Nous allons noter $\psi(g)_\lambda$ la restriction de g à E_λ .

ψ est injective Supposons que $g, h \in \mathcal{C}(f)$ tels que $\psi(g) = \psi(h)$. Vu que f est diagonalisable nous pouvons décomposer $x \in E$ en ses composantes sur les espaces propres⁶⁷ :

$$x = \sum_{\lambda \in \text{Spec}(f)} x_\lambda \quad (9.412)$$

avec $x_\lambda \in E_\lambda$. Nous avons alors

$$g(x) = \sum_{\lambda} g(x_\lambda) = \sum_{\lambda} \psi(g)_\lambda(x_\lambda). \quad (9.413)$$

Vu que nous avons $\psi(g)_\lambda = \psi(h)_\lambda$, nous avons aussi

$$g(x) = \sum_{\lambda} \psi(g)_\lambda(x_\lambda) = \sum_{\lambda} \psi(h)_\lambda(x_\lambda) = \sum_{\lambda} h(x_\lambda) = h(x). \quad (9.414)$$

Cela prouve $g = h$ et donc que ψ est injective.

ψ est surjective Si nous avons pour chaque $\lambda \in \text{Spec}(f)$ un endomorphisme g_λ de E_λ alors en posant

$$g(x) = \sum_{\lambda \in \text{Spec}(f)} g_\lambda(x_\lambda) \quad (9.415)$$

alors nous avons bien

$$\psi(g) = (g_{\lambda_1}, \dots, g_{\lambda_r}). \quad (9.416)$$

Nous pouvons donc conclure en écrivant

$$\dim(\mathcal{C}(f)) = \sum_{\lambda \in \text{Spec}(f)} \dim(\text{End}(E_\lambda)) = \sum_{\lambda \in \text{Spec}(f)} \dim(E_\lambda)^2. \quad (9.417)$$

□

Remarque 9.196.

Nous avons alors immédiatement

$$\dim(\mathcal{C}(f)) \geq \dim(E) \quad (9.418)$$

lorsque f est diagonalisable.

En suivant la notation (9.189), un endomorphisme est cyclique lorsqu'il existe $x \in E$ tel que $E_x = E$.

Proposition 9.197 ([214]).

Si f est un endomorphisme diagonalisable d'un espace vectoriel E de dimension n . Nous avons équivalence entre les faits suivants.

- (1) Le polynôme minimal est égal au polynôme caractéristique : $\mu_f = \chi_f$
- (2) L'endomorphisme f est cyclique.
- (3) $\mathcal{C}(f) = \mathbb{K}[f]$.
- (4) $\dim(\mathcal{C}(f)) = n$
- (5) L'endomorphisme f possède n valeurs propres distinctes.
- (6) $\dim(\mathbb{K}[f]) = n$

Démonstration. Le point important de cette proposition sont les équivalences (1)-(3). Les autres sont des intermédiaires. En particulier, dans le cas diagonalisable, nous allons voir que le point (5) est essentiellement une reformulation de (1).

(4) implique (5) Par la formule (9.410), les espaces propres de f ont dimension 1. Par conséquent f possède n valeurs propres distinctes.

67. Théorème 9.129(5).

(5) implique (6) Le théorème 9.129 nous dit que le polynôme minimal est scindé à racines simples. Vu que f possède n valeurs propres distinctes, μ est de degré n . Par l'isomorphisme $\mathbb{K}[f] = \mathbb{K}[X]/(\mu)$ de la proposition 9.107 nous avons $\dim(\mathbb{K}[f]) = \deg(\mu) = n$ par la proposition 6.40.

(6) implique (1) Par l'isomorphisme $\mathbb{K}[f] = \mathbb{K}[X]/(\mu)$ de la proposition 9.107 et la proposition 6.40 nous avons $n = \dim(\mathbb{K}[f]) = \deg(\mu)$. Vu que χ est un polynôme annulateur (Caley-Hamilton 9.116), il est divisé par μ . Maintenant μ et χ sont des polynômes unitaires de degré n et μ divise χ . Ils sont donc égaux.

(1) implique (2) Le fait que f soit diagonalisable permet d'utiliser le théorème 9.129 pour dire que μ est scindé à racines simples. L'égalisation avec χ nous permet de dire que f possède n valeurs propres distinctes. Soient $\{e_1, \dots, e_n\}$ une base de diagonalisation, et prouvons que le vecteur $v = e_1 + \dots + e_n$ est cyclique. Nous avons

$$f^k(v) = \sum_{i=1}^n \lambda_i^k e_i. \quad (9.419)$$

Pour prouver que cette famille (avec $k = 0, \dots, n-1$) est libre⁶⁸ nous en prenons une combinaison linéaire nulle et nous prouvons que les coefficients sont tous nuls. Soit donc

$$0 = \sum_{l=0}^{n-1} a_l f^l(v) = \sum_{l=0}^{n-1} a_l \sum_{i=1}^n \lambda_i^l e_i = \sum_{i=1}^n \left(\sum_{l=0}^{n-1} a_l \lambda_i^l \right) e_i. \quad (9.420)$$

Vu que cela est nul, nous avons pour tout i :

$$\sum_{l=0}^{n-1} a_l \lambda_i^l = 0. \quad (9.421)$$

En posant la matrice $A_{ij} = \lambda_i^j$, cela revient à étudier le système $\sum_j A_{ij} a_j = 0$. Ce système n'a des solutions non nulles que si $\det(A) = 0$; sinon il possède une unique solution et elle est $a_j = 0$ pour tout j . Nous devons donc calculer le déterminant

$$\det \begin{pmatrix} 1 & \lambda_1 & \lambda_1^2 & \dots & \lambda_1^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \lambda_n & \lambda_n^2 & \dots & \lambda_n^{n-1} \end{pmatrix}. \quad (9.422)$$

Il s'agit du déterminant de Vandermonde déjà étudié par la proposition 9.11. Nous avons $\det(A) = \prod_{1 \leq i < j \leq n} (\lambda_j - \lambda_i)$. Cela est bien non nul du fait que toutes les valeurs propres soient distinctes.

(2) implique (3) Soit v un vecteur cyclique de f . Un endomorphisme g donne lieu à un polynôme par le fait suivant : il existe des uniques a_k ($k = 0, \dots, n-1$) tels que

$$g(v) = \sum_{k=0}^{n-1} a_k f^k(v). \quad (9.423)$$

Cela donne une application linéaire

$$\begin{aligned} \psi: \mathcal{C}(f) &\rightarrow \mathbb{K}[f] \\ g &\mapsto P \text{ tel que } P(f)v = g(v). \end{aligned} \quad (9.424)$$

C'est une application injective parce que si $\psi(g) = 0$ alors $g(v) = 0$ et pour tout k nous avons $g(f^k(v)) = f^k(g(v)) = 0$. L'endomorphisme g s'annulant sur une base, est nul.

⁶⁸. Ce sera alors une base parce que n vecteurs libres dans un espace de dimension n est toujours une base, proposition 4.16.

(3) implique (4) Si $n_1, \dots, n_r$ sont les dimensions des différents espaces propres de f , nous avons les inégalités

$$\dim(\mathbb{K}[f]) = \deg(\mu) \leq n = n_1 + \dots + n_r \leq n_1^2 + \dots + n_r^2 = \dim(\mathcal{C}(f)). \quad (9.425)$$

Par hypothèse d'égalité entre le premier et le dernier terme de cette suite d'inégalités, toutes les inégalités sont des égalités et en particulier $\dim(\mathcal{C}(f)) = n$.

Nous avons fini de prouver toutes les équivalences demandées. $\square$

Exemple 9.198.

Pour mieux comprendre pourquoi le fait d'avoir n valeurs propres distinctes est équivalent à être cyclique, notons que si deux valeurs propres sont identiques, alors un morceau de la matrice de f serait par exemple $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$, et dans ce cas n'importe quelle combinaison $ae_i + be_j$ reste proportionnelle à elle-même après application de f . Si nous avons des valeurs propres différentes par contre, nous avons par exemples dans $\mathbb{R}^2$ la matrice $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ qui donne $f(e_1 + e_2) = e_1 + 2e_2$. La partie $\{e_1 + e_2, e_1 + 2e_2\}$ est une base. $\triangle$

9.12.3 Commutant : cas général

Nous considérons encore un espace vectoriel E de dimension finie n et un endomorphisme $f: E \rightarrow E$. Nous notons μ son polynôme minimal et μ_x le polynôme minimal ponctuel en x .

Lemme 9.199 ([215, 210, 101]).

Nous avons

$$\dim(\mathcal{C}(f)) \geq \dim(E) \quad (9.426)$$

Démonstration. Si f est donnée, l'espace $\mathcal{C}(f)$ est l'espace des solutions de $fg = gf$. Supposons avoir choisi une base de E et notons A la matrice de f et X celle de g . L'équation est $AX - XA = 0$.

Si A est trigonalisable Nous supposons avoir choisi la base de telle sorte que A soit triangulaire supérieure, et nous allons nous contenter de chercher les solutions X qui sont également triangulaires supérieures. S'il y en a déjà plus que n , a fortiori le résultat sera vrai.

Le produit de deux matrices triangulaires supérieures étant une matrice triangulaire supérieure, l'équation $AX - XA$ contient, pour les coefficients de X , $n(n+1)/2$ équations. Mais il se fait que les termes diagonaux ne sont pas de vraies équations parce que

$$(AX - XA)_{kk} = \sum_i (A_{ki}X_{ik} - X_{ki}A_{ik}) = \sum_{k \leq i \leq k} (A_{ki}X_{ik} - X_{ki}A_{ik}) = 0. \quad (9.427)$$

Nous avons donc au maximum

$$\frac{n(n+1)}{2} - n \quad (9.428)$$

équations linéairement indépendantes pour un minimum de $n(n+1)/2$ inconnues. L'espace des solutions est donc de dimension au minimum n .

Cela a l'air d'être une majoration assez large, mais il existe des cas d'égalité.

Si A n'est pas trigonalisable La preuve que nous donnons ici est valable même pour les endomorphismes trigonalisables.

Nous considérons le résultat de Frobenius 9.188. Nous avons donc la structure suivante :

- une décomposition en somme directe $E = E_1 \oplus \dots \oplus E_r$,
- les espaces E_i sont fixés par f ,
- les endomorphismes $f_i = f|_{E_i}$ sont cycliques
- le polynôme minimal de f_i est μ_i et $\prod_{i=1}^r \mu_i = \chi_f$.

Les endomorphismes f_i^k commutent évidemment avec f_j , et la partie $\{f_i^k\}_{k=0,\dots,\deg(\mu_i)-1}$ est libre. Libre en tout cas en tant que partie de $\text{End}(E_i)$. Mais en prolongeant par 0 sur E , ça reste libre en tant que partie de $\text{End}(E)$.

Bien entendu les f_j^k et les f_i^k ($i \neq j$) sont linéairement indépendants dans $\text{End}(E)$ parce qu'ils n'agissent pas sur les mêmes vecteurs. Donc les endomorphismes $f_i^{k_i}$ avec $k_i = 0, \dots, \deg(\mu_i) - 1$ forment une partie libre de $\text{End}(E)$ composée d'endomorphismes qui commutent avec f . Il y en a en tout

$$\sum_{i=1}^r \deg(\mu_i) = \deg(\chi_f) = n. \quad (9.429)$$

Par conséquent $\dim(\mathcal{C}(f)) \geq \dim(E)$.

□

Théorème 9.200 ([201]).

Soit un endomorphisme $f: E \rightarrow E$ sur l'espace vectoriel de dimension finie n . Nous notons μ et χ les polynômes minimal et caractéristique. Nous avons équivalence entre les faits suivants :

- (1) $\mu = \chi$,
- (2) f est cyclique,
- (3) $\mathcal{C}(f) = \mathbb{K}[f]$.

Démonstration. Plusieurs implications. Notons que (1) implique (1) a déjà été démontré par le lemme 9.187.

(1) implique (2) Conformément à ce que nous permet le lemme 9.99 nous choisissons⁶⁹ $a \in E$ de telle sorte à avoir $\mu_a = \mu$. De plus pour $x \in E$ nous considérons l'application

$$\begin{aligned} \varphi_x: \mathbb{K}[X] &\rightarrow E \\ P &\mapsto P(f)x. \end{aligned} \quad (9.430)$$

Nous avons $\varphi_a(P) = P(f)a$. Étant donné que E_a est engendré par les $f^k(a)$ nous avons $\varphi_a(\mathbb{K}[X]) = E_a$. De plus l'application φ_a passe aux classes pour (μ_a) . Pour rappel, un élément de $\mathbb{K}[X]/(\mu_a)$ est de la forme

$$\bar{P} = \{P + Q\mu_a\}_{Q \in \mathbb{K}[X]}. \quad (9.431)$$

Nous considérons donc l'application

$$\varphi_a: \frac{\mathbb{K}[X]}{(\mu_a)} \rightarrow E_a \quad (9.432)$$

et nous prouvons que c'est un isomorphisme d'espace vectoriel.

Linéaire Parce que $(\lambda P + Q)(f) = (\lambda P)(f) + Q(f)$.

Injectif Si $\varphi_a(\bar{P}) = 0$ alors $\varphi_a(P) = 0$ (dans la deuxième, φ_a est l'application définie sur les polynômes et non sur les classes), ce qui montre que P est annulateur de a . Mais par définition 9.95 du polynôme minimal ponctuel, μ_a est générateur de $\ker(\varphi_a)$; donc il existe $Q \in \mathbb{K}[X]$ tel que $P = Q\mu_a$. En d'autres termes, du point de vue du quotient, $\bar{P} = 0$.

Surjectif Si $x \in E_a$ alors il existe des coefficients $x_k \in \mathbb{K}$ tels que $x = \sum_{k=0}^{\deg(\mu_a)-1} x_k f^k(a)$, c'est-à-dire $x = P(f)a = \varphi_a(P)$.

Mais par hypothèse et par choix de a nous avons $\mu_a = \mu = \chi$, donc en fait $E_a = \mathbb{K}[X]/(\chi)$. Mais nous savons que $\deg(\chi) = \dim(E)$ et que $\dim(\mathbb{K}[X]/P) = \deg(P)$ par la proposition 9.107. Au final nous avons $\dim(E_a) = \deg(\chi) = \dim(E)$. Et par conséquent $E_a = E$. Cela prouve que a est un vecteur cyclique pour f .

69. Dans toute la suite, nous devrions écrire μ_f et $\mu_{f,a}$ mais nous omettons d'indiquer explicitement la dépendance en f .

(2) implique (3) Soit $g \in \mathcal{C}(f)$; nous devons prouver que g est un polynôme de f . Par hypothèse nous avons un vecteur cyclique que nous notons v . Nous avons un polynôme P (dépendant de g) tel que $g(v) = P(f)v$. Nous allons voir que $g = P(f)$. Soient $y \in E$ et Q un polynôme tels que $y = Q(f)v$; en notant que g commute avec $P(f)$ nous avons

$$g(y) = g(Q(f)v) = Q(f)(g(v)) = Q(f)(P(f)v) = P(f)Q(f)v = P(f)y. \quad (9.433)$$

Donc $g = P(f)$.

(3) implique (1) Nous avons les inégalités :

$$n \leq \dim(\mathcal{C}(f)) = \dim(\mathbb{K}[f]) = \deg(\mu) \leq \deg(\chi) = n. \quad (9.434)$$

La première est le lemme 9.199. Toutes les inégalités sont des égalités. En particulier $\deg(\mu) = n$, ce qui signifie que $\mu = \chi$ parce que μ est un polynôme diviseur de χ , de même degré que χ et unitaire tout comme χ . □

Corolaire 9.201 ([101]).

En suivant les notations sur les extensions de corps de base de la section 9.10, l'endomorphisme $f: E \rightarrow F$ est cyclique si et seulement si l'endomorphisme $f_{\mathbb{L}}: E_{\mathbb{L}} \rightarrow F_{\mathbb{L}}$ est cyclique.

Démonstration. Nous savons par le théorème 9.200 qu'un endomorphisme est cyclique si et seulement si son polynôme minimal est égal à son polynôme caractéristique. Or par les propositions 9.181 et 9.182, nous savons que ces polynômes sont identiques pour f et pour $f_{\mathbb{L}}$. □

Théorème 9.202 (Similitude et extension de corps[101]).

Les applications linéaires $f, g: E \rightarrow E$ sont semblables si et seulement si $f_{\mathbb{L}}$ et $g_{\mathbb{L}}$ le sont.

Démonstration. En ce qui concerne le sens direct, s'il existe $m \in \text{GL}(E)$ tel que $f = m g m^{-1}$ alors il suffit d'appliquer le lemme 9.177 pour avoir $f_{\mathbb{L}} = m_{\mathbb{L}} g_{\mathbb{L}} m_{\mathbb{L}}^{-1}$.

Nous considérons les invariants de similitude de f du théorème 9.188. Il existe une unique suite de polynômes unitaires μ_i ($i = 1, \dots, s$) tels que $\mu_i \mid \mu_{i+1}$ et pour laquelle nous avons une décomposition $E = E_1 \oplus \dots \oplus E_s$ pour laquelle $f|_{E_i}: E_i \rightarrow E_i$ est cyclique et de polynôme minimal μ_i .

Nous avons aussi $E_{\mathbb{L}} = (E_1)_{\mathbb{L}} \oplus \dots \oplus (E_s)_{\mathbb{L}}$ et les $(E_i)_{\mathbb{L}}$ sont stables sous $f_{\mathbb{L}}$ qui y sera également cyclique (corolaire 9.201). De plus le polynôme minimal de $f_{\mathbb{L}}|_{(E_i)_{\mathbb{L}}}$ est également μ_i .

Autrement dit, la suite μ_i est également la suite des invariants de similitude de $f_{\mathbb{L}}$. La remarque 9.189 nous permet de conclure que f et g sont semblables si et seulement si $f_{\mathbb{L}}$ et $g_{\mathbb{L}}$ le sont. □

9.13 Hyperplans et formes linéaires

Définition 9.203.

Si E est un espace vectoriel de dimension n , un **hyperplan** de E est un sous-espace vectoriel de dimension $n - 1$.

Proposition 9.204 ([216]).

À propos d'hyperplans et de formes linéaires sur un espace vectoriel E sur le corps $\mathbb{K}$.

- (1) Si φ est une forme linéaire non nulle, alors $\ker(\varphi)$ est un hyperplan.
- (2) Si H est un hyperplan de E , il existe une forme linéaire dont H est le noyau :

$$H = \ker(\varphi). \quad (9.435)$$

Démonstration. En deux parties.

- (1) Soit un supplémentaire A de H . Nous considérons la restriction $\varphi_A: A \rightarrow \mathbb{K}$. Vu que les éléments non nuls de A sont hors de H , nous avons $\varphi(x) \neq 0$ dès que x est non nul dans A . Cela implique que φ_A est surjective.

D'autre part, φ_A est également injective : si $\varphi_A(x) = \varphi_A(y)$, alors $\varphi_A(x - y) = 0$, ce qui signifie que $x - y = 0$ ou encore que $x = y$.

Donc φ_A est un isomorphisme de $\mathbb{K}$ -espaces vectoriels ; nous en déduisons par le corolaire 4.40 que A est de dimension 1 sur $\mathbb{K}$, parce que $\mathbb{K}$ est de dimension 1.

- (2) Nous utilisons le théorème de la base incomplète 4.11(4) pour considérer une base $\{e_i\}_{i=1,\dots,n}$ de E telle que $\text{Span}\{e_1, \dots, e_{n-1}\} = H$. Nous pouvons alors considérer la forme linéaire définie par

$$\varphi(e_i) = \begin{cases} 0 & \text{si } i = 1, \dots, n-1 \\ 1 & \text{si } i = n. \end{cases} \quad (9.436)$$

Cette forme vérifie $\ker(\varphi) = H$.

□

Proposition 9.205 ([100]).

Soit un espace vectoriel E de dimension finie $n \geq 2$. Soit un sous-espace vectoriel V de E de dimension s . Alors V est une intersection de $n - s$ hyperplans de E .

Démonstration. Nous considérons une base de V que nous complétons⁷⁰ en une base de E : si $x = \sum_{i=1}^n x_i e_i$, nous avons $x \in V$ si et seulement si $x_{s+1} = \dots = x_n = 0$. Nous considérons les formes linéaires

$$\begin{aligned} \varphi_i: E &\rightarrow \mathbb{R} \\ x &\mapsto x_i, \end{aligned} \quad (9.437)$$

et nous considérons les parties $H_i = \ker(\varphi_i)$ qui sont de hyperplans par la proposition 9.204. Les H_i avec $s+1 \leq i \leq n$ sont une famille de $n - s$ hyperplans qui vérifient

$$V = \bigcap_{i=s+1}^n \ker(\varphi_i) \quad (9.438)$$

parce que $x \in \ker(\varphi_i)$ si et seulement si $x_i = 0$.

Donc V peut être écrit comme intersection de $n - s$ hyperplans de E .

□

Proposition 9.206 ([100]).

Soit un $\mathbb{K}$ -espace vectoriel E de dimension finie $n \geq 2$. Si H_i sont des hyperplans de E , alors

$$\dim\left(\bigcup_{i=1}^m H_i\right) \geq n - m. \quad (9.439)$$

Démonstration. N'oubliez pas de prouver que $\bigcap_{i=1}^m H_i$ est un espace vectoriel. À part ça, nous faisons une petite récurrence.

Pour $m = 2$ Nous savons déjà par la proposition 4.43 que

$$\dim(H_1 \cap H_2) = \dim(H_1) + \dim(H_2) - \dim(H_1 + H_2). \quad (9.440)$$

De plus $\dim(H_1 + H_2) \leq n$. En remplaçant, par les valeurs,

$$\dim(H_1 \cap H_2) = \dim(H_1) + \dim(H_2) - \dim(H_1 + H_2) \quad (9.441a)$$

$$= n - 1 + n - 1 - \dim(H_1 + H_2) \quad (9.441b)$$

$$\geq 2n - 2 - n \quad (9.441c)$$

$$= n - 2. \quad (9.441d)$$

Donc $\dim(H_1 \cap H_2) \geq n - 2$.

70. Théorème de la base incomplète, 4.11(4).

La récurrence Nous calculons $\dim(H_1 \cap \dots \cap H_m \cap H_{m+1})$ en commençant encore par la proposition 4.43 :

$$\dim(H_1 \cap \dots \cap H_m \cap H_{m+1}) = \underbrace{\dim(H_1 \cap \dots \cap H_m)}_{\leq n-m} + \dim(H_{m+1}) \quad (9.442a)$$

$$- \underbrace{\dim((H_1 \cap \dots \cap H_m) + H_{m+1})}_{\leq n} \quad (9.442b)$$

$$\geq n - m + (n - 1) - n \quad (9.442c)$$

$$= n - m - 1. \quad (9.442d)$$

C'est bon pour la récurrence.

□

9.13.1 Trouver la matrice d'une symétrie donnée

Les notions de déterminants, produit scalaire et vectoriels⁷¹ donnent une bonne intuition géométrique des matrices. Nous pouvons alors chercher les matrices de quelques symétries dans $\mathbb{R}^2$ ou $\mathbb{R}^3$.

9.13.1.1 Symétrie par rapport à un plan

Comment trouver par exemple la matrice A qui donne la symétrie autour du plan $z = 0$? La définition d'une telle symétrie est que les vecteurs du plan $z = 0$ ne bougent pas, tandis que les vecteurs perpendiculaires changent de signe. Ces informations vont permettre de trouver comment A agit sur une base de $\mathbb{R}^3$. En effet :

- (1) Le vecteur $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ est dans le plan $z = 0$, donc il ne bouge pas,
- (2) le vecteur $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ est également dans le plan, donc il ne bouge pas non plus,
- (3) et le vecteur $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ est perpendiculaire au plan $z = 0$, donc il va changer de signe.

Cela nous donne directement les valeurs de A sur la base canonique et nous permet d'écrire

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}. \quad (9.443)$$

Pour écrire cela, nous avons juste mis en colonne les images des vecteurs de base. Les deux premiers n'ont pas changé et le troisième a changé.

Et si maintenant on donne un plan moins facile que $z = 0$? Le principe reste le même : il faudra trouver deux vecteurs qui sont dans le plan (et dire qu'ils ne bougent pas), et puis un vecteur qui est perpendiculaire au plan⁷², et dire qu'il change de signe.

Voyons ce qu'il en est pour le plan $x = -z$. Il faut trouver deux vecteurs linéairement indépendants dans ce plan. Prenons par exemple

$$f_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad f_2 = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}. \quad (9.444)$$

71. Définitions 9.8, 9.261 et 11.30.

72. Pour le trouver, penser au produit vectoriel.

Nous avons

$$\begin{aligned} Af_1 &= f_1 \\ Af_2 &= f_2. \end{aligned} \quad (9.445)$$

Afin de trouver un vecteur perpendiculaire au plan, calculons le produit vectoriel :

$$f_3 = f_1 \times f_2 = \begin{vmatrix} e_1 & e_2 & e_3 \\ 0 & 1 & 0 \\ 1 & 0 & -1 \end{vmatrix} = -e_1 - e_3 = \begin{pmatrix} -1 \\ 0 \\ -1 \end{pmatrix}. \quad (9.446)$$

Nous avons

$$Af_3 = -f_3. \quad (9.447)$$

Afin de trouver la matrice A , il faut trouver Ae_1 , Ae_2 et Ae_3 . Pour ce faire, il faut d'abord écrire $\{e_1, e_2, e_3\}$ en fonction de $\{f_1, f_2, f_3\}$. La première des équations (9.444) dit que

$$f_1 = e_2. \quad (9.448)$$

Ensuite, nous avons

$$\begin{aligned} f_2 &= e_1 - e_3 \\ f_3 &= -e_1 - e_3. \end{aligned} \quad (9.449)$$

La somme de ces deux équations donne $-2e_3 = f_2 + f_3$, c'est-à-dire

$$e_3 = -\frac{f_2 + f_3}{2} \quad (9.450)$$

Et enfin, nous avons

$$e_1 = \frac{f_2 - f_3}{2}. \quad (9.451)$$

Maintenant nous pouvons calculer les images de e_1 , e_2 et e_3 en faisant

$$\begin{aligned} Ae_1 &= \frac{Af_2 - Af_3}{2} = \frac{1}{2} \begin{pmatrix} 0 \\ 0 \\ -2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix}, \\ Ae_2 &= Af_1 = f_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \\ Ae_3 &= -\frac{f_2 - f_3}{2} = -\frac{1}{2} \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix}. \end{aligned} \quad (9.452)$$

La matrice A s'écrit maintenant en mettant les trois images trouvées en colonnes :

$$A = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}. \quad (9.453)$$

9.13.1.2 Symétrie par rapport à une droite

Le principe est exactement le même : il faut trouver trois vecteurs f_1 , f_2 et f_3 sur lesquels on connaît l'action de la symétrie. Ensuite il faudra exprimer e_1 , e_2 et e_3 en termes de f_1 , f_2 et f_3 .

Le seul problème est de trouver les trois vecteurs f_i . Le premier est tout trouvé : c'est n'importe quel vecteur sur la droite. Pour les deux autres, il faut un peu ruser parce qu'il faut impérativement qu'ils soient perpendiculaire à la droite. Pour trouver f_2 , on peut écrire

$$f_2 = \begin{pmatrix} 1 \\ 0 \\ x \end{pmatrix}, \quad (9.454)$$

et puis fixer le x pour que le produit scalaire de f_2 avec f_1 soit nul. S'il n'y a pas moyen (genre si f_1 a sa troisième composante nulle), essayer avec $\begin{pmatrix} x \\ 1 \\ 0 \end{pmatrix}$. Une fois que f_2 est trouvé (il y a des milliards de choix possibles), trouver f_3 est super facile : prendre le produit vectoriel entre f_1 et f_2 .

9.13.1.3 En résumé

La marche à suivre est

- (1) Trouver trois vecteurs f_1 , f_2 et f_3 sur lesquels on connaît l'action de la symétrie. Typiquement : des vecteurs qui sont sur l'axe ou le plan de symétrie, et puis des perpendiculaires. Pour la perpendiculaire, penser au produit scalaire et au produit vectoriel.
- (2) Exprimer la base canonique e_1 , e_2 et e_3 en termes de f_1 , f_2 , f_3 .
- (3) Trouver Ae_1 , Ae_2 et Ae_3 en utilisant leur expression en termes des f_i , et le fait que l'on connaisse l'action de A sur les f_i .
- (4) La matrice s'obtient en mettant les images des e_i en colonnes.

9.14 Théorème de Burnside

Lemme 9.207.

Soit P , un polynôme sur $\mathbb{K}$. Une racine de P est une racine simple si et seulement si elle n'est pas racine de P' .

Théorème 9.208.

Toute représentation⁷³ d'un groupe abélien d'exposant fini sur $\mathbb{C}^n$ a une image finie.

Démonstration. Étant donné que G est d'exposant fini, il existe $\alpha \in \mathbb{N}^*$ tel que $g^\alpha = e$ pour tout $g \in G$. Le polynôme $P(X) = X^\alpha - 1$ est scindé à racines simples. En effet tout polynôme sur $\mathbb{C}$ est scindé. Le fait qu'il soit à racines simples provient du lemme 9.207 parce que si $a^\alpha = 1$, alors il n'est pas possible d'avoir $\alpha a^{\alpha-1} = 0$.

Par ailleurs $P(g) = 0$. Le fait que nous ayons un polynôme annulateur de g scindé à racines simples implique que g est diagonalisable (théorème 9.129). Le fait que G soit abélien montre qu'il existe une base de $\mathbb{C}^n$ dans laquelle tous les éléments de G sont diagonaux. Nous devons par conséquent montrer qu'il existe un nombre fini de matrices de la forme

$$\begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}. \quad (9.455)$$

Nous savons que $\lambda_i^\alpha = 1$ parce que $g^\alpha = \mathbb{1}$, par conséquent chacun des λ_i est une racine de l'unité dont il n'existe qu'un nombre fini. $\square$

Théorème 9.209 (Burnside[90, 217]).

Un sous-groupe de $\mathrm{GL}(n, \mathbb{C})$ est fini si et seulement s'il est d'exposant⁷⁴ fini.

Démonstration. Soit G un sous-groupe de $\mathrm{GL}(n, \mathbb{C})$. Si G est fini, l'ordre de ses éléments divise $|G|$ (corolaire 2.36 au théorème de Lagrange) et l'exposant est le PPCM qui est donc fini également. Le théorème est déjà démontré dans un sens.

Dans l'autre sens, nous notons $e < \infty$ l'exposant de G , et nous allons prouver que l'ensemble G est fini. Nous commençons par remarquer que tous les éléments de G sont des racines du polynôme $X^e - 1$, et ensuite nous nous lançons dans le travail.

⁷³. Définition 4.145.

⁷⁴. Définition 2.21.

Générateurs Le groupe G est une partie de $\mathbb{M}(n, \mathbb{C})$ dont nous considérons l'algèbre engendrée ⁷⁵ $\mathcal{G}$. Soit $C_1, \dots, C_r$ une famille génératrice de $\mathcal{G}$ constituée d'éléments de G et la fonction

$$\begin{aligned} \tau: G &\rightarrow \mathbb{C}^r \\ A &\mapsto (\operatorname{Tr}(AC_1), \dots, \operatorname{Tr}(AC_r)). \end{aligned} \quad (9.456)$$

τ est injective Soient $A, B \in G$ tels que $\tau(A) = \tau(B)$. Si C_i est un générateur de G , nous avons $\operatorname{Tr}(AC_i) = \operatorname{Tr}(BC_i)$ et par la linéarité de la trace, nous avons

$$\operatorname{Tr}(AM) = \operatorname{Tr}(BM) \quad (9.457)$$

pour tout $M \in G$. Notons par ailleurs

$$N = AB^{-1} - \mathbb{1}, \quad (9.458)$$

qui est diagonalisable parce que $AB^{-1} \in G$ et donc est annulé par le polynôme $X^e - 1$ qui est scindé à racines simples. Du coup AB^{-1} est diagonalisable ; posons $PAB^{-1}P^{-1} = D$, alors $P(AB^{-1} - \mathbb{1})P^{-1} = D - \mathbb{1}$ qui est encore diagonale. Donc N est diagonalisable.

Par ailleurs nous avons

$$\operatorname{Tr}((AB^{-1})^p) = \operatorname{Tr}(AB^{-1}(AB^{-1})^{p-1}) \quad (9.459a)$$

$$= \operatorname{Tr}(BB^{-1}(AB^{-1})^{p-1}) \quad (9.457) \quad (9.459b)$$

$$= \operatorname{Tr}((AB^{-1})^{p-1}). \quad (9.459c)$$

En continuant nous obtenons

$$\operatorname{Tr}((AB^{-1})^p) = \operatorname{Tr}(\mathbb{1}) = n. \quad (9.460)$$

D'autre part,

$$N^k = (AB^{-1} - \mathbb{1})^k = \sum_{p=0}^k \binom{p}{k} (-1)^{k-p} (AB^{-1})^p \quad (9.461)$$

En prenant la trace, et en tenant compte du fait que $\operatorname{Tr}((AB^{-1})^p) = n$,

$$\operatorname{Tr}(N^k) = \sum_{p=0}^k \binom{p}{k} (-1)^{k-p} n = n(1-1)^k = 0. \quad (9.462)$$

Donc la trace de N^k est nulle et le lemme 9.122 nous enseigne que N est alors nilpotente. Étant donné qu'elle est aussi diagonalisable, elle est nulle. Nous en concluons que $AB^{-1} = \mathbb{1}$ et donc que $A = B$. La fonction τ est donc injective.

Nombre fini de valeurs Les éléments de G sont annulés par $X^e - 1$ qui est un polynôme scindé à racines simples. Donc le polynôme minimal d'un élément de G est (a fortiori) scindé à racines simples et le théorème 9.129 nous assure alors que ces éléments sont diagonalisables. Du coup les valeurs propres des matrices de G sont des racines e ïèmes de l'unité. Par conséquent les traces des éléments de G ne peuvent prendre qu'un nombre fini de valeurs : toutes les sommes de n racines e ïèmes de l'unité. Mais vu que les C_i sont dans G , nous avons

$$\operatorname{Image}(\tau) = \{\operatorname{Tr}(A) \text{ tel que } A \in G\}^r, \quad (9.463)$$

qui est un ensemble fini. Par conséquent G est fini parce que τ est injective.

□

75. Définition 1.230.

9.14.1 Théorème de Lie-Kolchin

Contrairement à ce que l'on peut parfois croire, il n'est pas vrai que toute matrice à coefficient réel est diagonalisable, même pas sur $\mathbb{C}$. La raison est qu'une telle matrice peut très bien avoir des valeurs propres multiples.

Exemple 9.210.

Le théorème 9.129 nous donne une façon simple de trouver des matrices non diagonalisables sur $\mathbb{C}$: il suffit que le polynôme minimal ne soit pas scindé à racines simples. Par exemple

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad (9.464)$$

dont le polynôme caractéristique est $\chi_A = (1 - X)^2$. Ce polynôme n'a manifestement pas des racines simples. Nous pouvons faire le calcul explicite pour montrer que A n'est pas diagonalisable. D'abord l'unique valeur propre de A est 1 et nous pouvons sans peine résoudre

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \quad (9.465)$$

qui revient au système

$$\begin{cases} x + y = x \\ y = y. \end{cases} \quad \begin{matrix} (9.466a) \\ (9.466b) \end{matrix}$$

La première équation donne directement $y = 0$. Le seul espace propre est de dimension 1 et est engendré par $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$. $\triangle$

La remarque 9.159 donne un exemple un peu plus avancé, qui montre la multiplicité algébrique et géométrique d'une racine d'un polynôme caractéristique.

Lemme 9.211 (Trigonalisation simultanée).

Une famille de matrices de $\mathrm{GL}(n, \mathbb{C})$ commutant deux à deux est simultanément trigonalisable.

Démonstration. Commençons par enfoncer une porte ouverte par la proposition 9.136 : toutes les matrices de $\mathrm{GL}(n, \mathbb{C})$ sont trigonalisables parce que tous les polynômes sont scindés.

Nous effectuons la démonstration par récurrence sur la dimension. Si $n = 1$ alors toutes les matrices sont triangulaires et nous ne nous posons pas de questions. Nous supposons donc $n > 1$.

Soit la famille $(A_i)_{i \in I}$ dans $\mathrm{GL}(n, \mathbb{C})$ et A_0 un de ses éléments. Nous nommons $\lambda_1, \dots, \lambda_r$ les valeurs propres distinctes de A_0 . Le théorème de décomposition primaire 9.160 nous donne la somme directe d'espaces caractéristiques⁷⁶

$$E = F_{\lambda_1}(A_0) \oplus \dots \oplus F_{\lambda_r}(A_0). \quad (9.467)$$

Nous pouvons supposer que cette somme n'est pas réduite à un seul terme. En effet si tel était le cas, A_0 serait un multiple de l'identité parce que A_0 n'aurait qu'une seule valeur propre et les sommes dans la décomposition de Dunford 9.162(3) se réduisent à un seul terme (et $p_i = \mathrm{Id}$). En particulier les dimensions des espaces $F_\lambda(A_0)$ sont strictement plus petites que n .

Vu que tous les A_i commutent avec A_0 , les espaces $F_\lambda(A_0)$ sont stables par les A_i et nous pouvons trigonaliser les A_i simultanément sur chacun des $F_\lambda(A_0)$ en utilisant l'hypothèse de récurrence. $\square$

Théorème 9.212 (Lie-Kolchin[218]).

Tout sous-groupe connexe et résoluble de $\mathrm{GL}(n, \mathbb{C})$ est conjugué à un groupe de matrices triangulaires.

⁷⁶. Définition 9.157.

Démonstration. Soit G un sous-groupe connexe et résoluble de $\mathrm{GL}(n, \mathbb{C})$.

Si sous-espace non trivial stable par G Nous commençons par voir ce qu'il se passe s'il existe un sous-espace vectoriel non trivial V de $\mathbb{C}^n$ stabilisé par G . Pour cela nous considérons une base de $\mathbb{C}^n$ dont les premiers éléments forment une base de V (base incomplète, théorème 4.11). Les éléments de G s'écrivent, dans cette base,

$$\begin{pmatrix} g_1 & * \\ 0 & g_2 \end{pmatrix}. \quad (9.468)$$

Les matrices g_1 et g_2 sont carrés. Nous considérons alors l'application ψ définie par

$$\begin{aligned} \psi: G &\rightarrow \mathrm{GL}(V) \\ g &\mapsto g_1. \end{aligned} \quad (9.469)$$

Cela est un morphisme de groupes parce que

$$\begin{pmatrix} g_1 & * \\ 0 & g_2 \end{pmatrix} \begin{pmatrix} h_1 & * \\ 0 & h_2 \end{pmatrix} = \begin{pmatrix} g_1 h_1 & * \\ 0 & g_2 h_2 \end{pmatrix}, \quad (9.470)$$

de telle sorte que $\psi(gh) = \psi(g)\psi(h)$.

Le groupe $\psi(G)$ est connexe et résoluble. En effet $\psi(G)$ est connexe en tant qu'image d'un connexe par une application continue (proposition 7.95). Et il est résoluble en tant qu'image d'un groupe résoluble par un homomorphisme par la proposition 2.46. Vu que $\psi(G)$ est un sous-groupe résoluble et connexe de $\mathrm{GL}(V)$ et que la dimension de V est strictement plus petite que celle de $\mathbb{C}^n$, une récurrence sur la dimension indique que $\psi(G)$ est conjugué à un groupe de matrices triangulaires. C'est-à-dire qu'il existe une base de V dans laquelle toutes les matrices g_1 (avec $g \in G$) sont triangulaires supérieures.

On fait de même avec l'application $g \mapsto g_2$, ce qui donne une base du supplémentaire de V dans laquelle les matrices g_2 sont triangulaires.

En couplant ces deux bases, nous obtenons une base de $\mathbb{C}^n$ dans laquelle toutes les matrices (9.468) (c'est-à-dire toutes les matrices de G) sont triangulaires supérieures.

Sinon Nous supposons à présent que $\mathbb{C}^n$ n'a pas de sous-espaces non triviaux stables sous G . Nous posons $m = \min\{k \text{ tel que } D^k(G) = \{e\}\}$, qui existe parce que G est résoluble et que sa suite dérivée termine sur e (proposition 2.45).

Si $m = 1$ Si $m = 1$ alors G est abélien et il existe une base de G dans laquelle toutes les matrices de G sont triangulaires (lemme 9.211). Le premier vecteur d'une telle base serait stable par G , mais comme nous avons supposé qu'il n'y avait pas de sous-espaces non triviaux stabilisés par G , il faut déduire que ce vecteur stable est à lui tout seul non trivial, c'est-à-dire que $n = 1$. Dans ce cas, le théorème est démontré.

Si $m > 1$ Nous devons maintenant traiter le cas où $m > 1$. Nous posons $H = D^{m-1}(G)$; cela est un sous-groupe normal et abélien de G . Encore une fois le résultat de trigonalisation simultanée 9.211 donne une base dans laquelle tous les éléments de H sont triangulaires. En particulier le premier élément de cette base est un vecteur propre commun à toutes les matrices de H .

Soit V le sous-espace engendré par tous les vecteurs propres communs de H . Nous venons de voir que V n'est pas vide. Nous allons montrer que V est stable par G . Soient $h \in H$, $v \in V$ et $g \in G$:

$$h(g(v)) = g \underbrace{g^{-1}hg}_{\in H}(v) = g(\lambda v) = \lambda g(v) \quad (9.471)$$

parce que v est vecteur propre de $g^{-1}hg$. Ce que le calcul (9.471) montre est que $g(v)$ est vecteur propre de h pour la valeur propre λ . Donc $g(v) \in V$ et V est stabilisé par G . Mais comme il n'existe pas d'espaces non triviaux stabilisés par G , nous en déduisons que $V = \mathbb{C}^n$. Donc tous les vecteurs de $\mathbb{C}^n$ sont vecteurs propres communs de H . Autrement dit on a une base de diagonalisation simultanée de H .

H est dans le centre de G Montrons à présent que H est dans le centre de G , c'est-à-dire que pour tout $g \in G$ et $h \in H$ il faut $ghg^{-1} = h$. D'abord ghg^{-1} est une matrice diagonale (parce que elle est dans H) ayant les mêmes valeurs propres que h . En effet si λ est valeur propre de ghg^{-1} pour le vecteur propre v , alors

$$(ghg^{-1})(v) = \lambda v \quad (9.472a)$$

$$h(g^{-1}v) = \lambda(g^{-1}v), \quad (9.472b)$$

c'est-à-dire que λ est également valeur propre de h , pour le vecteur propre $g^{-1}v$. Mais comme h a un nombre fini de valeurs propres, il n'y a qu'un nombre fini de matrices diagonales ayant les mêmes valeurs propres que h . L'ensemble $\mathbf{Ad}(G)h$ est donc un ensemble fini. D'autre part, l'application $g \mapsto g^{-1}hg$ est continue, et G est connexe, donc l'ensemble $\mathbf{Ad}(G)h$ est connexe. Un ensemble fini et connexe dans $\mathrm{GL}(n, \mathbb{C})$ est nécessairement réduit à un seul point. Cela prouve que $ghg^{-1} = h$ pour tout $g \in G$ et $h \in H$.

Espaces propres stables pour tout G Soit $h \in H$ et W un espace propre de h (ça existe non vide parce que H est triangularisé, voir plus haut). Alors nous allons prouver que W est stable pour tous les éléments de G . En effet si $w \in W$ avec $h(w) = \lambda w$ alors en permutant g et h ,

$$hg(w) = g(hw) = \lambda g(w), \quad (9.473)$$

donc $g(w)$ est aussi vecteur propre de h pour la valeurs propre λ , c'est-à-dire que $g(w) \in W$. Vu que nous supposons que $\mathbb{C}^n$ n'a pas d'espaces invariants non triviaux, nous devons conclure que $W = \mathbb{C}^n$, c'est-à-dire que H est composé d'homothéties. C'est-à-dire que pour tout $h \in H$ nous avons $h = \lambda_h \mathbb{1}$.

Contradiction sur la minimalité de m Les éléments d'un groupe dérivé sont de déterminant 1 parce que $\det(g_1 g_2 g_1^{-1} g_2^{-1}) = 1$. Par conséquent pour tout h , le nombre λ_h est une racine n^{e} de l'unité. Vu qu'il n'y a qu'une quantité finie de racines n^{e} de l'unité, le groupe H est fini et connexe et donc une fois de plus réduit à un élément, c'est-à-dire $H = \{e\}$. Cela contredit la minimalité de m et donc produit une contradiction. Nous devons donc avoir $m = 1$.

Conclusion Nous avons vu que si $\mathbb{C}^n$ avait un sous-espace non trivial fixé par G alors le théorème était démontré. Par ailleurs si $\mathbb{C}^n$ n'a pas un tel sous-espace, soit $m = 1$ (et alors le théorème est également prouvé), soit $m > 1$ et alors on a une contradiction.

Bref, le théorème est prouvé sous peine de contradiction. □

9.15 Formes bilinéaires et quadratiques

Plus à propos de formes bilinéaires dans le thème 52.

Définition 9.213 ([219]).

Soient trois espaces vectoriels E, F et V sur le même corps commutatif $\mathbb{K}$. Une application $b: E \times F \rightarrow V$ est **bilinéaire** si elle est séparément linéaire en ses deux variables, c'est-à-dire si

$$(1) \quad b(u_1 + u_2, v) = b(u_1, v) + b(u_2, v),$$

$$(2) \quad b(u, v_1 + v_2) = b(u, v_1) + b(u, v_2)$$

$$(3) \quad b(\lambda u, v) = b(u, \lambda v) = \lambda b(u, v)$$

pour tout $u, u_1, u_2 \in E$, $v, v_1, v_2 \in F$ et pour tout $\lambda \in \mathbb{K}$.

Dans le cas $E = F$ et $V = \mathbb{K}$, nous parlons de **forme bilinéaire** sur E .

Nous parlons de forme bilinéaire **symétrique** si de plus $b(u, v) = b(v, u)$.

9.214.

Une application bilinéaire $E \times E \rightarrow \mathbb{K}$ n'est pas une application linéaire ; la distinction est importante. La linéarité est

$$b(\lambda u, \lambda v) = b(\lambda(u, v)) = \lambda b(u, v) \quad (9.474)$$

et la bilinéarité est

$$b(\lambda u, v) = b(u, \lambda v) = \lambda b(u, v). \quad (9.475)$$

En réalité la seule forme qui soit à la fois linéaire et bilinéaire est la forme identiquement nulle : la condition

$$b(\lambda u, \lambda v) = \lambda^2 b(u, v) = \lambda b(u, v) \quad (9.476)$$

pour tout $\lambda \in \mathbb{K}$ implique $b(u, v) = 0$.

Exemple 9.215 ([220]).

L'application

$$\begin{aligned} b: \mathbb{M}(n, \mathbb{K}) \times \mathbb{M}(n, \mathbb{K}) &\rightarrow \mathbb{K} \\ (A, B) &\mapsto \text{Tr}(AB) \end{aligned} \quad (9.477)$$

est une forme bilinéaire symétrique.

La vérification est un calcul :

$$\text{Tr}(BA) = \sum_i (BA)_{ii} = \sum_{ik} B_{ik} A_{ki} = \sum_{ik} A_{ki} B_{ik} = \sum_k (AB)_{kk} = \text{Tr}(AB). \quad (9.478)$$

△

9.15.1 Dégénérescence d'une forme bilinéaire

Soit b , une forme bilinéaire symétrique non dégénérée sur l'espace vectoriel E de dimension n sur $\mathbb{K}$ où $\mathbb{K}$ est un corps de caractéristique différente de 2. Nous notons q la forme quadratique associée.

Définition 9.216.

Une forme bilinéaire est **non dégénérée** $b(x, z) = 0$ pour tout z implique $x = 0$.

Lemme 9.217.

Soit b une forme bilinéaire non dégénérée. Si x et y sont tels que $b(x, z) = b(y, z)$ pour tout z , alors $x = y$.

Démonstration. C'est immédiat du fait de la linéarité en le premier argument et de la non-dégénérescence : si $b(x, z) - b(y, z) = 0$ alors

$$b(x - y, z) = 0 \quad (9.479)$$

pour tout z , ce qui implique $x - y = 0$. □

Proposition 9.218.

Une forme bilinéaire est non-dégénérée⁷⁷ si et seulement si sa matrice associée est inversible.

Démonstration. Nous savons que la matrice associée est symétrique et qu'elle peut donc être diagonalisée (théorème 9.146). En nous plaçant dans une base de diagonalisation, nous devons prouver que la forme est non-dégénérée si et seulement si les éléments diagonaux de la matrice sont tous non nuls.

Écrivons $b(x, z)$ en choisissant pour z le vecteur de base e_k de composantes $(e_k)_j = \delta_{kj}$:

$$b(x, e_k) = \sum_{ij} x_i (e_k)_j = \sum_i b_{ik} x_i = b_{kk} x_k. \quad (9.480)$$

Si b est dégénérée et si x est un vecteur non nul (disons que la composante x_i est non nulle) de E tel que $b(x, z) = 0$ pour tout $z \in E$, alors $b_{ii} = 0$, ce qui montre que la matrice de b n'est pas inversible.

Réciproquement si la matrice de b est inversible, alors tous les b_{kk} sont différents de zéro, et le seul vecteur x tel que $b_{kk} x_k = 0$ pour tout k est le vecteur nul. □

77. Définition 9.216.

9.15.2 Topologie

La topologie considérée sur $Q(E)$ est celle de la norme

$$N(q) = \sup_{\|x\|_E=1} |q(x)|, \quad (9.481)$$

qui du point de vue de $S(n, \mathbb{R})$ est

$$N(A) = \sup_{\|x\|_E=1} |x^t A x|. \quad (9.482)$$

Notons que à droite, c'est la valeur absolue usuelle sur $\mathbb{R}$.

Proposition 9.219.

Soit $\{e_i\}$ une base de E . L'application

$$\begin{aligned} \phi: Q(E) &\rightarrow S(n, \mathbb{R}) \\ q &\mapsto (b(e_i, e_j))_{i,j} \end{aligned} \quad (9.483)$$

où b est forme bilinéaire associée à q est une bijection linéaire et continue⁷⁸.

Démonstration. Si $\phi(q) = \phi(q')$; alors

$$q(x) = \sum_{i,j} \phi(q)_{ij} x_i x_j = \sum_{i,j} \phi(q')_{ij} x_i x_j = q'(x). \quad (9.484)$$

Donc $q = q'$. L'application ϕ est donc injective

De plus elle est surjective parce que si $B \in S(n, \mathbb{R})$ alors la forme quadratique

$$q(x) = \sum_{i,j} B_{ij} x_i x_j \quad (9.485)$$

a évidemment B comme matrice associée. L'application ϕ est donc surjective.

Notre application ϕ est de plus linéaire parce que l'association d'une forme quadratique à la forme bilinéaire associée est linéaire.

En ce qui concerne la continuité, nous la prouvons en zéro en considérant une suite convergente $q_n \xrightarrow{Q(E)} 0$. C'est-à-dire que

$$\sup_{\|x\|=1} |q_n(x)| \rightarrow 0. \quad (9.486)$$

Nous rappelons l'identité de polarisation :

$$b_n(x, y) = \frac{1}{2} (q_n(x - y) - q(x) - q(y)). \quad (9.487)$$

En ce qui concerne deux des trois termes, il n'y a pas de problèmes :

$$|\phi(q_n)_{ij}| = |b_n(e_i, e_j)| \leq \frac{1}{2} |b_n(e_i - e_j)| + \frac{1}{2} |q_n(e_i)| + \frac{1}{2} |q_n(e_j)|. \quad (9.488)$$

Si n est assez grand, nous avons tout de suite

$$|\phi(q_n)_{ij}| \leq \frac{1}{2} |q_n(e_i - e_j)| + \epsilon. \quad (9.489)$$

Nous définissons e_{ij} et α_{ij} de telle sorte que $e_i - e_j = \alpha_{ij} e_{ij}$ avec $\|e_{ij}\| = 1$. Si $\alpha = \max\{\alpha_{ij}, 1\}$ alors nous avons

$$q_n(e_i - e_j) = \alpha_{ij}^2 q_n(e_{ij}) \leq \alpha^2 q_n(e_{ij}). \quad (9.490)$$

Il suffit maintenant de prendre n assez grand pour avoir $\sup_{\|x\|=1} |q_n(x)| \leq \frac{\epsilon}{\alpha^2}$ pour avoir

$$|\phi(q_n)_{ij}| \leq \frac{\epsilon}{2} + \frac{\epsilon}{\alpha^2}. \quad (9.491)$$

□

⁷⁸. Pour les topologies des normes (9.481) et (9.482).

9.15.3 Isotropie

Définition 9.220 (Isotropie).

Un vecteur est **isotrope** pour b s'il est perpendiculaire à lui-même ; en d'autres termes, x est isotrope si et seulement si $b(x, x) = 0$. Un sous-espace $W \subset E$ est **totalelement isotrope** si pour tout $x, y \in W$, nous avons $b(x, y) = 0$.

Le **cône isotrope** de b est l'ensemble de ses vecteurs isotropes :

$$C(b) = \{x \in E \text{ tel que } b(x, x) = 0\}. \quad (9.492)$$

Nous introduisons quelques notations. D'abord pour $y \in E$ nous notons

$$\begin{aligned} \Phi_y : E &\rightarrow \mathbb{R} \\ x &\mapsto b(x, y) \end{aligned} \quad (9.493)$$

et ensuite

$$\begin{aligned} \Phi : E &\rightarrow E^* \\ y &\mapsto \Phi_y. \end{aligned} \quad (9.494)$$

Définition 9.221.

Le fait pour une forme bilinéaire b d'être dégénérée signifie que l'application Φ n'est pas injective. Le **noyau** de la forme bilinéaire est celui de Φ , c'est-à-dire

$$\ker(b) = \{z \in E \text{ tel que } b(z, y) = 0 \forall y \in E\}. \quad (9.495)$$

Autrement dit, $\ker(b) = E^\perp$ où le perpendiculaire est pris par rapport à b .

Notons tout de même que nous utilisons la notation $\perp$ même si b est dégénérée et éventuellement pas positive ; c'est-à-dire même si la formule $(x, y) \mapsto b(x, y)$ ne fournit pas un produit scalaire.

9.16 Formes bilinéaires et quadratiques

Plus à propos de formes bilinéaires dans le thème 52.

9.16.1 Généralités

Définition 9.222 ([221]).

Soit un espace vectoriel E et $\mathbb{F}$ un corps de caractéristique différente de 2. Une **forme quadratique** sur E est une application $q : E \rightarrow \mathbb{F}$ pour laquelle il existe une forme bilinéaire symétrique $b : E \times E \rightarrow \mathbb{F}$ satisfaisant $q(x) = b(x, x)$ pour tout $x \in E$.

L'ensemble des formes quadratiques réelles sur E est noté $Q(E)$.

Définition 9.223 (Application bilinéaire définie positive, thème 45).

Si b est une application bilinéaire⁷⁹ sur un espace vectoriel E nous disons qu'elle est

- (1) **définie positive** si $b(x, x) \geq 0$ pour tout $x \in E$ et $b(x, x) = 0$ si et seulement si $x = 0$.
- (2) **semi-définie positive** si $b(x, x) \geq 0$ pour tout $x \in E$. Nous dirons aussi parfois qu'elle est simplement « positive ».

Cela est évidemment à lier à la définition 9.148 et à la proposition 9.229 : une application bilinéaire est définie positive si et seulement si sa matrice symétrique associée l'est.

Proposition 9.224.

Soit une forme bilinéaire b et la forme quadratique associée q . Alors nous avons l'**identité de polarisation** :

$$b(x, y) = \frac{1}{2}(q(x) + q(y) - q(x - y)). \quad (9.496)$$

79. Définition 9.213.

Démonstration. Il suffit de substituer dans le membre de droite $q(x) = b(x, y)$ et d'utiliser la bilinéarité :

$$q(x) + q(y) - q(x - y) = b(x, x) + b(y, y) - b(x - y, x - y) \quad (9.497a)$$

$$= b(x, x) + b(y, y) - b(x) + b(x, y) + b(y, x) - b(y, y) \quad (9.497b)$$

$$= 2b(x, y) \quad (9.497c)$$

où nous avons utilisé le fait que b est symétrique : $b(x, y) = b(y, x)$. $\square$

Lemme 9.225.

Si q est une forme quadratique, il existe une unique forme bilinéaire b telle que $q(x) = b(x, x)$.

Démonstration. L'existence n'est pas en cause : c'est la définition d'une forme quadratique. Pour l'unicité, étant donné une forme quadratique, la forme bilinéaire b doit forcément vérifier l'identité de polarisation de la proposition 9.224. Elle est donc déterminée par q . $\square$

Notons la division par 2 qui est le pourquoi de la demande de la caractéristique différente de 2 pour $\mathbb{F}$ dans la définition de forme quadratique.

Définition 9.226.

Soit une forme quadratique q sur E . Nous disons que $v, w \in E$ sont **q -orthogonaux** si $b(v, w) = 0$ la forme bilinéaire b associée à q par le lemme 9.225.

9.16.2 Matrice associée à une forme bilinéaire

Définition 9.227.

Soit une forme bilinéaire⁸⁰ $b: E \times E \rightarrow \mathbb{K}$ et une base quelconque $\{f_\alpha\}$ de E . Nous définissons les nombres

$$B_{\alpha\beta} = b(f_\alpha, f_\beta), \quad (9.498)$$

qui forment une matrice symétrique dans $\mathbb{M}(n, \mathbb{K})$. Cette matrice est la **matrice associée** à la forme bilinéaire b .

La matrice d'une forme quadratique est celle associée à sa forme bilinéaire associée.

Lemme 9.228.

Soit une forme bilinéaire $b: E \times E \rightarrow \mathbb{K}$ et une base quelconque $\{f_\alpha\}$ de E . Nous notons B la matrice de b (définition 9.227) et q la forme quadratique associée.

Alors nous avons

$$b(x, y) = \sum_{\alpha\beta} B_{\alpha\beta} x_\alpha y_\beta. \quad (9.499)$$

et

$$b(x, y) = x \cdot By. \quad (9.500)$$

où le point est le produit scalaire usuel (composante par composante).

Démonstration. Si $x = \sum_\alpha x_\alpha f_\alpha$ et $y = \sum_\beta y_\beta f_\beta$:

En utilisant la convention (4.84) et les choses autour (voir aussi -2.1),

$$b(x, y) = \sum_\alpha x_\alpha \sum_\beta B_{\alpha\beta} y_\beta = \sum_\alpha x_\alpha (By)_\alpha = x \cdot By. \quad (9.501)$$

$\square$

Proposition 9.229.

Une application bilinéaire est définie positive si et seulement si sa matrice symétrique associée l'est.

80. Définition 9.213.

Démonstration. La définition 9.223 dit que b est strictement définie positive lorsque $b(x, x) \geq 0$ et $b(x, x) = 0$ si et seulement si $x = 0$.

D'autre part, le lemme 9.152 dit que la matrice B est strictement définie positive lorsque $x \cdot Bx \geq 0$ et $x \cdot Bx = 0$ si et seulement si $x = 0$.

Le lien entre les deux est que le lemme 9.228 nous enseigne que pour tout x et y ,

$$b(x, y) = x \cdot By \quad (9.502)$$

où B est la matrice de b . □

Proposition 9.230.

Soit une forme quadratique $q: E \rightarrow \mathbb{K}$ et sa matrice⁸¹ $(q_{ij}) \in \mathbb{M}(n, \mathbb{K})$. Nous avons

$$q(x) = \sum_{i=1}^n \sum_{j=1}^n q_{ij} x_i x_j \quad (9.503a)$$

$$= \sum_{i=1}^n q_{ii} x_i^2 + 2 \sum_{1 \leq i < j \leq n} q_{ij} x_i x_j. \quad (9.503b)$$

9.231.

De nombreux auteurs préfèrent écrire des choses comme $x^t By$ ou $xB^t y$ ou $xB y^t$ et se poser de longues questions sur qui est un « vecteur colonne » et qui est un « vecteur ligne », et si la matrice B soit être transposée ou non. Toutes ces notations servent(?) à cacher un bête produit scalaire.

9.232.

Notons que la matrice associée à une forme bilinéaire (ou quadratique associée) est uniquement valable pour une base donnée. Si nous changeons de base, la matrice change. Cependant lorsque nous travaillons sur $\mathbb{R}^n$, la base canonique est tellement canonique que nous allons nous permettre de parler de « la » matrice associée à une forme bilinéaire.

9.16.3 Changement de base : matrice d'une forme bilinéaire

Proposition 9.233 (Voir la section -2.1).

Soit une forme bilinéaire⁸² $b: V \times V \rightarrow \mathbb{K}$ dont la matrice⁸³ dans la base $\{e_i\}$ est A et celle dans la base $\{f_\alpha\}$ est B . Nous supposons que les bases sont liées par $f_\alpha = \sum_i Q_{i\alpha} e_i$. Alors

$$B = Q^t A Q. \quad (9.504)$$

Démonstration. Soit $x, x' \in V$ de coordonnées (x_i) et (x'_i) dans la base $\{e_i\}$ et $(y_\alpha), (y'_\alpha)$ dans la base $\{f_\alpha\}$. Par définition de la matrice associée à une forme bilinéaire,

$$b(x, x') = \sum_{ij} A_{ij} x_i x'_j = \sum_{\alpha\beta} B_{\alpha\beta} y_\alpha y'_\beta. \quad (9.505)$$

En remplaçant les x_i et x'_i par leurs valeurs en fonction de y_α et y'_β données par la proposition 4.111, nous trouvons

$$b(x, x') = \sum_{ij\alpha\beta} A_{ij} Q_{i\alpha} y_\alpha Q_{j\beta} y'_\beta \quad (9.506a)$$

$$= \sum_{\alpha\beta} (Q^t A Q)_{\alpha\beta} y_\alpha y'_\beta \quad (9.506b)$$

où Q^t désigne la transposée de la matrice $Q: Q_{ij}^t = Q_{ji}$. Vu que les nombres y_α et y'_β sont arbitraires nous déduisons⁸⁴ que $B = Q^t A Q$. □

81. Matrice associée à une forme quadratique, définition 9.227.

82. Définition 9.213

83. Définition 9.498.

84. Lemme 4.62.

Remarque 9.234.

Notons que cette « loi de transformation » n'est pas la même que celle pour une application linéaire⁸⁵. Ici nous avons Q^t alors que pour les applications linéaires nous avons Q^{-1} .

Pour cette raison, tant que nous travaillons avec des bases orthonormées, c'est-à-dire tant que Q est orthogonale⁸⁶, nous pouvons confondre une application linéaire avec une application bilinéaire en passant par la matrice. Mais cette identification n'est pas du tout canonique : elle repose sur le fait que les bases soient orthonormées.

Il en découle que la réduction des endomorphismes et la réduction des formes bilinéaires ne sont pas tout à fait les mêmes théories. Par exemple la pseudo-diagonalisation simultanée (corolaire 11.42) est un résultat de réduction de forme bilinéaire et non d'endomorphismes.

9.16.4 Diagonalisation**Lemme-Définition 9.235.**

Soit une forme quadratique q sur l'espace vectoriel V sur $\mathbb{K}$. Soit A la matrice de q dans la base $\{e_i\}$ et B sa matrice dans la base $\{f_\alpha\}$. Nous supposons que le changement de base est orthogonal.

Alors les valeurs propres de A et B sont les mêmes.

Ces valeurs sont les **valeurs propres** de q .

Démonstration. Nous nous rappelons de la définition 9.227 de la matrice associée à Q , et à la proposition 9.233 qui parle de changement de base : $B = Q^t A Q$ où Q est orthogonale.

Soit un vecteur propre v de A , de valeur propre λ . Alors nous prouvons que $Q^t v$ est un vecteur propre pour B , de même valeur propre λ . En effet,

$$BQ^t v = Q^t A Q Q^t v = Q^t A v = \lambda Q^t v \quad (9.507)$$

où nous avons utilisé $Q Q^t = \mathbb{1}$ et $A v = \lambda v$. □

Proposition 9.236.

Dans la base de diagonalisation de sa matrice associée, une forme quadratique a la forme

$$q(x) = \sum_i \lambda_i x_i^2 \quad (9.508)$$

où les λ_i sont les valeurs propres de la matrice associée à q .

Démonstration. Soit q une forme quadratique et b la forme bilinéaire associée. Si $\{f_i\}$ est une base de diagonalisation⁸⁷ de la matrice de b alors dans cette base nous avons

$$q(x) = b(x, x) = \sum_{ij} x_i x_j b(f_i, f_j) = \sum_i \lambda_i x_i^2 \quad (9.509)$$

où les λ_i sont les valeurs propres de la matrice de b . □

Notons que si nous choisissons une autre base de diagonalisation, les λ_i ne changent pas (à part l'ordre éventuellement).

Cela justifie la définition pour dire que nous nous permettrons de parler des **valeurs propres** d'une forme quadratique comme étant les valeurs propres de la matrice associée.

9.16.5 Réduction de Gauss**Théorème 9.237** (Réduction de Gauss[222, 223]).

Soit une forme quadratique non nulle q sur l'espace vectoriel E sur le corps $\mathbb{K}$. Il existe une base $\{l_i\}_{i=1,\dots,n}$ de E^* et des coefficients $\alpha_i \in \mathbb{K}$ tels que

$$q(x) = \sum_{i=1}^n \alpha_i l_i(x)^2. \quad (9.510)$$

85. Proposition 4.114.

86. Définition 4.94.

87. Qui existe parce que la matrice est symétrique, théorème 9.146.

Démonstration. Notre point de départ sont les formules (9.503) pour la forme quadratique. Nous allons faire la preuve par récurrence sur la dimension de l'espace. Si $n = 1$, alors nous avons seulement

$$q(x) = \alpha x^2 \quad (9.511)$$

et donc le théorème est fait avec $l(x) = x$.

Nous supposons que le théorème est prouvé pour tout espace de dimension n . Une forme quadratique pour un espace de dimension $n + 1$ s'écrit

$$q(x) = \sum_{i=1}^{n+1} m_{ii} x_i^2 + 2 \sum_{1 \leq i < j \leq n+1} m_{ij} x_i x_j. \quad (9.512)$$

Vu que q est non nulle, un des m_{ij} est non nul. Nous allons diviser en plusieurs cas.

- $m_{11} \neq 0$
- $m_{kk} \neq 0$ avec $k \neq 1$
- $m_{12} \neq 0$ et $m_{ii} = 0$ pour tout i .
- $m_{kl} \neq 0$ avec $(k, l) \neq (1, 2)$ et $m_{ii} = 0$ pour tout i .

Ces cas ne sont pas exclusifs, mais ils couvrent toutes les possibilités.

Si $m_{11} \neq 0$ Nous écrivons q sous la forme

$$q(x) = m_{11} x_1^2 + \sum_{i=2}^{n+1} m_{ii} x_i^2 + 2 \sum_{i=1}^n \left(\sum_{j=i+1}^{n+1} m_{ij} x_i x_j \right) \quad (9.513a)$$

$$= m_{11} x_1^2 + \sum_{i=2}^{n+1} m_{ii} x_i^2 + 2 \sum_{j=2}^{n+1} m_{1j} x_1 x_j + 2 \sum_{i=2}^n \sum_{j=i+1}^{n+1} (m_{ij} x_i x_j) \quad (9.513b)$$

$$= m_{11} x_1^2 + 2x_1 \sum_{j=2}^{n+1} m_{1j} x_j + R(x_2, \dots, x_{n+1}) \quad (9.513c)$$

$$= m_{11} \left(x_1^2 + 2x_1 \sum_{j=2}^{n+1} \frac{m_{1j}}{m_{11}} x_j \right) + R(x_2, \dots, x_{n+1}) \quad (9.513d)$$

$$= m_{11} (x_1^2 + 2x_1 f(x_2, \dots, x_{n+1})) + R(x_2, \dots, x_{n+1}) \quad (9.513e)$$

$$= m_{11} (x_1 + f(x_2, \dots, x_{n+1}))^2 - f(x_2, \dots, x_{n+1}) + R(x_2, \dots, x_{n+1}) \quad (9.513f)$$

où

- R est une forme quadratique de $n - 1$ variables ;
- nous avons noté $f(x_2, \dots, x_{n+1}) = \sum_{j=2}^{n+1} \frac{m_{1j}}{m_{11}} x_j$.

Maintenant, toute la partie $-f(x_2, \dots, x_{n+1})^2 + R(x_2, \dots, x_{n+1})$ est une forme quadratique de n variables. Par hypothèse de récurrence, il existe des coefficients α_i et des formes linéairement indépendantes sur $\mathbb{K}^n$ $l'_i(x_2, \dots, x_{n+1})$ telles que

$$-f(x_2, \dots, x_{n+1})^2 + R(x_2, \dots, x_{n+1}) = \sum_{i=2}^{n+1} \alpha_i l'_i(x_2, \dots, x_{n+1})^2. \quad (9.514)$$

En posant ensuite $l_j(x_1, \dots, x_{n+1}) = l'_j(x_2, \dots, x_{n+1})$, ainsi que $l_1(x_1, \dots, x_{n+1}) = x_1 + f(x_2, \dots, x_{n+1})$, nous avons

$$q(x) = m_{11} l_1(x)^2 + \sum_{j=2}^{n+1} \alpha_j l_j(x)^2. \quad (9.515)$$

Si $m_{kk} \neq 0$ avec $k \neq 1$ Nous nommons k le plus petit entier pour lequel $m_{kk} \neq 0$, et nous supposons que $k \neq 1$, parce que nous avons déjà couvert ce cas. Dans ce cas, nous avons

$$q(x) = m_{kk}x_k^2 + \sum_{j=k+1}^{n+1} m_{jj}x_j^2 + 2 \sum_{i=1}^n \left(\sum_{j=i+1}^{n+1} m_{ij}x_i x_j \right), \quad (9.516)$$

et tout tourne comme dans le premier cas.

$m_{ii} = 0$ pour tout i et $m_{12} \neq 0$ Nous écrivons q en séparant les termes m_{1k} :

$$q(x) = 2 \sum_{1 \leq i < j \leq n+1} m_{ij}x_i x_j \quad (9.517a)$$

$$= 2m_{12}x_1x_2 + 2 \sum_{2 \leq j \leq n+1} m_{1j}x_1x_j + 2 \sum_{2 \leq i < j \leq n+1} m_{ij}x_i x_j \quad (9.517b)$$

$$= 2m_{12}x_1x_2 + 2x_1 \sum_{2 \leq j \leq n+1} m_{1j}x_j + 2 \sum_{3 \leq j \leq n+1} m_{2j}x_2x_j + 2 \sum_{3 \leq i < j \leq n+1} m_{ij}x_i x_j \quad (9.517c)$$

$$= 2m_{12}x_1x_2 + x_1f(x_2, \dots, x_{n+1}) + x_2g(x_3, \dots, x_{n+1}) + T(x_3, \dots, x_{n+1}) \quad (9.517d)$$

où f et g sont linéaires et T est multilinéaire.

À ce moment, nous tentons de factoriser toute la partie concernant x_1 et x_2 . L'idée est d'utiliser ceci :

$$(x_1 + g)(x_2 + f) = x_1x_2 + x_1f + x_2g + fg, \quad (9.518)$$

mais en mettant les bons coefficients pour reproduire ce que nous avons dans (9.517d) :

$$(2m_{12} + 2g)\left(x_1 + \frac{f}{m_{12}}\right) - \frac{2fg}{m_{12}} = 2m_{12}x_1x_2 + 2x_1f + 2x_2g. \quad (9.519)$$

Cela pour dire que

$$q(x) = 2(m_{12}x_1 + g)\left(x_2 + \frac{f}{m_{12}}\right) - \frac{2fg}{m_{12}} + T \quad (9.520)$$

où $-2fg/m_{12} + T$ est une forme quadratique de $x_3, \dots, x_{n+1}$, c'est à dire de $n - 1$ variables. L'hypothèse de récurrence nous donne des formes linéaires $(l_i)_{i=3, \dots, n+1}$ telles que

$$\frac{2fg}{m_{12}} + T = \sum_{i=3}^{n+1} \alpha_i l_i(x)^2. \quad (9.521)$$

Nous pouvons donc déjà écrire

$$q(x) = 2l'_1(x)l'_2(x) + \sum_{i=3}^{n+1} \alpha_i l_i(x)^2 \quad (9.522)$$

où

- Les forme l_i avec $i \geq 3$ ne dépendent pas de x_1 et x_2 , et sont donc indépendantes de l_1 et l_2 .
- La forme l'_1 ne dépend pas de x_2 ,
- La forme l'_2 ne dépend pas de x_1 .

Ce sont donc $n + 1$ formes linéaires indépendantes. Le seul problème résiduel est que les formes l'_1 et l'_2 arrivent en produit l'une de l'autre. Nous en définissons donc deux de plus :

$$\begin{aligned} l_1(x) &= \frac{1}{2}(l'_1 + l'_2) \\ l_2(x) &= \frac{1}{2}(l'_1 - l'_2), \end{aligned} \quad (9.523)$$

qui sont linéairement indépendantes l'une de l'autre et indépendantes des l_i ($i \geq 3$). Au final,

$$q(x) = l_1(x)^2 + l_2(x)^2 + \sum_{i=3}^{n+1} \alpha_i l_i(x)^2. \quad (9.524)$$

Si $m_{ii} = 0$ et $m_{12} = 0$ et $m_{kl} \neq 0$ avec $k < l$ Nous considérons la permutation

$$\sigma: \{1, \dots, n+1\} \rightarrow \{1, \dots, n+1\}$$

$$i \mapsto \begin{cases} 1 & \text{si } i = k \\ 2 & \text{si } i = l \\ k & \text{si } i = 1 \\ l & \text{si } i = 2 \\ i & \text{sinon,} \end{cases} \quad (9.525)$$

c'est à dire que σ permute 1 et k ainsi que 2 et l . Ensuite nous posons

$$s: \mathbb{R}^{n+1} \rightarrow \mathbb{R}^{n+1}$$

$$e_i \mapsto e_{\sigma(i)}. \quad (9.526)$$

Nous allons un peu considérer $q \circ s$, pour changer :

$$(q \circ s)(x) = \sum_{i,j} m_{ij} s(x)_i s(x)_j = \sum_{i,j} x_{\sigma(i)} x_{\sigma(j)}. \quad (9.527)$$

parce que $s(x)_i = x_{\sigma(i)}$.

Utilisons un petit abus de notation pour considérer

$$\sigma: \{1, \dots, n+1\} \times \{1, \dots, n+1\} \rightarrow \{1, \dots, n+1\} \times \{1, \dots, n+1\}$$

$$(i, j) \mapsto (\sigma(i), \sigma(j)). \quad (9.528)$$

Cela est une bijection ; nous pouvons utiliser le lemme 1.206 pour permuter les termes dans (9.527) :

$$(q \circ s)(x) = \sum_{i,j} m_{\sigma(i)\sigma(j)} x_{\sigma\sigma(i)} x_{\sigma\sigma(j)} \quad (9.529a)$$

$$= \sum_{i,j} a_{ij} x_i x_j \quad (9.529b)$$

où nous avons posé $a_{ij} = m_{\sigma(i)\sigma(j)}$ et utilisé le fait que $\sigma = \sigma^{-1}$. Le point intéressant de l'histoire est que dans (9.529b), $a_{12} = m_{kl} \neq 0$. La forme $q \circ s$ est donc dans le cas déjà traité et il existe des formes linéaires l'_i telles que

$$(q \circ s)(x) = \sum_{i=1}^{n+1} \alpha_i l'_i(x)^2. \quad (9.530)$$

En évaluant cela en $s(x)$, et en tenant compte de $s = s^{-1}$, nous trouvons

$$q(x) = \sum_i \alpha_i (l_i \circ s)(x)^2, \quad (9.531)$$

de telle sorte que $l_i = l'_i \circ s$ soit la réponse à notre théorème.

□

9.16.6 Orthogonalité

Proposition 9.238 ([223]).

Soient un espace vectoriel $(E, \mathbb{K})$ et une forme quadratique⁸⁸ q . Une base de E est q -orthogonale⁸⁹ si et seulement si la matrice de q dans cette base est diagonale.

⁸⁸. Définition 9.222.

⁸⁹. Définition 9.226.

Démonstration. La matrice de q est donnée par $Q_{ij} = b(e_i, e_j)$. Donc oui, cette matrice est diagonale si et seulement si les e_i sont orthogonaux. $\square$

Proposition 9.239.

Soit une forme quadratique q . Si une base (e_i) de E est q -orthogonale, alors $\mathcal{B} = \{e_i \text{ tel que } q(e_i) = 0\}$ est une base de $\ker(q)$.

Démonstration. Nous considérons un vecteur de base e_j , et nous montrons que $q(e_j) = 0$ si et seulement si $e_j \in \ker(q)$. Nous savons par la proposition 9.238 que la matrice de q dans la base (e_i) est diagonale et que les éléments diagonaux sont les $q(e_i)$. Soit $K = \{i \text{ tel que } q(e_i) = 0\}$.

$\text{Span}\{e_i\}_{i \in K} \subset \ker(q)$ Si $x = \sum_{i \in K} x_i e_i$, alors

$$q(x) = b(x, x) = \sum_{i, j \in K} |x_i|^2 b(e_i, e_j) = \sum_{i, j \in K} |x_i|^2 \delta_{ij} q(e_i) = 0 \quad (9.532)$$

parce que $q(e_i) = 0$ dès que $i \in K$.

$\ker(q) \subset \text{Span}\{e_i\}_{i \in K}$ Soit $x \in \ker(q)$ et écrivons-le sous la forme $x = \sum_{i=1}^n x_i e_i$. Nous avons

$$0 = q(x) = \sum_i |x_i|^2 q(e_i). \quad (9.533)$$

Mais $|x_i|^2 \geq 0$ et $q(e_i) \geq 0$, donc si $q(e_i) \neq 0$, alors $x_i = 0$. Donc les seules composantes non nulles de x sont celles sur lesquelles q s'annule. En d'autres termes $x = \sum_i x_i e_i \in \text{Span}\{e_i\}_{i \in K}$. $\square$

Théorème 9.240 ([223, 1]).

Toute forme quadratique sur un espace vectoriel de dimension finie admet une base formée de vecteurs 2 à 2 orthogonaux (pour la forme considérée).

Démonstration. Nous considérons la base $\{l_i\}$ de E^* donnée par la réduction de Gauss (théorème 9.237). La forme quadratique q s'écrit

$$q(x) = \sum_{i=1}^n \alpha_i l_i(x)^2. \quad (9.534)$$

La base préduale⁹⁰ $\{e_i\}$ de $\{l_i\}$ répond aux conditions. Pour le vérifier, nous considérons la forme bilinéaire associée à q par l'identité de polarisation 9.224 :

$$b(e_i, e_j) = \frac{1}{2}(q(e_i) + q(e_j) - q(e_i - e_j)). \quad (9.535)$$

Vu que $l_k(e_i) = \delta_{ki}$, nous avons

$$q(e_i) = \sum_{k=1}^n \alpha_k l_k(e_i)^2 = \alpha_i. \quad (9.536)$$

En utilisant la linéarité,

$$q(e_i - e_j) = \sum_k \alpha_k l_k(e_i - e_j)^2 \quad (9.537a)$$

$$= \sum_k \alpha_k (\delta_{ki} - \delta_{kj})^2 \quad (9.537b)$$

$$= \sum_k \alpha_k (\delta_{ki} + \delta_{kj} - 2\delta_{ki}\delta_{kj}) \quad (9.537c)$$

$$= \alpha_i + \alpha_j - 2\delta_{ij}\alpha_i. \quad (9.537d)$$

Donc

$$b(e_i, e_j) = \delta_{ij}\alpha_i. \quad (9.538)$$

Les vecteurs $\{e_i\}$ sont donc bien deux à deux q -orthogonaux. $\square$

⁹⁰. Définition, existence, unicité dans la proposition 4.129.

Notons qu'en l'absence de notion de racine carrée sur $\mathbb{K}$, il n'est pas possible de considérer $\sqrt{\alpha_i}$ et donc de base q -orthonormée.

9.16.7 Diagonalisation

Le théorème 9.240 a déjà donné une base orthogonale pour toute forme quadratique sur un espace vectoriel $(E, \mathbb{K})$ de dimension finie. Dans le cas de $\mathbb{R}^n$, nous pouvons en donner une preuve basée sur le théorème spectral, c'est la proposition 9.241.

Proposition 9.241.

Soit une forme bilinéaire symétrique b sur un $\mathbb{R}^n$. Il existe une matrice orthogonale Q telle que

(1) $D = Q^t b Q$ est diagonale

(2) $D(x, y) = b(Qx, Qy)$ pour tout $x, y \in E$.

Il existe une base $(f_i)_{i=1, \dots, n}$ qui est b -orthogonale.

Dans cet énoncé, nous mélangeons sans vergogne les formes et les matrices, en supposant qu'une base soit fixée⁹¹. Par exemple

$$D(x, y) = \sum_{ij} D_{ij} x_i y_j. \quad (9.539)$$

Démonstration. Pour la matrice diagonale, c'est le théorème spectral 9.146(2) qui joue parce que la matrice d'une forme bilinéaire symétrique est symétrique (c'est vu de la définition (9.498)).

Pour le reste c'est un calcul :

$$D(x, y) = \sum_{ijkl} Q_{ik}^t b_{kl} Q_{lj} x_i y_j \quad (9.540a)$$

$$= \sum_{ijkl} b_{kl} (Q_{ki} x_i) (Q_{lj} y_j) \quad (9.540b)$$

$$= \sum_{kl} b_{kl} (Qx)_k (Qy)_l \quad (9.540c)$$

$$= b(Qx, Qy). \quad (9.540d)$$

Nous avons utilisé le produit matrice fois vecteur donné par (4.79).

En ce qui concerne l'existence d'une base b -orthogonale, vu que D est diagonale, nous avons, pour $i \neq j$ que $D(e_i, e_j) = 0$. Donc en posant $f_i = Qe_i$, nous trouvons

$$0 = D(e_i, e_j) = b(Qe_i, Qe_j) = b(f_i, f_j). \quad (9.541)$$

La base $(Qe_i)_{i=1, \dots, n}$ est donc b -orthogonale. $\square$

9.16.8 Isométrie, forme quadratique et bilinéaire

Exemple 9.242.

La forme quadratique $q(x) = x_1^2 + x_2^2$ donne la norme euclidienne. La forme bilinéaire associée est $b(x, y) = x_1 y_1 + x_2 y_2$, qui est le produit scalaire usuel. $\triangle$

Il ne faudrait pas déduire trop vite que la formule $\|x\|^2 = q(x)$ donne une norme dès que q est non dégénérée. En effet q peut ne pas être définie positive. La forme $q(x) = x_1^2 - x_2^2$ prend des valeurs positives et négatives. A fortiori $d(x, y) = q(x - y)$ ne donne pas toujours une distance.

Définition 9.243.

Une **isométrie** pour la forme quadratique q est une application bijective $f: V \rightarrow V$ telle que

$$q(x - y) = q(f(x) - f(y)). \quad (9.542)$$

Dans les cas où q donne une distance, alors c'est une isométrie au sens usuel.

91. Autrement dit, si vous avez en tête d'utiliser cette proposition pour $\mathbb{R}^n$ c'est bon ; mais sinon vous devez choisir une base et considérer toutes les matrices dans cette base.

Définition 9.244 (Thème 69).

Soit un espace vectoriel E muni d'une forme bilinéaire b . Une **isométrie** pour b est une bijection $f: E \rightarrow E$ telle que

$$b(f(x), f(y)) = b(x, y) \quad (9.543)$$

pour tout $x, y \in E$.

Lemme 9.245.

Soient q une forme quadratique et b la forme bilinéaire associée par le lemme 9.225. Une application $f: E \rightarrow E$ telle que $f(0) = 0$ est une isométrie pour b si et seulement si elle est une isométrie pour q .

Démonstration. Pour une application bijective $f: E \rightarrow E$ telle que $f(0) = 0$, nous devons prouver l'équivalence des propriétés suivantes :

- (1) $b(f(x), f(y)) = b(x, y)$ pour tout $x, y \in E$;
- (2) $q(f(x) - f(y)) = q(x - y)$ pour tout $x, y \in E$.

Dans le sens direct, en posant $x = y$ nous trouvons tout de suite $q(f(x)) = q(x)$; ensuite en utilisant la distributivité de b ,

$$q(f(x) - f(y)) = b(f(x) - f(y), f(x) - f(y)) \quad (9.544a)$$

$$= q(f(x)) - 2b(f(x), f(y)) + q(f(y)) \quad (9.544b)$$

$$= q(x) + q(y) - 2b(x, y) \quad (9.544c)$$

$$= q(x - y). \quad (9.544d)$$

Dans l'autre sens, nous commençons par remarquer que l'hypothèse $f(0) = 0$ donne $q(x) = q(f(x))$. Ensuite nous utilisons l'identité de polarisation (9.496) :

$$b(f(x), f(y)) = \frac{1}{2}[q(f(x)) + q(f(y)) - q(f(x - y))] \quad (9.545a)$$

$$= \frac{1}{2}[q(x) + q(y) - q(x - y)] \quad (9.545b)$$

$$= b(x, y). \quad (9.545c)$$

□

9.16.9 Isométries

Voici un théorème pas toujours bien énoncé dans les cours de physique qui font de la relativité. Au moment de « prouver » les transformations de Lorentz⁹², beaucoup oublient de justifier pourquoi elles devraient être linéaires.

Théorème 9.246 ([224]).

Une isométrie⁹³ d'une forme bilinéaire non dégénérée est linéaire.

Démonstration. Soient une forme bilinéaire non-dégénérée b sur l'espace vectoriel E ainsi qu'une isométrie f pour icelle. Soit $z \in E$; étant donné que f est bijective nous pouvons considérer l'élément $f^{-1}(z) \in E$ et calculer

$$b(f(x + y), z) = b(f(x + y), f(f^{-1}(z))) \quad (9.546a)$$

$$= b(x + y, f^{-1}(z)) \quad (9.546b)$$

$$= b(x, f^{-1}(z)) + b(y, f^{-1}(z)) \quad (9.546c)$$

$$= b(f(x), z) + b(f(y), z) \quad (9.546d)$$

$$= b(f(x) + f(y), z), \quad (9.546e)$$

92. Théorème 18.174.

93. Définition 9.244.

donc $f(x + y) = f(x) + f(y)$ par le lemme 9.217.

De la même façon on trouve $b(f(\lambda x), z) = b(\lambda f(x), z)$ qui prouve que $f(\lambda x) = \lambda f(x)$ et donc que f est linéaire. $\square$

Exemple 9.247.

Une isométrie peut ne pas être linéaire quand la forme bilinéaire est dégénérée. Par exemple pour la forme bilinéaire sur $\mathbb{R}^2$ donnée par

$$b((a, b), (x, y)) = ax, \quad (9.547)$$

nous pouvons faire

$$f(x, y) = \begin{pmatrix} x \\ \lambda(x, y) \end{pmatrix} \quad (9.548)$$

où λ est n'importe quoi. $\triangle$

Théorème 9.248.

Soit un espace vectoriel E muni d'une forme quadratique q . Soit une isométrie $f: E \rightarrow E$ pour q . Alors

- (1) si $f(0) = 0$, alors f est linéaire ;
- (2) si $f(0) \neq 0$ alors f est affine⁹⁴.

Démonstration. Nous considérons la forme bilinéaire associée b . Si $f(0) = 0$, nous savons par le lemme 9.245 que $b(f(x), f(y)) = b(x, y)$. La proposition 9.246 nous dit alors que f est linéaire.

Si $f(0) \neq 0$, alors nous posons $g(x) = f(x) - f(0)$ qui vérifie $g(0) = 0$ et

$$q(g(x) - g(y)) = q(f(x) - f(0) - f(y) + f(0)) = q(x - y). \quad (9.549)$$

Nous pouvons donc appliquer le premier point à g , déduire que g est linéaire et donc que f est affine. C'est la caractérisation du lemme 8.54 des fonctions affines. $\square$

Nous pouvons maintenant particulariser tout cela au cas de $\mathbb{R}^n$ muni du produit scalaire usuel et de la norme associée pour voir quel résultat nous avons à peine prouvé.

Lemme 9.249 ([225]).

Une isométrie d'un espace vectoriel normé de dimension finie est bijective.

Démonstration. Si $f: E \rightarrow E$ est une isométrie, elle est linéaire par le théorème 9.246. Elle vérifie également $\|f(x)\| = \|x\|$, et donc $f(x) = 0$ si et seulement si $x = 0$, c'est-à-dire que f est injective. Elle est alors bijective par le corolaire 4.44 du théorème du rang. $\square$

Nous notons ici $T(n)$ le groupe des translations sur $\mathbb{R}^n$. Un élément de $T(n)$ est une translation τ_v donnée par un vecteur v et agissant sur $\mathbb{R}^n$ par

$$\begin{aligned} \tau_v: \mathbb{R}^n &\rightarrow \mathbb{R}^n \\ x &\mapsto x + v. \end{aligned} \quad (9.550)$$

Ce groupe est isomorphe au groupe abélien $(\mathbb{R}^n, +)$, et nous allons souvent identifier τ_v à v .

Vous savez par culture générale que les isométries de $\mathbb{R}^n$ pour le produit scalaire usuel sont les matrices orthogonales. En voici une petite généralisation (pensez à $\eta = \mathbb{1}$ dans le cas du produit scalaire usuel).

Proposition 9.250.

Soit une forme bilinéaire b sur $\mathbb{R}^n$ de matrice symétrique η . Si A est la matrice d'une application linéaire $\mathbb{R}^n \rightarrow \mathbb{R}^n$ telle que

$$b(Ax, Ay) = b(x, y) \quad (9.551)$$

pour tout $x, y \in \mathbb{R}^n$, alors

$$A^t \eta A = \eta. \quad (9.552)$$

94. Définition 8.9.

Démonstration. En suivant la formule générale (9.499),

$$b(Ax, Ay) = \sum_{ij} \eta_{ij} (Ax)_i (Ay)_j = \sum_{ijkl} \eta_{ij} A_{ik} A_{jl} x_k y_l. \quad (9.553)$$

En imposant que ce soit égal à $\sum_{kl} \eta_{kl} x_k y_l$ pour tout x, y nous avons la contrainte

$$\sum_{ij} \eta_{ij} A_{ik} A_{jl} = \eta_{kl} \quad (9.554)$$

qui signifie exactement $A^t \eta A = \eta$. □

9.17 Signature, théorème de Sylvester

Définition 9.251 (Signature^[226]).

Soit une forme quadratique⁹⁵ Q sur un espace vectoriel E de dimension finie n . L'**indice d'inertie** de Q est le nombre

$$q = \max\{\dim(F) \text{ tel que } Q(v) < 0 \forall v \in F \setminus \{0\}\}. \quad (9.555)$$

Nous définissons aussi

$$p = \max\{\dim(G) \text{ tel que } Q(v) > 0 \forall v \in G \setminus \{0\}\}. \quad (9.556)$$

Le couple (p, q) est la **signature** de Q .

Définition 9.252 (Rang d'une forme quadratique).

Si $Q: E \times E \rightarrow \mathbb{K}$ est une forme quadratique, nous considérons l'application

$$\begin{aligned} f_Q: E &\rightarrow E^* \\ x &\mapsto [y \mapsto B(x, y)]. \end{aligned} \quad (9.557)$$

Le **rang** de Q est le rang de l'application linéaire f_Q .

Proposition 9.253.

Le rang d'une forme quadratique est le rang de sa matrice dans n'importe quelle base.

Démonstration. Nous considérons une forme quadratique Q sur l'espace vectoriel E . Sa trace est, par définition, la trace de l'application linéaire f_Q de la définition 9.252. Or cette dernière trace ne dépend pas des bases choisies sur E et E^* . Nous la calculons donc maintenant.

Soit une base $\{e_i\}$ de E ainsi que sa base duale $\{e_i^*\}$ de E^* . Si $v = \sum_k v_k e_k \in E$, alors

$$f_Q(e_i)v = \sum_k v_k B(e_i, e_k) = \sum_k Q_{ik} v_k \quad (9.558)$$

où nous avons noté B la forme bilinéaire associée à Q et utilisé la définition 9.227 de la matrice associée à la forme quadratique Q . Nous avons donc $f_Q(e_i) = \sum_k Q_{ik} e_k^*$ ou encore

$$f_Q(e_i)_k = Q_{ik}, \quad (9.559)$$

ce qui signifie, par (1) que la matrice associée à f_Q est la matrice Q^t .

Le rang de f_Q est donc celui de Q^t , qui est le même que celui de la matrice Q (ici, nous avons noté Q la matrice de la forme quadratique Q). Le rang de f_Q est celui de sa matrice par la proposition 4.105. □

95. Définition 9.222.

Lemme 9.254 ([226]).

Soient une forme quadratique Q ainsi que deux bases Q -orthogonales $\{e_1, \dots, e_n\}$ et $\{e'_1, \dots, e'_n\}$. Nous posons

$$r = \text{Card}\{e_i \text{ tel que } q(e_i) > 0\} \quad (9.560a)$$

$$r' = \text{Card}\{e_i \text{ tel que } q(e'_i) > 0\} \quad (9.560b)$$

$$s = \text{Card}\{e_i \text{ tel que } q(e_i) < 0\} \quad (9.560c)$$

$$s' = \text{Card}\{e_i \text{ tel que } q(e'_i) < 0\} \quad (9.560d)$$

Alors $r = r'$ et $s = s'$.

Démonstration. Nous posons

$$I = \{i \text{ tel que } Q(e_i) > 0\} \quad (9.561a)$$

$$J = \{j \text{ tel que } Q(e_j) < 0\} \quad (9.561b)$$

Nous commençons par prouver que $\{e_i\}_{i \in I} \cup \{e'_j\}_{j \in J}$ est libre. Supposons pour cela que

$$\sum_{i \in I} x_i e_i + \sum_{j \in J} y_j e'_j = 0, \quad (9.562)$$

et posons $z = \sum_{i \in I} x_i e_i$. Nous avons

$$Q(z) = \sum_{i \in I} x_i^2 Q(e_i) \geq 0. \quad (9.563)$$

Mais nous avons aussi $z = -\sum_{j \in J} y_j e'_j$, donc

$$Q(z) = \sum_{j \in J} y_j^2 Q(e'_j) \leq 0. \quad (9.564)$$

Donc $Q(z) = 0$. Vu (9.563), et le fait que $Q(e_i) > 0$, avoir $Q(z) = 0$ impose $x_i = 0$ pour tout i . La relation (9.564) nous donne aussi immédiatement que les y_j sont nuls. Donc la partie $\{e_i\}_{i \in I} \cup \{e'_j\}_{j \in J}$ est libre.

Le lemme 4.9 nous indique qu'une partie libre est toujours de cardinal plus petit ou égal à la dimension de l'espace⁹⁶. Tout ça pour dire que

$$\underbrace{\text{Card}(I)}_{=r} + \underbrace{\text{Card}(J)}_{=n-r'} \leq n, \quad (9.565)$$

et donc $r \leq r'$.

Le même raisonnement, en partant de $I = \{i \text{ tel que } Q(e_i) \leq 0\}$ et de $J = \{j \text{ tel que } Q(e'_j) > 0\}$, prouve que $r' \leq r$.

La preuve de $s = s'$ est du même tonneau. $\square$

Lemme 9.255 ([227]).

Soit une forme quadratique Q sur E . Si F est un sous-espace de E , alors

$$\dim(F) + \dim(F^\perp) \geq n \quad (9.566)$$

où $F^\perp$ est l'orthogonal par rapport à Q .

Démonstration. Nous posons $p = \dim(F)$. Nous considérons une base $\{f_i\}_{i=1, \dots, n}$ de E telle que $\{f_i\}_{i=1, \dots, p}$ est une base de F ⁹⁷. Nous posons

$$\begin{aligned} \phi: E &\rightarrow F \\ x &\mapsto \sum_{i=1}^p B(x, f_i) f_i \end{aligned} \quad (9.567)$$

96. Ici nous utilisons l'hypothèse que V est de dimension finie.

97. Théorème de la base incomplète, 4.22.

où B est la forme bilinéaire associée à Q . Ce ϕ est une application linéaire à qui nous appliquons le théorème du rang (4.47) :

$$\dim(E) = \text{rang}(\phi) + \dim(\ker(\phi)). \quad (9.568)$$

Mais vu que l'image de ϕ est dans F , nous avons $\text{rang}(\phi) \leq \dim(F)$. De plus, $\ker(\phi) = F^\perp$. Donc (9.568) devient

$$\dim(E) \leq \dim(F) + \dim(F^\perp). \quad (9.569)$$

□

Lemme 9.256 ([227]).

Soit un espace vectoriel E de dimension finie et un sous-espace F sur lequel la forme quadratique Q est strictement définie positive ou négative. Alors

$$E = F \oplus F^\perp. \quad (9.570)$$

Démonstration. D'abord nous montrons que $F \cap F^\perp = \{0\}$. Si $v \neq 0$ est dans F , alors $Q(v) > 0$, et donc v n'est pas dans $F^\perp$. Donc $F \cap F^\perp \subset \{0\}$. L'inclusion inverse est immédiate.

Nous avons vu dans le lemme 9.255 que

$$\dim(E) \leq \dim(F) + \dim(F^\perp). \quad (9.571)$$

Vu que F et $F^\perp$ n'ont pas d'intersection autre que $\{0\}$, nous avons

$$\dim(E) \geq \dim(F \oplus F^\perp) = \dim(F) + \dim(F^\perp) \geq \dim(E). \quad (9.572)$$

Toutes ces inégalités sont donc des égalités et $\dim(E) = \dim(F) + \dim(F^\perp)$. □

Théorème 9.257 (de Sylvester[226]).

Soit Q une forme quadratique réelle de signature⁹⁸ (p, q) . Alors pour toute base Q -orthogonale $\{e_i\}$ de $\mathbb{R}^{p+q}$ nous avons les propriétés suivantes.

(1) Les nombres p et q sont donnée par

$$p = \text{Card}\{i \text{ tel que } Q(e_i) > 0\} \quad (9.573a)$$

$$q = \text{Card}\{i \text{ tel que } Q(e_i) < 0\}. \quad (9.573b)$$

(2) Si A est la matrice de Q dans une base, alors il existe une matrice inversible P telle que

$$P^t A P = \begin{pmatrix} -\mathbb{1}_q & & \\ & \mathbb{1}_p & \\ & & 0 \end{pmatrix}. \quad (9.574)$$

(3) Le rang de Q est $p + q$.

Démonstration. Soit F un sous-espace de dimension maximale q sur lequel Q est définie négative. Le fait que la dimension de F soit q est la définition 9.251 de la signature. Nous notons $F^\perp$ sont Q -orthogonal, c'est à dire que

$$F^\perp = \{v \in E \text{ tel que } B(v, x) = 0 \forall x \in F\}. \quad (9.575)$$

Le lemme 9.256 nous assure que $E = F \oplus F^\perp$.

Le théorème 9.240 sur l'existence de bases Q -orthogonales nous permet de considérer une base Q -orthogonale de F et une de $F^\perp$. En réunissant les deux, nous avons une base de E . Nous la notons $\{f_1, \dots, f_n\}$ avec

— La partie $\{f_1, \dots, f_q\}$ est une base de F ,

98. Définition 9.251.

- La partie $\{f_{q+1}, \dots, f_n\}$ est une base de $F^\perp$,
- Remarquez cependant qu'il n'est pas dit que $n = q + p$.

Notons que pour $i > q$, nous avons $Q(f_i) \geq 0$, sinon la maximalité de F serait contredite par $\text{Span}\{f_1, \dots, f_q, f_i\}$.

Cela prouve que

$$\text{Card}\{i \text{ tel que } Q(f_i) > 0\} = p. \quad (9.576)$$

Le lemme 9.254 nous dit alors que

$$\text{Card}\{i \text{ tel que } Q(e_i) > 0\} = \text{Card}\{i \text{ tel que } Q(f_i) > 0\} = p. \quad (9.577)$$

C'est l'égalité (9.573b). L'égalité (9.573a) se prouve de la même façon, en prenant F maximal pour la propriété que Q y est strictement définie positive.

Le point (1) est prouvé.

Dans une base Q -orthogonale, la matrice de Q est diagonale, et contient sur la diagonale les valeurs de $Q(e_i)$. Parmi celles-ci, on en a p strictement positives et q strictement négatives. Les $n - p - q$ autres sont nulles. Vu que Q est à valeur réelle, nous avons une notion de racine carré, et nous pouvons considérer $e_i/\sqrt{|Q(e_i)|}$ au lieu de e_i . De cette façon, $Q(e_i)$ est normalisé. Avec ça, la matrice de Q est

$$D = \begin{pmatrix} \mathbb{1}_p & & \\ & -\mathbb{1}_q & \\ & & 0 \end{pmatrix}. \quad (9.578)$$

Nous venons de prouver qu'il existe une base $\{e_i\}$ dans laquelle la matrice de Q est (9.578). Si A est la matrice de Q dans une base quelconque $\{f_i\}$ et si P est la matrice de changement de base $f_j = \sum_i P_{ij}e_i$, la proposition 9.233 donne $D = P^t A P$.

Le point (2) est prouvé.

Pour (3), la proposition 9.253 nous permet de calculer le rang de Q par le rang de sa matrice dans n'importe quelle base. Nous choisissons la base qui donne la matrice (9.578). Le rang est alors bien $p + q$. $\square$

Définition 9.258 (Équivalence de forme quadratique[221]).

Deux formes quadratiques Q et Q' sont **équivalentes** si il existe une application linéaire inversible ϕ telle que $Q' = Q \circ \phi$.

Proposition 9.259 ([226]).

Deux formes quadratiques sont équivalentes⁹⁹ si et seulement si elles ont même signature.

9.17.1 Invariance de la trace

Proposition 9.260 ([1]).

Soit une application linéaire f . Si la matrice de f dans une base est A et est B dans une autre base, alors

$$\text{Tr}(A) = \text{Tr}(B). \quad (9.579)$$

Démonstration. Les matrices A et B sont liées par la proposition 4.114 : $B = Q^{-1} A Q$ où Q est la matrice qui lie les vecteurs des deux bases. L'invariance cyclique de la trace donnée en le lemme 4.60 implique que

$$\text{Tr}(B) = \text{Tr}(Q^{-1} A Q) = \text{Tr}(Q Q^{-1} A) = \text{Tr}(A). \quad (9.580)$$

$\square$

99. Définition 9.258.

9.18 Produit scalaire, produit hermitien

Définition 9.261.

Un **produit scalaire** sur un espace vectoriel réel est une forme bilinéaire¹⁰⁰ symétrique strictement définie positive¹⁰¹.

La définition suivante est utile pour celles qui veulent faire de la relativité¹⁰².

Définition 9.262.

Un **produit pseudo-scalaire** sur un espace vectoriel réel est une forme bilinéaire et symétrique.

Vu que nous allons voir un pâté d'espaces avec des produits scalaires, nous leur donnons un nom.

Définition 9.263.

Un espace vectoriel **euclidien** est un espace vectoriel de dimension finie muni d'un produit scalaire (définition 9.261).

Avouez que c'est drôle qu'un espace vectoriel est euclidien lorsqu'il possède une *multiplication* alors qu'un anneau est euclidien lorsqu'il possède une *division* (voir la définition 3.100). C'est pas très profond, mais si ça peut vous servir de moyen mnémotechnique...

Définition 9.264 ([228]).

Soit E est un espace vectoriel sur $\mathbb{C}$. Une application $\langle \cdot, \cdot \rangle: E \times E \rightarrow \mathbb{C}$ est **sesquilinéaire à droite** si pour tout $x, y \in E$ et pour tout $\lambda \in \mathbb{C}$,

$$(1) \langle \lambda x, y \rangle = \lambda \langle x, y \rangle = \langle x, \bar{\lambda} y \rangle,$$

$$(2) \langle x + y, z \rangle = \langle x, z \rangle + \langle y, z \rangle,$$

$$(3) \langle x, y + z \rangle = \langle x, y \rangle + \langle x, z \rangle.$$

Cette forme est **hermitienne** si de plus

$$\langle x, y \rangle = \overline{\langle y, x \rangle}. \quad (9.581)$$

Un **produit hermitien** est une forme hermitienne strictement définie positive, c'est-à-dire telle que $\langle x, x \rangle \geq 0$ pour tout $x \in E$ et $\langle x, x \rangle = 0$ si et seulement si $x = 0$.

Exemple 9.265.

L'ensemble $E = \mathbb{C}^n$ vu comme espace vectoriel de dimension n sur $\mathbb{C}$ est muni d'une forme sesquilinéaire

$$\langle x, y \rangle = \sum_{k=1}^n x_k \bar{y}_k \quad (9.582)$$

pour tout $x, y \in \mathbb{C}^n$. Cela est un espace vectoriel hermitien. $\triangle$

La proposition suivante est une version plus « pragmatique » de la proposition 4.131.

Proposition 9.266 ([111]).

Soient un espace euclidien¹⁰³ de dimension finie V ainsi qu'un sous-espace M . Nous posons

$$M^\perp = \{x \in V \text{ tel que } x \cdot y = 0 \forall y \in M\}. \quad (9.583)$$

Alors $M \oplus M^\perp = V$.

100. Définition 9.213.

101. Définition 9.223.

102. Voir le théorème 18.174 qui établit les transformations de Lorentz.

103. Qui possède un produit scalaire, définition 9.263.

Démonstration. D'abord si $x \in M \cap M^\perp$, alors $x \cdot x = 0$ et donc $x = 0$. Donc nous avons déjà $M \cap M^\perp = \{0\}$. Nous considérons une base $\{b_1, \dots, b_k\}$ de M , et nous définissons l'application linéaire

$$\begin{aligned} f: V &\rightarrow \mathbb{R}^k \\ x &\mapsto (x \cdot b_1, \dots, x \cdot b_k). \end{aligned} \quad (9.584)$$

Nous avons que $M^\perp = \ker(f)$. Le théorème du rang 4.42 nous indique que

$$\dim(V) = \dim(\ker(f)) + \dim(\text{Image}(f)) \leq \dim(M^\perp) + k = \dim(M^\perp) + \dim(M). \quad (9.585)$$

Une justification : vu que f prend ses valeurs dans $\mathbb{R}^k$, la dimension de son image est majorée par k .

Nous en déduisons que

$$\dim(M) + \dim(M^\perp) \geq \dim(V), \quad (9.586)$$

et la proposition 4.151 nous permet de conclure que $M \oplus M^\perp = V$. $\square$

9.18.1 Ellipsoïde

Lemme 9.267.

Toute matrice peut être décomposée de façon unique en une partie symétrique et une partie antisymétrique. Cette décomposition est donnée par

$$S = \frac{M + M^t}{2}, \quad A = \frac{M - M^t}{2} \quad (9.587)$$

Démonstration. L'existence est une vérification immédiate de $S + A = M$ en utilisant (9.587). Pour l'unicité, si $S + A = S' + A'$ alors $S - S' = A - A'$. Mais $S - S'$ est symétrique et $A - A'$ est antisymétrique ; l'égalité implique l'annulation des deux membres, c'est-à-dire $S = S'$ et $A = A'$. $\square$

Définition 9.268.

Un **ellipsoïde** dans $\mathbb{R}^n$ centré en v est le lieu des points x vérifiant l'équation

$$\langle x - v, M(x - v) \rangle = 1 \quad (9.588)$$

où M est une matrice symétrique strictement définie positive¹⁰⁴.

Lorsque nous parlons d'ellipsoïde plein, il suffit de changer l'égalité en une inégalité.

Remarque 9.269.

Le fait que M soit symétrique n'est pas tout à fait obligatoire ; la chose importante est que toutes les valeurs propres soient strictement positives. En effet si M a toutes ses valeurs propres strictement positives, nous nommons S la partie symétrique de M et A la partie antisymétrique (lemme 9.267). Alors pour tout $x \in \mathbb{R}^n$ nous avons

$$x^t A x = \langle x, A x \rangle = \langle A^t x, x \rangle = -\langle A x, x \rangle = -\langle x, A x \rangle, \quad (9.589)$$

donc $x^t A x = 0$. L'équation $x^t M x = 1$ est donc équivalente à $x^t S x = 1$ (elles ont les mêmes solutions).

De plus S reste strictement définie positive parce que pour tout $x \in \mathbb{R}^n$ nous avons

$$0 < x^t M x = x^t S x. \quad (9.590)$$

Proposition 9.270.

Si $\mathcal{E}$ est un ellipsoïde centrée à l'origine, il existe une base de $\mathbb{R}^n$ dans laquelle son équation est :

$$\sum_{i=1}^n \frac{x_i^2}{a_i^2} = 1. \quad (9.591)$$

104. Définition 9.148.

Démonstration. Nous avons une matrice symétrique strictement définie positive S telle que l'équation soit $\langle x, Sx \rangle = 1$. Le théorème spectral 9.146 nous fournit une base orthonormale $\{e_i\}$ dans laquelle $Se_i = \lambda_i e_i$ avec $\lambda_i > 0$. En substituant dans l'équation $\langle x, Sx \rangle = 1$ nous trouvons l'équation

$$\sum_i \lambda_i x_i^2 = 1. \quad (9.592)$$

En posant $a_i = \frac{1}{\sqrt{\lambda_i}}$, nous trouvons le résultat. Cette définition des a_i est toujours possible parce que $\lambda_i > 0$. $\square$

Corolaire 9.271.

Un ellipsoïde plein centré en l'origine admet une équation de la forme $q(x) \leq 1$ où q est une forme quadratique strictement définie positive.

Pour rappel de notation, l'ensemble des formes quadratiques strictement définies positives sur l'espace vectoriel E est noté $Q^{++}(E)$.

Démonstration. Soit $\{e_i\}$ une base de $\mathbb{R}^n$ telle que l'ellipsoïde $\mathcal{E}$ ait pour équation

$$\sum_{i=1}^n \frac{x_i^2}{a_i^2} \leq 1. \quad (9.593)$$

Nous considérons la forme quadratique

$$\begin{aligned} q: \mathbb{R}^n &\rightarrow \mathbb{R} \\ x &\mapsto \sum_{i=1}^n \frac{\langle x, e_i \rangle^2}{a_i^2}. \end{aligned} \quad (9.594)$$

Nous avons évidemment $\mathcal{E} = \{x \in \mathbb{R}^n \text{ tel que } q(x) \leq 1\}$. De plus la forme q est strictement définie positive parce que dès que $x \neq 0$, au moins un des produits scalaires $\langle x, e_i \rangle$ est non nul et $q(x) > 0$. $\square$

9.19 Système d'équations linéaires : méthode de Gauss

Pour résoudre un système d'équations linéaires, on procède comme suit :

(1) Écrire le système sous forme matricielle.

$$\text{p.ex. } \begin{cases} 2x + 3y = 5 \\ x + 2y = 4 \end{cases} \Leftrightarrow \left(\begin{array}{cc|c} 2 & 3 & 5 \\ 1 & 2 & 4 \end{array} \right)$$

(2) Se ramener à une matrice avec un maximum de 0 dans la partie de gauche en utilisant les transformations admissibles :

(2a) Remplacer une ligne par elle-même + un multiple d'une autre ;

$$\text{p.ex. } \left(\begin{array}{cc|c} 2 & 3 & 5 \\ 1 & 2 & 4 \end{array} \right) \xrightarrow{L_1 - 2L_2 \rightarrow L'_1} \left(\begin{array}{cc|c} 0 & -1 & -3 \\ 1 & 2 & 4 \end{array} \right)$$

(2b) Remplacer une ligne par un multiple d'elle-même ;

$$\text{p.ex. } \left(\begin{array}{cc|c} 0 & -1 & -3 \\ 1 & 2 & 4 \end{array} \right) \xrightarrow{-L_1 \rightarrow L'_1} \left(\begin{array}{cc|c} 0 & 1 & 3 \\ 1 & 2 & 4 \end{array} \right)$$

(2c) Permuter des lignes.

$$\text{p.ex. } \left(\begin{array}{cc|c} 0 & 1 & 3 \\ 1 & 0 & -2 \end{array} \right) \xrightarrow{L_1 \leftrightarrow L'_2 \text{ et } L_2 \leftrightarrow L'_1} \left(\begin{array}{cc|c} 1 & 0 & -2 \\ 0 & 1 & 3 \end{array} \right)$$

(3) Retransformer la matrice obtenue en système d'équations.

$$\text{p.ex. } \left(\begin{array}{cc|c} 1 & 0 & -2 \\ 0 & 1 & 3 \end{array} \right) \Leftrightarrow \begin{cases} x &= -2 \\ y &= 3 \end{cases}$$

Remarque 9.272. — Si on obtient une ligne de zéros, on peut l'enlever :

$$\text{p.ex. } \left(\begin{array}{ccc|c} 3 & 4 & -2 & 2 \\ 4 & -1 & 3 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right) \Leftrightarrow \left(\begin{array}{ccc|c} 3 & 4 & -2 & 2 \\ 4 & -1 & 3 & 0 \end{array} \right)$$

— Si on obtient une ligne de zéros suivie d'un nombre non-nul, le système d'équations n'a pas de solution :

$$\text{p.ex. } \left(\begin{array}{ccc|c} 3 & 4 & -2 & 2 \\ 4 & -1 & 3 & 0 \\ 0 & 0 & 0 & 7 \end{array} \right) \Leftrightarrow \begin{cases} \dots \\ \dots \\ 0x + 0y + 0z = 7 \end{cases} \Rightarrow \textbf{Impossible}$$

— Si on a moins d'équations que d'inconnues, alors il y a une infinité de solutions qui dépendent d'un ou plusieurs paramètres :

$$\text{p.ex. } \left(\begin{array}{ccc|c} 1 & 0 & -2 & 2 \\ 0 & 1 & 3 & 0 \end{array} \right) \Leftrightarrow \begin{cases} x - 2z = 2 \\ y + 3z = 0 \end{cases} \Leftrightarrow \begin{cases} x = 2 + 2\lambda \\ y = -3\lambda \\ z = \lambda \end{cases}$$

Chapitre 10

Analyse réelle : topologie et continuité

10.1 Intervalles

Définition 10.1 (Intervalle).

Une partie I de $\mathbb{R}$ est un **intervalle** si pour tout $a, b \in I$ nous avons $t \in I$ dès que $a \leq t \leq b$.

Un intervalle est **ouvert** s'il est de la forme $]a, b[$ avec éventuellement $a = -\infty$ ou $b = +\infty$.
Un intervalle est **fermé** s'il est de la forme $[a, b]$ ou $]-\infty, b]$ ou $[a, +\infty[$ avec $a, b \in \mathbb{R}$.

Remarque 10.2.

L'ensemble $\mathbb{R}$ ne contient pas $-\infty$ et $+\infty$. L'intervalle $[-\infty, 5]$ par exemple, n'est pas une partie de $\mathbb{R}$.

Exemple 10.3. (1) Les ensembles $]3, 7[$ et $]-\infty, \pi[$ sont des intervalles ouverts.

(2) Les ensembles $[10, 15]$ et $[-1, +\infty[$ sont des intervalles fermés.

(3) L'ensemble $] -4, -2[\cup]2, 9[$ n'est pas un intervalle (il y a un « trou » entre -2 et 2).

(4) L'ensemble $\mathbb{R}$ lui-même est un intervalle ; par convention, il est à la fois ouvert et fermé.

Un intervalle peut n'être ni ouvert ni fermé ; par exemple $]4, 8]$. Cet intervalle est « ouvert en 4 et fermé en 8 » . $\triangle$

Définition 10.4 (Fonction, domaine, image, graphe).

Soient X et Y deux ensembles. Une **fonction** f définie sur X et à valeurs dans Y est une correspondance qui associe à chaque élément x dans X **au plus** un élément y dans Y . On écrit $y = f(x)$.

- La partie de X qui contient tous les x sur lesquels f peut opérer est dite **domaine** de f . Le domaine de f est indiqué par $\text{Domaine } f$.
- L'élément de $y \in Y$ associé par f à un élément $x \in \text{Domaine } f$ (c'est-à-dire $f(x) = y$) est appelé **image** de x par f . L'**image** de la fonction f est la partie de Y qui contient les images de tous les éléments de $\text{Domaine } f$. L'image de f est indiquée par $\Im f$.
- Le **graphe** de f est l'ensemble de toutes les couples $(x, f(x))$ pour $x \in \text{Domaine } f$. Le graphe de f est une partie de l'ensemble noté $X \times Y$ et il est indiqué par $\text{Graph } f$. Dans ce cours $X = \mathbb{R}$ et $Y = \mathbb{R}$, donc le graphe de f est contenu dans le plan cartésien.

Définition 10.5 (Fonction croissante, décroissante et monotone).

Soit $f: \mathbb{R} \rightarrow \mathbb{R}$ une fonction définie sur un intervalle $I \subset \mathbb{R}$.

- (1) La fonction f est **croissante** sur I si pour tout $x < y$ dans I nous avons $f(x) \leq f(y)$. Elle est strictement croissante si $f(x) < f(y)$ dès que $x < y$.
- (2) La fonction f est **décroissante** sur I si pour tout $x < y$ dans I nous avons $f(x) \geq f(y)$. Elle est strictement décroissante si $f(x) > f(y)$ dès que $x < y$.

(3) La fonction f est dite **monotone** sur I si elle est soit croissante soit décroissante sur I .

Exemple 10.6.

La fonction $x \mapsto x^2$ est décroissante sur l'intervalle $]-\infty, 0]$ et croissante sur l'intervalle $[0, \infty[$. Elle n'est par contre ni croissante ni décroissante sur l'intervalle $[-4, 3]$. $\triangle$

10.2 Application réciproque

10.2.1 Définitions

Les définitions d'injection, surjection, bijection et d'application réciproque sont les définitions 7.86 et 7.87.

Exemple 10.7. (1) La fonction $x \mapsto x^2$ n'est pas une bijection de $\mathbb{R}$ vers $\mathbb{R}$ parce qu'il n'existe aucun x tel que $x^2 = -1$.

(2) La fonction

$$\begin{aligned} f: [0, +\infty[&\rightarrow [0, +\infty[\\ x &\mapsto x^2 \end{aligned} \tag{10.1}$$

est une bijection. Notez que c'est la même fonction que celle de l'exemple précédent. Seul l'intervalle sur laquelle nous nous plaçons a changé.

(3) La fonction

$$\begin{aligned} f: \mathbb{R} &\rightarrow [0, \infty[\\ x &\mapsto x^2 \end{aligned} \tag{10.2}$$

n'est pas une bijection parce qu'il existe plusieurs x pour lesquels $f(x) = 4$.

(4) Nous verrons un peu plus tard (12.343) que l'application

$$\begin{aligned} f: [0, \infty[&\rightarrow [0, \infty[\\ x &\mapsto x^2 \end{aligned} \tag{10.3}$$

est une bijection.

En conclusion : il est très important de préciser les domaines des fonctions considérées. $\triangle$

Remarque 10.8.

Dire que la fonction $f: I \rightarrow J$ est bijective, c'est dire que l'équation $f(x) = y$ d'inconnue x peut être résolue de façon univoque pour tout $y \in J$.

Remarque 10.9.

Toute fonction strictement monotone sur un intervalle I est injective.

Exemple 10.10.

Trouvons la fonction réciproque de la fonction affine $f: \mathbb{R} \rightarrow \mathbb{R}$, $x \mapsto 3x - 2$. Si $y \in \mathbb{R}$ le nombre $f^{-1}(y)$ est la valeur de x pour laquelle $f(x) = y$. Il s'agit donc de résoudre

$$3x - 2 = y \tag{10.4}$$

par rapport à x . La solution est $x = \frac{y+2}{3}$ et donc nous écrivons

$$f^{-1}(y) = \frac{y+2}{3}. \tag{10.5}$$

Notons que dans les calculs, il est plus simple d'écrire « y » que « x » la variable de la fonction réciproque. Il est néanmoins (très) recommandé de nommer « x » la variable dans la réponse finale. Dans notre cas nous concluons donc

$$f^{-1}(x) = \frac{x+2}{3}. \tag{10.6}$$

$\triangle$

10.2.2 Graphe de la fonction réciproque

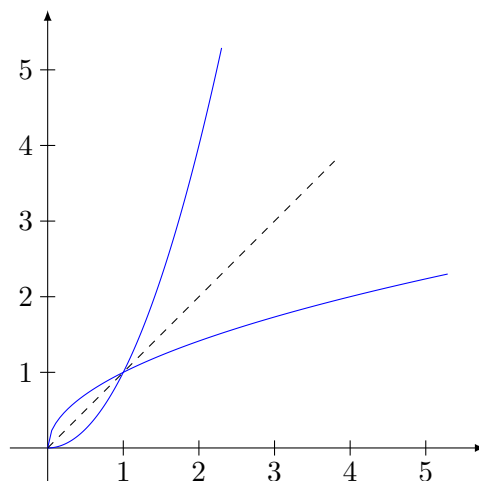
Par définition le graphe de la fonction f est l'ensemble des points de la forme (x, y) vérifiant $y = f(x)$. Afin de déterminer le graphe de la bijection réciproque nous pouvons faire le raisonnement suivant.

Le point (x_0, y_0) est sur le graphe de f
 $\Leftrightarrow$
 La relation $f(x_0) = y_0$ est vérifiée
 $\Leftrightarrow$
 La relation $x_0 = f^{-1}(y_0)$ est vérifiée
 $\Leftrightarrow$
 Le point (y_0, x_0) est sur le graphe de f^{-1} .

À retenir 10.11

Dans un repère orthonormal, le graphe de la bijection réciproque est obtenu à partir du graphe de f en effectuant une symétrie par rapport à la droite d'équation $y = x$.

Le dessin suivant montre le cas de la courbe de la fonction carré comparé à celle de la racine carrée.



10.3 Topologie sur l'ensemble des réels

Nous allons à présent donner la topologie sur $\mathbb{R}$ et ainsi résoudre les questions laissées en suspens lors de la construction des réels, voir 1.284.

Afin de pouvoir étudier la topologie des espaces métriques, il faut savoir quelques propriétés des réels parce que nous allons étudier la fonction distance qui est une fonction continue à valeurs dans les réels.

La valeur absolue de la définition 1.253(2) permet de définir une norme sur $\mathbb{R}$.

Lemme 10.12.

L'application

$$x \mapsto |x| \tag{10.7}$$

est une norme¹ sur $\mathbb{R}$.

Démonstration. Grâce au lemme 1.257 et à la remarque 1.258, on a, pour tous $x, y, \lambda \in \mathbb{R}$:

(1) $|x| = 0$ implique $x = 0$,

1. Définition 7.118.

$$(2) |\lambda x| = |\lambda||x|,$$

$$(3) |x + y| \leq |x| + |y|,$$

et donc, les conditions de la définition 7.118 sont immédiatement vérifiées. $\square$

Définition 10.13 (Topologie sur $\mathbb{R}$ et sur $\mathbb{Q}$).

Le lemme 10.12 donne une norme sur $\mathbb{R}$ et $\mathbb{Q}$ à partir de la valeur absolue. La définition 7.99 donne alors une structure d'espace topologique. Hors cas rarissimes qui seront signalés, nous utiliserons toujours cette topologie sur $\mathbb{R}$ et sur $\mathbb{Q}$.

Proposition 10.14.

Les rationnels sont denses dans les réels².

Démonstration. Soient $r \in \mathbb{R}$ et $\epsilon \in \mathbb{R}^+$. Nous devons prouver l'existence d'un rationnel dans $B(x, \epsilon)$. Le lemme 1.307 dit qu'il existe un rationnel dans $]x - \epsilon/2, x + \epsilon/2[$ et donc dans $B(x, \epsilon)$. $\square$

Proposition 10.15 ([1]).

Quel que soit le réel r , il existe une suite croissante de rationnels convergente vers r .

Démonstration. Soient $x \in \mathbb{R}$ et $\delta \in \mathbb{R}$; vu que $x - \delta$ et x sont des réels, le lemme 1.307 donne un élément $x_\delta \in \mathbb{Q}$ tel que

$$x - \delta < x_\delta < x. \quad (10.8)$$

Il suffit alors de pêcher parmi ces x_δ pour trouver une suite croissante, et on montrera que cette suite converge vers x .

Soit x_0 un rationnel plus petit que x . Nous posons $\delta_0 = x - x_0$ et ensuite :

$$\begin{cases} \delta_i = x - x_i \\ x_{i+1} = x_{\delta_i/2} \in \mathbb{Q}. \end{cases} \quad (10.9a)$$

$$(10.9b)$$

Ainsi nous avons pour tout i les inégalités

$$x_i = x - \delta_i < x - \frac{\delta_i}{2} < x_{i+1} < x. \quad (10.10)$$

La suite (x_i) est donc une suite de rationnels, croissante et toujours plus petite que x . Mais nous avons à chaque étape $\delta_{i+1} < \frac{\delta_i}{2}$, ce qui implique que la suite des δ_i converge vers 0. Soit $\epsilon > 0$. Il existe k_0 tel que pour tout $k > k_0$, $\delta_k < \epsilon$. Pour un tel k , nous avons alors

$$x_{k+1} \in B(x, \frac{\delta_k}{2}) \subset B(x, \epsilon). \quad (10.11)$$

Tous les x_k , pour $k > k_0 + 1$, sont tels que $|x - x_k| < \epsilon$: la suite des x_k converge donc vers x . $\square$

10.3.1 Compacité pour les réels

Pour la définition générale d'un compact, c'est 7.50.

Proposition 10.16.

Les parties compactes de $\mathbb{R}$ sont fermées et bornées.

Démonstration. Prouvons d'abord qu'un ensemble compact est borné. Pour cela, supposons que K est un compact non borné vers le haut³. Donc il existe une suite infinie de nombres strictement croissante $x_1 < x_2 < \dots$ tels que $x_i \in K$. Prenons n'importe quel recouvrement ouvert de la partie de K plus petite ou égale à x_1 , et complétons ce recouvrement par les ouverts $\mathcal{O}_i =]x_{i-1}, x_i[$. Le tout forme bien un recouvrement de K par des ouverts.

2. Pour les topologies usuelles données en la définition 10.13.

3. Nous laissons à titre d'exercice le cas où K est borné par le haut et pas par le bas.

Il n'y a cependant pas moyen d'en tirer un sous recouvrement fini parce que si on ne prend qu'un nombre fini parmi les $\mathcal{O}_i$, on en aura fatalement un maximum, disons $\mathcal{O}_k$. Dans ce cas, les points $x_{k+1}, x_{k+1}, \dots$ ne seront pas dans le choix fini d'ouverts.

Cela prouve que K doit être borné.

Pour prouver que K est fermé, nous allons prouver que le complémentaire est ouvert. Et pour cela, nous allons prouver que si le complémentaire n'est pas ouvert, alors nous pouvons construire un recouvrement de K dont on ne peut pas extraire de sous recouvrement fini.

Si $\mathbb{R} \setminus K$ n'est pas ouvert, il possède un point, disons x , tel que tout voisinage de x intersecte K . Soit $B(x, \epsilon_1)$, un de ces voisinages, et prenons $k_1 \in K \cap B(x, \epsilon_1)$. Ensuite, nous prenons ϵ_2 tel que k_1 n'est pas dans $B(x, \epsilon_2)$, et nous choisissons $k_2 \in K \cap B(x, \epsilon_2)$. De cette manière, nous construisons une suite de $k_i \in K$ tous différents et de plus en plus proches de x . Prenons un recouvrement quelconque par des ouverts de la partie de K qui n'est pas dans $B(x, \epsilon_1)$. Les nombres k_i ne sont pas dans ce recouvrement.

Nous ajoutons à ce recouvrement les ensembles $\mathcal{O} =]k_i, k_{i+1}[$. Le tout forme un recouvrement (infini) par des ouverts dont il n'y a pas moyen de tirer un sous recouvrement fini, pour exactement la même raison que la première fois. $\square$

Théorème 10.17 (Borel-Lebesgue).

Un intervalle de $\mathbb{R}$ est compact si et seulement si il est de la forme $[a, b]$.

Démonstration. Tous les intervalles de $\mathbb{R}$ sont listés dans la proposition 1.325. Un compact est fermé et borné (proposition 10.16). Donc les intervalles dont une borne est $\pm\infty$ ne sont pas compacts. Parmi les intervalles $]a, b[,]a, b], [a, b[$ et $[a, b]$, seul le dernier est fermé. Nous avons prouvé que si un intervalle est compact, alors il est de la forme $[a, b]$.

Nous prouvons à présent l'implication inverse : tous les intervalles de la forme $[a, b]$ sont compacts.

Soit Ω , un recouvrement du segment $[a, b]$ par des ouverts, c'est-à-dire que

$$[a, b] \subseteq \bigcup_{\mathcal{O} \in \Omega} \mathcal{O}. \quad (10.12)$$

Nous notons par M le sous-ensemble de $[a, b]$ des points m tels que l'intervalle $[a, m]$ peut être recouvert par un sous-ensemble fini de Ω . C'est-à-dire que M est le sous-ensemble de $[a, b]$ sur lequel le théorème est vrai. Le but est maintenant de prouver que $M = [a, b]$.

M est non vide En effet, $a \in M$ parce que il existe un ouvert $\mathcal{O} \in \Omega$ tel que $a \in \mathcal{O}$. Donc $\mathcal{O}$ tout seul recouvre l'intervalle $[a, a]$.

M est un intervalle Soient $m_1, m_2 \in M$. Le but est de montrer que si $m' \in [m_1, m_2]$, alors $m' \in M$. Il y a un sous recouvrement fini de l'intervalle $[a, m_2]$ (par définition de $m_2 \in M$). Ce sous recouvrement fini recouvre évidemment aussi $[a, m']$ parce que $[a, m'] \subseteq [a, m_2]$, donc $m' \in M$.

M est une ensemble ouvert Soit $m \in M$. Le but est de prouver qu'il y a un ouvert autour de m qui est contenu dans M . Mettons que Ω' soit un sous recouvrement fini qui contienne l'intervalle $[a, m]$. Dans ce cas, on a un ouvert $\mathcal{O} \in \Omega'$ tel que $m \in \mathcal{O}$. Tous les points de $\mathcal{O}$ sont dans M , vu qu'ils sont tous recouverts par Ω' . Donc $\mathcal{O}$ est un voisinage de m contenu dans M .

M est un ensemble fermé M est un intervalle qui commence en a , en contenant a , et qui finit on ne sait pas encore où. Il est donc soit de la forme $[a, m]$, soit de la forme $[a, m[$. Nous allons montrer que M est de la première forme en démontrant que M contient son supremum s . Ce supremum est un élément de $[a, b]$, et donc il est contenu dans un des ouverts de Ω . Disons $s \in \mathcal{O}_s$. Soit c , un élément de $\mathcal{O}_s$ strictement plus petit que s ; étant donné que s est supremum de M , cet élément c est dans M , et donc on a un sous recouvrement fini Ω' qui recouvre $[a, c]$. Maintenant, le sous recouvrement constitué de Ω' et de $\mathcal{O}_s$ est fini et recouvre $[a, s]$.

Nous pouvons maintenant conclure : le seul intervalle non vide de $[a, b]$ qui soit à la fois ouvert et fermé est $[a, b]$ lui-même (proposition 7.46), ce qui prouve que $M = [a, b]$, et donc que $[a, b]$ est compact⁴. $\square$

Lemme 10.18 ([229]).

Si $a < b \in \mathbb{R}$ alors le segment $[a, b]$ est compact⁵.

Démonstration. Soit $\{\mathcal{O}_i\}_{i \in I}$ un recouvrement de $[a, b]$ par des ouverts. Nous posons

$$M = \{x \in [a, b] \text{ tel que } [a, x] \text{ admet un sous-recouvrement fini extrait de } \{\mathcal{O}_i\}_{i \in I}\}. \quad (10.13)$$

Notre but est de prouver que $b \in M$.

a est dans M Le point a est naturellement dans un des $\mathcal{O}_i$. L'intervalle $[a, a]$ est donc recouvert par un seul des $\mathcal{O}_i$.

M est un intervalle Soient $m \in M$ et $m' \in [a, m[$. Le sous-recouvrement fini qui recouvre $[a, m]$ recouvre a fortiori $[a, m']$.

Les trois possibilités restantes À ce niveau de la preuve, il reste trois possibilités pour M soit il est de la forme $[a, c]$ ou $[a, c[$ avec $c < b$, soit il est de la forme $[a, b]$. Nous allons maintenant éliminer les deux premiers cas.

Ce que M n'est pas D'abord M n'est pas de la forme $[a, c[$ avec $c < b$. Par l'absurde, commençons par considérer $\mathcal{O}_{i_0}$ un ouvert du recouvrement qui contient c ; choisissons $m \in \mathcal{O}_{i_0}$ tel que $m < c$. Alors $m \in M$, et, si nous joignons $\mathcal{O}_{i_0}$ à un recouvrement fini de $[a, m]$ alors nous avons un recouvrement fini de $[a, c]$. On en déduit $c \in M$.

Ensuite M n'est pas de la forme $[a, c]$ avec $c < b$. En effet si on a un recouvrement fini de $[a, c]$ par des ouverts, alors un de ces ouverts contient c et donc contient des éléments de $[a, b]$ plus grands que c .

Nous déduisons que $M = [a, b]$ et qu'il est possible d'extraire un sous-recouvrement fini recouvrant $[a, b]$. $\square$

Lemme 10.19 ([1]).

Si K_1 et K_2 sont des compacts dans $\mathbb{R}$ alors $K_1 \times K_2$ est compact dans $\mathbb{R}^2$.

Démonstration. Soit $\{\mathcal{O}_i\}_{i \in I}$ un recouvrement de $K_1 \times K_2$ par des ouverts; grâce au lemme 7.61 nous pouvons supposer que ce sont des carrés. Pour chaque $x \in K_1$, l'ensemble $\{x\} \times K_2$ est compact et donc recouvert par un nombre fini des $\mathcal{O}_i$. Soit R_x un ensemble fini des $\mathcal{O}_i$ recouvrant $\{x\} \times K_2$.

Vu que R_x est une collection finie de carrés nous pouvons considérer m_x , le minimum des rayons. L'ensemble K_1 est recouvert par les boules $B(x, m_x)$ et il existe donc une collection finie de $\{x_i\}_{i \in A}$ tels que $B(x_i, m_{x_i})$ recouvre K_1 .

Alors $\{R_{x_i}\}_{i \in A}$ recouvre $K_1 \times K_2$ parce que R_{x_i} recouvre l'ensemble $B(x_i, m_{x_i}) \times \{K_2\}$. $\square$

10.3.2 Conséquence : les fermés bornés sont compacts

Théorème 10.20 (Théorème de Borel-Lebesgue).

Une partie d'un espace vectoriel normé réel de dimension finie est compacte si et seulement si elle est fermée et bornée.

Démonstration. Sens direct.

4. Si vous n'aimez pas le coup du fermé et ouvert, le lemme 10.18 donne une autre preuve.

5. Définition 7.50

Compact implique borné En effet si K est non borné dans E alors K contient une suite (x_n) avec $\|x_n\| > n$. Les boules $B_i(x_i, \frac{1}{3})$ sont disjointes. On pose $\mathcal{O}_0 = \mathbb{C} \setminus \overline{\bigcup_i B(x_i, \frac{1}{5})}$, qui est ouvert comme complément d'un fermé. Pour $i \geq 1$ nous posons $\mathcal{O}_i = B(x_i, \frac{1}{4})$. Nous avons

$$K \subset \bigcup_{i \in \mathbb{N}} \mathcal{O}_i \quad (10.14)$$

mais vu que x_i est uniquement dans $\mathcal{O}_i$, nous ne pouvons pas extraire de sous-recouvrement fini.

Compact implique fermé Cela est le lemme 7.63(2).

Sens réciproque.

Un intervalle fermé et borné est compact dans $\mathbb{R}$ C'est le lemme 10.18.

Un produit de segments est compact Le produit de deux compacts de $\mathbb{R}$ est un compact dans $\mathbb{R}^2$ par le lemme 10.19.

Un fermé et borné est compact Soit K fermé et borné. Vu que K est borné, il est contenu dans un produit de segments. L'ensemble K est donc compact parce que fermé dans un compact, lemme 7.63.

□

Exemple 10.21 (Compacité de la boule unité).

La boule unité fermée $\overline{B(0, 1)}$ d'un espace vectoriel normé de dimension finie est compacte parce que fermée et bornée. En dimension infinie, cela n'est plus le cas. Certes la boule unité est encore fermée et bornée, mais elle n'est plus compacte. En effet nous allons donner un recouvrement par des ouverts duquel il ne sera pas possible d'extraire un sous-recouvrement fini.

Autour de chacune des extrémités des vecteurs de base, nous considérons la boule $A_i = B(e_i, \frac{1}{3})$. Ensuite aussi l'ouvert

$$B(0, 1) \setminus \bigcup_i \overline{B(e_i, \frac{1}{4})}. \quad (10.15)$$

Le tout recouvre $B(0, 1)$ mais toutes les premières boules sont nécessaires. △

Le théorème de Bolzano-Weierstrass 7.201 nous permettra de prouver plus simplement la non compacité en dimension infinie. Voir l'exemple 7.109.

10.3.3 Suites et limites dans les réels

10.3.3.1 Limites, convergence

Dans le cas de suites réelles, nous avons la caractérisation suivante qui est souvent donnée comme une définition lorsque seule la topologie sur $\mathbb{R}$ est considérée.

Proposition 10.22 (Limite d'une suite numérique).

La suite (x_n) est convergente si et seulement s'il existe un réel ℓ tel que

$$\forall \epsilon > 0, \exists N \in \mathbb{N} \text{ tel que } \forall n \geq N, |x_n - \ell| < \epsilon. \quad (10.16)$$

Dans ce cas, le nombre ℓ est la limite de la suite (x_n) .

Proposition-Définition 10.23.

Une suite (x_n) dans un espace vectoriel normé V est convergente⁶ si et seulement si il existe un élément $\ell \in V$ tel que

$$\forall \epsilon > 0, \exists N \in \mathbb{N} \text{ tel que } n \geq N \Rightarrow \|x_n - \ell\| < \epsilon. \quad (10.17)$$

Dans ce cas, ℓ est la limite de la suite (x_n) .

6. Définition 7.13.

Démonstration. En deux parties.

Sens direct Si $x_n \rightarrow \ell$ et si $\epsilon > 0$ il existe N_ϵ tel que pour tout $n \geq N$ nous avons $x_n \in B(\ell, \epsilon)$ (parce que cette boule est un ouvert contenant ℓ). Vue la définition d'une boule, cette condition s'écrit bien $\|x_n - \ell\| < \epsilon$.

Sens inverse Dans l'autre sens, soit $\mathcal{O}$ un ouvert contenant ℓ . Par définition de la topologie, il existe $\epsilon > 0$ tel que $B(\ell, \epsilon) \subset \mathcal{O}$. La condition (10.16) nous assure qu'il existe N_ϵ tel que pour tout $n \geq N_\epsilon$ nous ayons

$$x_n \in B(\ell, \epsilon) \subset \mathcal{O}, \quad (10.18)$$

ce qui assure que la suite (x_n) converge vers ℓ pour la topologie métrique de V .

□

Une façon équivalente d'exprimer le critère (10.16) est de dire que pour tout ϵ positif, il existe un rang $N \in \mathbb{R}$ tel que l'intervalle $[\ell - \epsilon, \ell + \epsilon]$ contient tous les termes x_n au-delà de N .

Il est à noter que le rang N dont il est question dans la définition de suite convergente dépend de ϵ .

Définition 10.24.

Nous disons qu'une suite réelle (x_n) converge⁷ vers ℓ lorsque pour tout ε , il existe un N tel que

$$n > N \Rightarrow |x_n - \ell| \leq \varepsilon. \quad (10.19)$$

Le concept fondamental de cette définition est la notion de valeur absolue qui permet de donner la « distance » entre deux réels. Dans un espace vectoriel normé quelconque, cette notion est généralisée par la distance associée à la norme (définition 7.118). Nous pouvons donc facilement définir le concept de convergence d'une suite dans un espace vectoriel normé.

10.3.4 Opérations sur les limites

Proposition 10.25 ([1]).

Soient des suites à valeurs réelles (a_i) et (b_j) si elles sont convergentes, alors la suite ab est convergente et

$$\left(\lim_i a_i\right) \left(\lim_j b_j\right) = \lim_i (a_i b_i). \quad (10.20)$$

Démonstration. Nous nommons a et b les limites des suites (a_i) et (b_j) . Soit $\epsilon > 0$ ainsi que $i \in \mathbb{N}$. Nous avons la majoration

$$|a_i b_i - ab| \leq |a_i b_i - a_i b| + |a_i b - ab| \quad (10.21a)$$

$$\leq |a_i| |b_i - b| + b |a_i - a|. \quad (10.21b)$$

Vu que la suite (a_i) est convergente, elle est bornée. Nous pouvons donc majorer $|a_i|$ par $R > 0$ qui ne dépend pas de i . Soit $\eta > 0$ tel que $(R + b)\eta < \epsilon$. Alors en prenant i assez grand pour que $|b_i - b| < \eta$ et $|a_i - a| < \eta$, nous avons bien

$$|a_i b_i - ab| \leq (R + b)\eta < \epsilon. \quad (10.22)$$

□

Proposition 10.26.

Soient des suites (x_n) et (y_n) dans un espace vectoriel normé V . Si $x_n \xrightarrow{V} x$ et $y_n \xrightarrow{V} y$, alors

$$x_n + y_n \xrightarrow{V} x + y. \quad (10.23)$$

7. Voir la définition 10.22 pour plus de détail.

Démonstration. Soit $\epsilon > 0$. Nous considérons N tel que si $n \geq N$, alors $\|x_n - x\| \leq \epsilon$ et $\|y_n - y\| \leq \epsilon$. En utilisant l'inégalité 7.118(4),

$$\|x_n + y_n - (x + y)\| \leq \|x_n - x\| + \|y_n - y\| \leq 2\epsilon. \quad (10.24)$$

Donc la suite $(x_n + y_n)$ converge vers $x + y$. $\square$

Lemme 10.27.

La fonction

$$\begin{aligned} f: \mathbb{R} \times \mathbb{R} &\rightarrow \mathbb{R} \\ (x, y) &\mapsto x + y \end{aligned} \quad (10.25)$$

est continue.

Démonstration. Pour rappel, la topologie considérée sur $\mathbb{R}^n$ est celle de la définition 7.128. En vertu de la proposition 7.164, il est suffisant de prouver la continuité séquentielle. Soit donc une suite convergente

$$(x_n, y_n) \xrightarrow{\mathbb{R} \times \mathbb{R}} (x, y). \quad (10.26)$$

Nous devons prouver que

$$f(x_n, y_n) \xrightarrow{\mathbb{R}} f(x, y). \quad (10.27)$$

La proposition 7.40 nous permet de déduire la convergence composante par composante : $x_n \xrightarrow{\mathbb{R}} x$ et $y_n \xrightarrow{\mathbb{R}} y$. En permutant somme et limite (proposition 10.26) nous avons le calcul

$$f(x_n, y_n) = x_n + y_n \xrightarrow{\mathbb{R}} x + y = f(x, y). \quad (10.28)$$

D'où la convergence demandée. $\square$

10.3.5 Exemples

Exemple 10.28.

Quelques suites usuelles.

- (1) La suite $x_n = \frac{1}{n}$ converge vers 0.
- (2) La suite $x_n = (-1)^n$ ne converge pas.

$\triangle$

Deux limites pour voir comment ça fonctionne.

Lemme 10.29.

Si $r > 1$ nous avons :

- (1) $\lim_{n \rightarrow \infty} r^n = \infty$.
- (2) $\lim_{n \rightarrow \infty} \frac{r^n}{n} = \infty$.

Démonstration. Vu que $r > 1$ nous pouvons écrire $r = 1 + \delta$ avec $\delta > 0$. La formule du binôme de Newton (3.59) nous donne

$$(1 + \delta)^n = \sum_{k=0}^n \binom{n}{k} \delta^k > \binom{n}{1} \delta = n\delta. \quad (10.29)$$

La proposition 1.306 ($\mathbb{R}$ est archimédien) nous indique que $n\delta$ est arbitrairement grand lorsque n est grand, quelle que soit $\delta > 0$. Cela finit la preuve de la première limite.

Pour la seconde, nous posons $a_n = \frac{r^n}{n}$. Nous avons

$$\frac{a_{n+1}}{a_n} = \frac{n}{n+1} r. \quad (10.30)$$

Vu que $\frac{n}{n+1} \rightarrow 1$, la suite $\frac{n}{n+1}r$ tend vers $r > 0$, et en particulier pour tout $\delta > 0$ tel que $r > 1 + \delta$, il existe $N \in \mathbb{N}$ tel que, pour tout $n > N$,

$$\frac{n}{n+1}r > 1 + \delta. \quad (10.31)$$

Soit maintenant $k \in \mathbb{N}$. En utilisant un produit télescopique,

$$a_{N+k} = a_N \frac{a_{N+1}}{a_N} \frac{a_{N+2}}{a_{N+1}} \cdots \frac{a_{N+k}}{a_{N+k-1}} > a_N (1 + \delta)^{k-1}. \quad (10.32)$$

Or $(1 + \delta)^{k-1}$ tend vers ∞ lorsque $k \rightarrow \infty$ par le premier point. Donc nous avons $\lim_{n \rightarrow \infty} r^n/n = \infty$. $\square$

Définition 10.30.

Nous disons que deux suites (u_n) et (v_n) sont **équivalentes** s'il existe une application $\alpha: \mathbb{N} \rightarrow \mathbb{R}$ telle que

(1) pour tout n à partir d'un certain rang, $u_n = v_n \alpha(n)$

(2) $\alpha(n) \rightarrow 1$.

10.3.6 Suites croissantes et bornées

Une suite est dite **contenue** dans un ensemble A si $x_n \in A$ pour tout n . Une suite est **bornée supérieurement** s'il existe un M tel que $x_n \leq M$ pour tout n . De la même manière, la suite est bornée inférieurement s'il existe un m tel que $x_n \geq m$ pour tout n .

Le lemme suivant est souvent utilisé pour prouver qu'une suite est convergente.

Lemme 10.31.

Une suite croissante et bornée supérieurement converge. Une suite décroissante bornée inférieurement est convergente.

Une erreur courante est de croire que la borne est la limite : le lemme n'affirme pas ça. Par contre il est vrai que la borne donne ... hum ... une borne inférieure (ou supérieure) pour la limite.

Proposition 10.32.

Une suite (x_n) dans $\mathbb{R}^m$ est convergente dans $\mathbb{R}^m$ si et seulement si les suites de chaque composante sont convergentes dans $\mathbb{R}$. Dans ce cas nous avons

$$\lim x_n = \left(\lim(x_n)_1, \lim(x_n)_2, \dots, \lim(x_n)_m \right) \quad (10.33)$$

où $(x_n)_k$ désigne la k -ième composante de (x_n) .

Exemple 10.33.

La suite $x_n = \left(\frac{1}{n}, 1 - \frac{1}{n}\right)$ converge vers $(0, 1)$ dans $\mathbb{R}^2$. En effet, en utilisant la proposition 10.32, nous devons calculer séparément les limites

$$\begin{aligned} \lim \frac{1}{n} &= 0 \\ \lim \left(1 - \frac{1}{n}\right) &= 1. \end{aligned} \quad (10.34)$$

$\triangle$

Exemple 10.34.

Étant donné que la suite $(-1)^n$ n'est pas convergente, la suite $x_n = \left((-1)^n, \frac{1}{n}\right)$ n'est pas convergente dans $\mathbb{R}^2$. $\triangle$

10.3.7 Suites adjacentes

Définition 10.35 ([230]).

Les suites (a_n) et (b_n) sont **adjacentes** si l'une est croissante, l'autre décroissante et si $a_n - b_n \rightarrow 0$.

Théorème 10.36 (Théorème des suites adjacentes).

Nous considérons des suites adjacentes (a_n) et (b_n) avec (a_n) croissante et (b_n) décroissante. Alors

- (1) $b_n \geq a_n$ pour tout n ,
- (2) $a_n \leq b_q$ pour tout n et q . C'est-à-dire que toute la suite a est plus petite que toute la suite b .
- (3) les suites a et b sont convergentes,
- (4) les suites a et b convergent vers la même limite, notée ℓ ,
- (5) nous avons $a_n \leq \ell \leq b_n$ pour tout n .

Démonstration. La suite $n \mapsto b_n - a_n$ est décroissante parce que $b_n - a_n \geq b_{n+1} - a_{n+1}$. Comme en plus $b_n - a_n \rightarrow 0$ nous avons

$$b_n - a_n \geq 0 \quad (10.35)$$

pour tout $n \in \mathbb{N}$. De plus $a_n \leq b_0$ pour tout n parce que si $a_N > b_0$ alors, b étant décroissante, $a_N > b_0 \geq b_N$ qui est contraire à ce que nous venons de prouver. La suite a étant croissante et majorée, elle est convergente⁸; notons ℓ sa limite.

La suite b peut maintenant être écrite par

$$b_n = (b_n - a_n) + a_n \quad (10.36)$$

qui est une somme de deux suites convergentes. Elle est donc convergente et sa limite est la somme des limites⁹, donc

$$\lim_{n \rightarrow \infty} b_n = \lim_{n \rightarrow \infty} (b_n - a_n) + a_n = 0 + \ell = \ell. \quad (10.37)$$

Voilà. Donc les suites a et b convergent et ont la même limite.

Pour tout $n, q \in \mathbb{N}$ nous avons l'inégalité $a_n \leq b_q$. En prenant la limite $n \rightarrow \infty$ nous trouvons

$$\ell \leq b_q \quad (10.38)$$

pour tout q . Et de la même façon, $b_n \geq a_q$ donne $\ell \geq a_q$. L'un avec l'autre donne

$$a_q \leq \ell \leq b_q \quad (10.39)$$

pour tout $q \in \mathbb{N}$. □

Proposition 10.37 ([231]).

Soit une suite (a_n) dans $\mathbb{R}$. Nous supposons que les suites extraites (a_{2n}) et (a_{2n+1}) convergent vers la même limite notée ℓ .

Alors $a_n \rightarrow \ell$.

Démonstration. Soit $\epsilon > 0$. Il existe N_1 tel que $|a_{2n} - \ell| \leq \epsilon$ dès que $n \geq N_1$. Il existe également N_2 dès que $|a_{2n+1} - \ell| \leq \epsilon$ dès que $n \geq N_2$.

Nous posons $N = \max\{2N_1, 2N_2 + 2\}$ et nous avons, pour tout $n \geq N$:

$$|a_n - \ell| \leq \epsilon, \quad (10.40)$$

c'est-à-dire que $a \rightarrow \ell$. □

8. Proposition 10.31.

9. Proposition 10.26.

10.3.8 Limite supérieure et inférieure

Lemme-Définition 10.38.

Soit (a_n) une suite dans $\bar{\mathbb{R}}$. Les limites suivantes existent dans $\bar{\mathbb{R}}$

$$\limsup_{n \rightarrow \infty} a_n = \lim_{n \rightarrow \infty} \left(\sup_{k \geq n} a_k \right) \quad (10.41)$$

et

$$\liminf_{n \rightarrow \infty} a_n = \lim_{n \rightarrow \infty} \left(\inf_{k \geq n} a_k \right). \quad (10.42)$$

Elles sont nommées **limite supérieure** et la **limite inférieure** de la suite (a_k) .

Démonstration. Pour la limite supérieure, l'ensemble des $k \geq n$ est de plus en plus petit lorsque n grandit. Donc les ensembles $A_n = \{a_k \text{ tel que } k \geq n\}$ sont emboîtés et la suite $n \rightarrow \sup A_n$ est une suite décroissante. Elle a donc une limite dans $\bar{\mathbb{R}}$. $\square$

10.39.

En ce qui concerne les suites d'ensembles, utiles en théorie des probabilités, nous définissons de même. Si les A_n sont des parties de Ω , nous définissons la **limite supérieure** et la **limite inférieure** de la suite A_n par

$$\limsup_{n \rightarrow \infty} A_n = \bigcap_{n \geq 1} \bigcup_{k \geq n} A_k \quad (10.43)$$

et

$$\liminf_{n \rightarrow \infty} A_n = \bigcup_{n \geq 1} \bigcap_{k \geq n} A_k \quad (10.44)$$

Nous avons

$$\limsup A_n = \{\omega \in \Omega \text{ tel que } \omega \in A_n \text{ pour une infinité de } n\}. \quad (10.45)$$

Lemme 10.40.

Nous avons les formules pratiques suivantes :

$$\limsup a_n = \inf_{n \geq 1} \left(\sup_{k \geq n} a_k \right) \quad (10.46a)$$

$$\liminf a_n = \sup_{n \geq 1} \left(\inf_{k \geq n} a_k \right). \quad (10.46b)$$

Démonstration. La suite $n \mapsto \sup_{k \geq n} a_k$ est une suite décroissante, donc la limite est l'infimum. Même argument pour l'autre. $\square$

Lemme 10.41.

La suite (a_n) dans $\mathbb{R}$ converge si et seulement si

$$\limsup a_n = \liminf a_n. \quad (10.47)$$

Dans ce cas, $\lim a_n = \limsup a_n = \liminf a_n$.

Démonstration. Nous commençons par supposer que $\limsup a_n = \liminf a_n = l$, et nous prouvons que $\lim a_n$ existe et vaut l . Soit $\epsilon > 0$. Il existe N tel que si $n \geq N$ nous avons

$$\left| \sup_{k \geq n} a_k - l \right| < \epsilon \quad (10.48)$$

et

$$\left| \inf_{k \geq n} a_k - l \right| < \epsilon. \quad (10.49)$$

Pour tout $k \geq N$ nous avons alors $a_k \leq l + \epsilon$ et $a_k \geq l - \epsilon$. Cela donne $a_n \in B(l, \epsilon)$, c'est-à-dire $a_k \rightarrow l$ par la proposition 10.22.

Dans l'autre sens, nous supposons que $\lim_n a_n = l$ et nous prouvons que les limites supérieures et inférieures sont toutes deux égales à l . Soit $\epsilon > 0$ et N_ϵ tel que $|a_n - l| < \epsilon$ pour tout $n \geq N_\epsilon$. Si $n \geq N_\epsilon$ nous avons

$$\left| \sup_{k \geq n} a_k - l \right| \leq \epsilon \quad (10.50)$$

et donc la limite de $\sup_{k \geq n} a_k$ lorsque $n \rightarrow \infty$ est bien l . $\square$

Lemme 10.42.

Soit une suite (a_i) dans $\mathbb{R}$. Il existe $N \in \mathbb{N}$ tel que pour tout $i \geq N$,

$$x_i \leq \limsup_i(a_i). \quad (10.51)$$

Démonstration. Soit M un nombre tel que pour tout N , il existe $k \geq N$ tel que $x_k > M$. Dans ce cas, pour tout N nous avons

$$\sup_{i \geq N}(a_i) \geq M \quad (10.52)$$

et donc

$$\limsup_n(a_n) = \lim_{N \rightarrow \infty} \sup_{i \geq N}(a_i) \geq M. \quad (10.53)$$

$\square$

10.3.9 Ouverts, voisinage, topologie

Lorsque $x \in E$, nous rappelons qu'un voisinage¹⁰ de x est n'importe quel sous-ensemble de E qui contient une boule ouverte centrée en x . La proposition 7.7 nous dit qu'un ensemble est ouvert s'il contient un voisinage de chacun de ses points. Au passage, rappelons que l'ensemble vide est ouvert.

Pour rappel, la remarque 7.100(2) dit que l'ensemble des boules ouvertes d'un espace métrique génère la topologie de l'espace.

Nous rappelons qu'une partie A d'un espace métrique est dite bornée¹¹ s'il existe une boule¹² qui contient A .

Mais revenons à $\mathbb{R} \dots$

Lemme 10.43.

Une partie ouverte de $\mathbb{R}$ ne contient pas son supremum.

Démonstration. Soit $\mathcal{O}$, un ensemble ouvert et s , son supremum. Si s était dans $\mathcal{O}$, on aurait un voisinage $B = B(s, r)$ de s contenu dans $\mathcal{O}$. Le point $s + r/2$ est alors à la fois dans $\mathcal{O}$ et plus grand que s , ce qui contredit le fait que s soit un supremum de $\mathcal{O}$. $\square$

Par le même genre de raisonnements, on montre que l'union et l'intersection de deux ouverts sont encore des ouverts.

Remarque 10.44.

L'intersection d'une infinité d'ouverts n'est pas spécialement un ouvert comme le montre l'exemple suivant :

$$\mathcal{O}_i =]1, 2 + \frac{1}{i}[.$$

Tous les ensembles $\mathcal{O}_i$ contiennent le point 2 qui est donc dans l'intersection. Mais quel que soit le $\epsilon > 0$ que l'on choisisse, le point $2 + \epsilon$ n'est pas dans $\mathcal{O}_{(1/\epsilon)+1}$. Donc aucun point au-delà de 2 n'est dans l'intersection, ce qui prouve que 2 ne possède pas de voisinages contenus dans $\bigcap_{i=1}^{\infty} \mathcal{O}_i$.

10. Définition 7.4.

11. Définition 7.104.

12. À titre d'exercice, convainquez-vous que l'on peut dire boule *ouverte* ou *fermée* au choix sans changer la définition.

Proposition 10.45.

Quelles que soient les parties A et B de $\mathbb{R}$, nous avons

$$\sup(A \cap B) \leq \sup A \leq \sup(A \cup B). \quad (10.54)$$

Démonstration. En deux parties.

$\sup(A \cap B) \leq \sup(A)$ Soit $s = \sup(A)$. En particulier, s est un majorant de A . Si $x \in A \cap B$, alors $x \in A$ et $s \geq x$. Donc s est également un majorant de $A \cap B$. Le lemme 1.324 conclut que $s \geq \sup(A \cap B)$.

$\sup(A) \leq \sup(A \cup B)$ Soit $s = \sup(A \cup B)$. Par définition, s est un majorant de $A \cup B$. À fortiori, s est un majorant de A et donc est plus grand ou égal à $\sup(A)$. □

10.3.10 Intervalles et connexité

Nous allons déterminer tous les sous-ensembles connexes¹³ de $\mathbb{R}$. Pour cela nous relisons d'abord la notion d'intervalle donnée en 1.15 ainsi que la proposition 1.325 qui liste tous les intervalles de $\mathbb{R}$. La partie $I \subset \mathbb{R}$ est un intervalle si pour tout $a, b \in I$, tout nombre entre a et b est également dans I . Cette définition englobe tous les exemples connus d'intervalles ouverts, fermés avec ou sans infini : $[a, b]$, $[a, b[$, $] - \infty, a]$, ... L'ensemble $\mathbb{R}$ lui-même est un intervalle.

Si I est un intervalle, les nombres $\inf(I)$ et $\sup(I)$ ¹⁴ sont les **extrémités** de I .

Définition 10.46.

Étant donnés deux points a et b dans $\mathbb{R}^p$ on appelle **segment** d'extrémités a et b , et on note $[a, b]$, l'image de $[0, 1]$ par l'application $s : [0, 1] \rightarrow \mathbb{R}^p$, $s(t) = (1 - t)a + tb$. On pose $]a, b[= s(]0, 1[)$, et $]a, b] = s(]0, 1])$.

Il faut observer que le segment $[a, b]$ est une courbe orientée : certes en tant que ensembles, $[a, b] = [b, a]$, mais si nous regardons la fonction de t correspondante à $[b, a]$, nous voyons qu'elle va dans le sens inverse de celle qui correspond à $[a, b]$. Nous approfondirons ces questions lorsque nous parlerons d'arcs paramétrés autour de la section 21.7.

Le segment $[b, a]$ est l'image de l'application $r : [0, 1] \rightarrow \mathbb{R}^p$ donnée par $r(t) = (1 - t)b + ta$.

Proposition 10.47.

Une partie de $\mathbb{R}$ est connexe si et seulement si c'est un intervalle¹⁵.

Démonstration. La preuve est en deux parties. D'abord nous démontrons que si un sous-ensemble de $\mathbb{R}$ est connexe, alors c'est un intervalle ; et ensuite nous démontrons que tout intervalle est connexe.

Afin de prouver qu'un ensemble connexe est toujours un intervalle, nous allons prouver que si un ensemble n'est pas un intervalle, alors il n'est pas connexe. Prenons A , une partie de $\mathbb{R}$ qui n'est pas un intervalle. Il existe donc $a, b \in A$ et un x_0 entre a et b qui n'est pas dans A . Comme le but est de prouver que A n'est pas connexe, il faut couper A en deux ouverts disjoints. L'élément x_0 qui n'est pas dans A est le bon candidat pour effectuer cette coupure. Prenons M , un majorant de A et m , un minorant de A , et définissons

$$\begin{aligned} \mathcal{O}_1 &=]m, x_0[\\ \mathcal{O}_2 &=]x_0, M[. \end{aligned}$$

Si A n'a pas de minorant, nous remplaçons la définition de $\mathcal{O}_1$ par $] - \infty, x_0[$, et si A n'a pas de majorant, nous remplaçons la définition de $\mathcal{O}_2$ par $]x_0, \infty[$. Dans tous les cas, ce sont deux

13. Définition 7.44.

14. Qui existent par la proposition 1.323, quitte à poser $\pm\infty$ comme infimum et supremum lorsque I n'est pas borné.

15. Définition 1.15.

ensembles ouverts dont l'union recouvre tout A . En effet, $\mathcal{O}_1 \cup \mathcal{O}_2$ contient tous les nombres entre un minorant de A et un majorant sauf x_0 , mais on sait que x_0 n'est pas dans A . Cela prouve que A n'est pas connexe.

Jusqu'à présent nous avons prouvé que si un ensemble n'est pas un intervalle, alors il ne peut pas être connexe. Pour remettre les choses à l'endroit, prenons un ensemble connexe, et demandons-nous s'il peut être autre chose qu'un intervalle ? La réponse est *non* parce que s'il était autre chose, il ne serait pas connexe.

Prouvons à présent que tout intervalle est connexe. Pour cela, nous refaisons le coup de la contraposée. Nous allons donc prendre une partie A de $\mathbb{R}$, supposer qu'elle n'est pas connexe et puis prouver qu'elle n'est alors pas un intervalle. Nous avons deux ouverts disjoints $\mathcal{O}_1$ et $\mathcal{O}_2$ tels que $A \subset \mathcal{O}_1 \cup \mathcal{O}_2$. Notons $A_1 = A \cap \mathcal{O}_1$ et $A_2 = A \cap \mathcal{O}_2$; et prenons $a \in A_1$ et $b \in A_2$. Pour fixer les idées, on suppose que $a < b$. Maintenant, le jeu est de montrer qu'il existe un point x_0 entre a et b qui ne soit pas dans A (cela montrerait que A n'est pas un intervalle). Nous allons prouver que c'est le cas du point

$$x_0 = \sup\{x \in \mathcal{O}_1 \text{ tel que } x < b\}.$$

Étant donné que l'ensemble $\mathcal{A} = \{x \in \mathcal{O}_1 \text{ tel que } x < b\}$ est ouvert¹⁶, le point x_0 n'est pas dans l'ensemble par le lemme 10.43. Nous avons donc

- soit x_0 n'est pas dans $\mathcal{O}_1$,
- soit $x_0 \leq b$,
- soit les deux en même temps.

Nous allons montrer qu'un tel x_0 ne peut pas être dans A . D'abord, remarquons que $\sup \mathcal{A} \leq \sup \mathcal{O}$ parce que $\mathcal{A}$ est une intersection de $\mathcal{O}$ avec quelque chose. Ensuite, il n'est pas possible que x_0 soit dans $\mathcal{O}_2$ parce que tout élément de $\mathcal{O}_2$ possède un voisinage contenu dans $\mathcal{O}_2$. Un point de $\mathcal{O}_2$ est donc toujours strictement plus grand que le supremum de $\mathcal{O}_1$.

Maintenant, remarque que si $x_0 \leq b$, alors $x_0 = b$, sinon b serait un majorant de $\mathcal{A}$ plus petit que x_0 , ce qui n'est pas possible vu que x_0 est le supremum de $\mathcal{A}$ et donc le plus petit majorant. Oui mais si $x_0 = b$, c'est que $x_0 \in \mathcal{O}_2$, ce qu'on vient de montrer être impossible. Nous voilà déjà débarrassé des deuxièmes et troisièmes possibilités.

Si la première possibilité est vraie, alors x_0 n'est pas dans A parce qu'on a aussi prouvé que $x_0 \notin \mathcal{O}_2$. Or n'être ni dans $\mathcal{O}_1$ ni dans $\mathcal{O}_2$ implique de ne pas être dans A . Ce point $x_0 = \sup \mathcal{A}$ est donc hors de A .

Oui, mais comme $a \in \mathcal{A}$, on a obligatoirement que $x_0 \geq a$. Mais par construction, on a aussi que $x_0 \leq b$ (ici, l'inégalité est même stricte, mais ce n'est pas important). Donc

$$a \leq x_0 \leq b$$

avec $a, b \in A$, et $x_0 \notin A$. Cela finit de prouver que A n'est pas un intervalle. $\square$

Le lemme suivant dit que si on recouvre un intervalle avec des ouverts, alors on peut ordonner ces ouverts de telle sorte qu'ils s'enchainent bien : on peut sauter de l'un à l'autre en passant par les intersections. C'est donc un lemme qui permet de passer du local au global.

Lemme 10.48.

Soient un intervalle I de $\mathbb{R}$ ainsi qu'un recouvrement $\{\mathcal{O}_i\}_{i=1,\dots,n}$ de I par des ouverts connexes tels que $\mathcal{O}_i \cap I \neq \emptyset$ pour tout i ¹⁷. Alors il existe une bijection $\psi: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ tel que

(1)

$$\bigcup_{i=1}^m \mathcal{O}_{\psi(i)} \quad (10.55)$$

est connexe pour tout m .

16. C'est l'intersection entre l'ouvert $\mathcal{O}_1$ et l'ouvert $\{x \text{ tel que } x < b\}$.

17. Il est cependant possible que les $\mathcal{O}_i$ ne soient pas inclus à I .

(2)

$$\mathcal{O}_{\psi(m)} \cap \bigcup_{i=1}^{m-1} \mathcal{O}_{\psi(i)} \neq \emptyset. \quad (10.56)$$

Démonstration. Nous allons construire ψ par récurrence ; plus précisément nous allons construire des applications $\psi_k : \{1, \dots, k\} \rightarrow \{1, \dots, n\}$ telle que

(1) ψ_k est injective.(2) Si $i \leq k$ alors $\psi_k(i) = \psi_i(i)$.

(3) La partie

$$\bigcup_{i=1}^m \mathcal{O}_{\psi_k(i)} \quad (10.57)$$

est connexe pour tout $m \leq k$.

(4) Nous avons

$$\mathcal{O}_{\psi_k(m)} \cap \bigcup_{i=1}^{m-1} \mathcal{O}_{\psi_k(i)} \neq \emptyset \quad (10.58)$$

pour tout $m \leq k$.

Nous commençons en douceur par

$$\begin{aligned} \psi_1 : \{1\} &\rightarrow \{1, \dots, n\} \\ 1 &\mapsto 1. \end{aligned} \quad (10.59)$$

Ai-je besoin de vous prouver que c'est injectif ?

Nous supposons que les applications ψ_i sont correctement définies pour $i \leq k$, et nous construisons ψ_{k+1} . Nous posons

$$A = \psi_k(\{1, \dots, k\}) \quad (10.60a)$$

$$B = \{1, \dots, n\} \setminus A \quad (10.60b)$$

$$P = \bigcup_{i=1}^k \mathcal{O}_{\psi_k(i)} \quad (10.60c)$$

$$Q = \bigcup_{i=k+1}^n \mathcal{O}_{\psi_k(i)} \quad (10.60d)$$

En tant qu'unions d'ouverts, les parties P et Q sont ouvertes dans $\mathbb{R}$. Elles recouvrent l'intervalle I qui est connexe par la proposition 10.47. De plus $P \cap I \neq \emptyset$ et $Q \cap I \neq \emptyset$; donc, par définition de la connexité nous avons $P \cap Q \neq \emptyset$.

Il existe donc $i_0 \in B$ tel que $P \cap \mathcal{O}_{i_0} \neq \emptyset$. Nous posons

$$\begin{aligned} \psi_{k+1} : \{1, \dots, k+1\} &\rightarrow \{1, \dots, n\} \\ i &\mapsto \begin{cases} \psi_k(i) & \text{si } i \neq k+1 \\ i_0 & \text{si } i = k+1. \end{cases} \end{aligned} \quad (10.61)$$

Vérifions que ce ψ_{k+1} vérifie les conditions.

(1) ψ_{k+1} est injective. Soient i, j tels que $\psi_{k+1}(i) = \psi_{k+1}(j)$. Si $i = k+1$ et $j \neq k+1$ alors $\psi_{k+1}(i) = i_0 \in B$, alors que $\psi_{k+1}(j) = \psi_k(j) \in A$. Donc le cas $i = k+1, j \neq k+1$ n'est pas possible.

Si $i, j \neq k+1$, alors $\psi_{k+1}(i) = \psi_k(i)$ et $\psi_{k+1}(j) = \psi_k(j)$. L'injectivité de ψ_k implique que $i = j$.

(2) Si $i \leq k$, nous avons $\psi_{k+1}(i) = \psi_k(i) = \psi_i(i)$ en utilisant la récurrence.

- (3) Nous séparons les cas $m = k + 1$ et $m \neq k + 1$. Si $m \neq k + 1$ alors tous les ψ_{k+1} dans (10.57)¹⁸ sont des ψ_k et la récurrence fonctionne. Si $m = k + 1$ alors

$$\bigcup_{i=1}^{k+1} \mathcal{O}_{\psi_{k+1}(i)} = \bigcup_{i=1}^k \mathcal{O}_{\psi_k(i)} \cup \mathcal{O}_{\psi_{k+1}(k+1)} = P \cup \mathcal{O}_{i_0}. \quad (10.62)$$

Le nombre i_0 a été choisit pour avoir $\mathcal{O}_{i_0} \cap P \neq \emptyset$. Vu que $\mathcal{O}_{i_0}$ et P sont de connexes, la proposition 7.48(1) implique que $P \cup \mathcal{O}_{i_0}$ est connexe.

- (4) Encore une fois, si $m \neq k + 1$, tous les ψ_{k+1} de (10.58) deviennent des ψ_k et la récurrence fonctionne. Avec $m = k + 1$ nous avons

$$\mathcal{O}_{\psi_{k+1}(k+1)} \cap \bigcup_{i=1}^k \mathcal{O}_{\psi_{k+1}(i)} = \mathcal{O}_{i_0} \cap P. \quad (10.63)$$

Cette intersection est non vide, par choix du i_0 .

Quand tous les ψ_k ($k = 1, \dots, n$) sont construits, en posant $\psi = \psi_n$ nous avons le résultat annoncé. $\square$

Théorème 10.49 (Théorème des bornes atteintes).

Une fonction à valeurs réelles continue sur un compact est bornée et atteint ses bornes.

C'est-à-dire qu'il existe $x_0 \in K$ tel que $f(x_0) = \inf\{f(x) \text{ tel que } x \in K\}$ ainsi que x_1 tel que $f(x_1) = \sup\{f(x) \text{ tel que } x \in K\}$.

Démonstration. Soient un espace topologique compact K et une fonction continue $f: K \rightarrow \mathbb{R}$. Alors le théorème 7.97 indique que $f(K)$ est compact. Par conséquent $f(K)$ est un fermé borné de $\mathbb{R}$ par le théorème de Borel-Lebesgue 10.20. Vu que $f(K)$ est borné, la fonction f est bornée.

De plus $f(K)$ étant fermé, son infimum est un minimum et son supremum est un maximum : il existe $x \in K$ tel que $f(x) = \sup f(K)$ et il existe $y \in K$ tel que $f(y) = \inf f(K)$. $\square$

Le théorème suivant est essentiellement inutile pour les raisons suivantes :

- Il est un cas particulier du théorème 7.108 qui donne pour tout espace métrique, l'équivalence entre la compacité et la compacité séquentielle.
- Il est un cas particulier du théorème 7.201 qui le donne pour tous les espaces compacts.

Bref, nous ne le laissons que pour le lecteur qui n'aurait pas en tête d'autres définitions de « compact » à part « fermé borné ».

Théorème 10.50 (Théorème de Bolzano-Weierstrass).

Toute suite contenue dans un compact de $\mathbb{R}^m$ admet une sous-suite convergente.

Démonstration. Nous rappelons qu'une partie compacte de $\mathbb{R}^n$ est fermée et bornée par le théorème de Borel-Lebesgue 10.20.

Soit (x_n) une suite contenue dans une partie bornée de $\mathbb{R}^m$. Considérons (a_n) , la suite réelle des premières composantes des éléments de (x_n) : pour chaque $n \in \mathbb{N}$, le nombre a_n est la première composante de x_n . Étant donné que la suite (x_n) est bornée, il existe un M tel que $\|x_n\| < M$. La croissance de la fonction racine carrée donne

$$|a_n| \leq \|x_n\| \leq M. \quad (10.64)$$

La suite (a_n) est donc une suite réelle bornée et donc contient une sous-suite convergente par le théorème correspondant dans $\mathbb{R}$: 7.108. Soit a_{I_1} une sous-suite convergente de (a_n) . Nous considérons maintenant x_{I_1} , c'est-à-dire la suite de départ dont on a enlevé tous les éléments qu'il faut pour qu'elle converge en ce qui concerne la première composante.

¹⁸. Nous sommes en train de parler de cette équation avec $k + 1$ au lieu de k , parce que nous sommes dans un processus de récurrence. Il est donc normal de dire qu'il y a des ψ_{k+1} dans cette équation.

Si nous considérons la suite b_{I_1} des *secondes* composantes de x_{I_1} , nous en extrayons, de la même façon que précédemment, une sous-suite convergente, c'est-à-dire que nous avons un $I_2 \subset I_1$ tel que b_{I_2} est convergent. Notons que a_{I_2} est une sous-suite de la (sous) suite convergente x_{I_1} , et donc a_{I_2} est encore convergente.

En continuant ainsi, nous construisons une sous-sous-sous-suite x_{I_3} telle que la suite des *troisièmes* composantes est convergente. Lorsque nous avons effectué cette procédure m fois, la suite x_{I_m} est une suite dont toutes les composantes convergent, et donc est une suite convergente par la proposition 10.32.

Le tableau suivant donne un petit schéma de la façon dont nous procédons. Les $\bullet$ sont les éléments de la suite que nous gardons, et les $\times$ sont ceux que nous « jetons ».

$$\begin{array}{cccccccccccc}
 x_{\mathbb{N}} & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \dots \\
 x_{I_1} & \times & \bullet & \bullet & \times & \bullet & \times & \times & \bullet & \bullet & \bullet & \dots \\
 x_{I_2} & \times & \bullet & \times & \times & \bullet & \times & \times & \bullet & \bullet & \times & \dots \\
 \vdots & & & & & & & & & & & \\
 x_{I_m} & \times & \times & \times & \times & \bullet & \times & \times & \times & \bullet & \times & \dots
 \end{array} \tag{10.65}$$

La première ligne, $x_{\mathbb{N}}$, est la suite de départ. □

Corolaire 10.51.

Si une suite est croissante et bornée alors elle est convergente.

Démonstration. Nous nommons (x_n) la suite et nous prenons un majorant M . Toute la suite est alors contenue dans le compact $[x_0, M]$, ce qui donne une sous-suite $(x_{\alpha(n)})$ convergente par le théorème de Bolzano-Weierstrass 7.201. Si ℓ est la limite de cette sous-suite alors nous avons $\ell \geq x_n$ pour tout n .

Pour tout $\epsilon > 0$ il existe K tel que si $n > K$ alors $|\ell - x_{\alpha(n)}| < \epsilon$. Vu que ℓ majore la suite nous avons même

$$x_{\alpha(n)} + \epsilon > \ell. \tag{10.66}$$

Vu que la suite est croissante pour tout $m > \alpha(K)$ nous avons $x_m + \epsilon > \ell$, ce qui signifie $|x_m - \ell| < \epsilon$. □

Nous aurons une version pour les fonctions croissantes et bornées en la proposition 12.53.

La proposition suivante dit que la notion d'ensemble non dénombrable ne prend pas réellement de force entre $\mathbb{R}$ et $\mathbb{R}^n$: il n'y a pas moyen de caser $\mathbb{R}$ dans $\mathbb{R}^n$ de façon à ce qu'il y tienne à son aise.

Proposition 10.52.

*Une partie non dénombrable de $\mathbb{R}^n$ possède un point d'accumulation*¹⁹.

Démonstration. Soit une partie $A \subset \mathbb{R}^n$ sans point d'accumulation. Nous allons prouver que A est dénombrable.

Soient les compacts $K_n = \overline{B(0, n)}$. La partie $A \cap K_n$ est finie ; sinon elle aurait une partie en bijection avec $\mathbb{N}$ (proposition 1.117) et donc une suite. Or une suite dans un compact possède un point d'accumulation par le théorème 7.201.

Donc tous les $A \cap K_n$ sont finis. Vu que $A = \bigcup_n A \cap K_n$, l'ensemble A est une réunion dénombrable d'ensembles finis. Il est donc dénombrable. □

10.3.11 Recouvrement par des intervalles ouverts

Soit un ensemble E et un ensemble $\mathcal{A}$ de parties de E . Soit $A \in \mathcal{A}$. Nous aimerions savoir quelles sont les éléments de $\mathcal{A}$ qui sont atteignables en partant de A et en ne « sautant » que d'intersection en intersection.

19. Définition 7.29.

Nous notons $\mathcal{A} = \{B_i\}_{i \in I}$ où I est un ensemble d'indices (un ensemble quelconque).

$$s_1(A) = \{i \in I \text{ tel que } B_i \cap A \neq \emptyset\} \quad (10.67a)$$

$$\sigma_1(A) = \bigcup_{B \in s_1(A)} B. \quad (10.67b)$$

Et ensuite :

$$s_{k+1}(A) = \{i \in I \text{ tel que } B_i \cap \sigma_k(A) \neq \emptyset\} \quad (10.68a)$$

$$\sigma_{k+1}(A) = \bigcup_{B \in s_{k+1}(A)} B \quad (10.68b)$$

Lemme 10.53.

Soient un intervalle A de $\mathbb{R}$ et $\mathcal{A} = \{I_i\}_{i=1, \dots, N}$ un recouvrement de A par des intervalles ouverts. Si $I_1 \cap A \neq \emptyset$ alors

$$(1) \quad \sigma_N = \sigma_{N+1}$$

$$(2) \quad A \subset \sigma_N(I_1).$$

Démonstration. Si $\sigma_{k+1} = \sigma_k$, alors tous les σ_{k+l} sont identiques. De plus si $\sigma_{k+1} \neq \sigma_k$, alors σ_{k+1} contient au moins un élément de plus que σ_k . Donc $\text{Card}(\sigma_k) \geq k$ et en particulier $N \leq \text{Card}(\sigma_N) \leq N$. Cela prouve le premier point.

L'ensemble $\sigma_N(I_1)$ est une union d'ouverts et est donc un ouvert. Quitte à renuméroter nous écrivons

$$\sigma_N(I_1) = I_1 \cup \dots \cup I_n. \quad (10.69)$$

L'ensemble

$$\tau = \bigcup_{k=n+1}^N I_k \quad (10.70)$$

est ouvert et est disjoint de $\sigma_N(I_1)$ parce que si I_l ($l \geq n+1$) intersectait $\sigma_N(I_1)$, nous aurions $l \in s_{N+1}$ ou encore $I_l \subset \sigma_{N+1} \setminus \sigma_N$.

Donc τ et σ_N sont deux ouverts disjoints qui recouvrent A . Vu que A est un intervalle, il est connexe²⁰. Donc soit $A \subset \tau$ soit $A \subset \sigma_N$. Comme $I_1 \cap A \neq \emptyset$ nous sommes dans le cas $A \subset \sigma_N$. $\square$

Lemme 10.54.

Soit $x \in \mathbb{R}$. Si $\mathcal{A} = \{I_s\}_{s \in S}$ est un ensemble d'intervalles contenant x , alors $I = \bigcup_{s \in S} I_s$ est un intervalle²¹.

Démonstration. Soient $a, b \in I$ (nous supposons $a < b$). Nous devons prouver que $[a, b] \subset I$. Pour cela nous considérons $y \in [a, b]$; il y a deux possibilités : soit $y < x$ soit $y > x$ (si $y = x$ alors $y \in I_s$).

Si $y < x$, alors $a \leq y < x$ et donc $y \in I_s$. Si $y > x$, alors $x < y \leq b$ et $y \in I_t$. $\square$

Proposition 10.55 ([232, 233]).

Un ouvert de $\mathbb{R}$ peut s'écrire comme union au plus dénombrable d'intervalles ouverts disjoints.

Plus précisément, si $\mathcal{O}$ est un ouvert de $\mathbb{R}$, il existe un ensemble $\mathcal{F} = \{I_s\}_{s \in S}$ où

(1) Chaque I_s est un intervalle ouvert contenu dans $\mathcal{O}$,

(2) Pour $s, t \in S$, si $I_s \neq I_t$, alors $I_s \cap I_t = \emptyset$.

(3) S est dénombrable,

20. Définition 7.44 et proposition 10.47.

21. Définition 1.15.

Démonstration. Pour $x \in \mathcal{O}$, nous définissons J_x comme étant l'union de tous les intervalles ouverts contenus dans $\mathcal{O}$ et contenant x . Les J_x ne sont pas vides parce qu'ils contiennent toujours une boule centrée en x ²².

En tant que union d'intervalles, J_x est un intervalle par le lemme 10.54. De plus, J_x est ouvert parce que toute union d'ouverts est ouverte.

Nous notons $\mathcal{A}$ l'ensemble des intervalles ouverts contenus dans $\mathcal{O}$, et

$$\mathcal{A}_x = \{I \in \mathcal{A} \text{ tel que } x \in I\}. \quad (10.71)$$

Si $y \in J_x$, alors $J_x = J_y$ Vu que $y \in J_x$, nous pouvons considérer $J = J_x \cap J_y$. Nous avons

$$J_y = \bigcup_{I \in \mathcal{A}_y} I \subset \bigcup_{I \in \mathcal{A}_y} \underbrace{(I \cup J)}_{\in \mathcal{A}_x} \subset \bigcup_{I \in \mathcal{A}_x} I = J_x. \quad (10.72)$$

L'inclusion dans l'autre sens s'obtient en écrivant la même chose en remplaçant x par y et vice-versa.

Les J_x sont disjoints Nous prouvons à présent que pour $x, y \in m\mathcal{O}$, nous avons $J_x = J_y$ ou $J_x \cap J_y = \emptyset$. En effet si $a \in J_x \cap J_y$, alors $J_a = J_x$ et $J_a = J_y$. Donc $J_x = J_y$.

Dénombrable C'est le moment d'écrire $\mathcal{F} = \{J_x\}_{x \in \mathcal{O}}$. Vu que tout intervalle contient au moins un rationnel (proposition 10.14), nous avons aussi

$$\mathcal{F} = \{J_x\}_{x \in \mathcal{O}} = \{J_q\}_{q \in \mathbb{Q} \cap \mathcal{O}}. \quad (10.73)$$

Cet ensemble $\mathcal{F}$ vérifie les conditions demandées.

□

10.3.12 Connexité par arcs

Définition 10.56.

Une partie A d'un espace topologique est **connexe par arcs** si pour tout $a, b \in A$, il existe une application continue $\gamma: [0, 1] \rightarrow A$ telle que $\gamma(0) = a$ et $\gamma(1) = b$.

10.57.

Un exemple d'ensemble connexe mais pas connexe par arcs est donné par la proposition 21.56. L'idée de cet exemple est de construire un ensemble en deux parties reliées par un chemin de longueur infinie.

Un espoir fou nous prend alors de croire que nous pouvons produire un exemple plus simple avec $\mathbb{R} \cup \{\infty\}$ parce que, dans cet ensemble, 1 et ∞ sont reliés par un chemin de longueur infinie. La proposition 12.56 nous montrera que non.

10.3.13 Un peu de connexité par arcs

Principe. L'idée est de considérer une propriété topologique (invariante par homéomorphisme) et de voir qu'elle est vérifiée par les ouverts de $\mathbb{R}^2$ mais pas ceux du cône.

Lemme 10.58.

Si V est un voisinage de 0 sur le cône C , alors $V \setminus \{0\}$ n'est pas connexe, donc n'est pas connexe par arc.

Démonstration. Le cône C est la réunion de $C^+ = C \cap (\mathbb{R}^2 \times \mathbb{R}_0^+)$ et $C^- = C \cap (\mathbb{R}^2 \times \mathbb{R}_0^-)$ car le seul point à cote nulle est la singularité 0. Dès lors, V s'écrit comme l'union disjointe de $V \cap C^+$ et $V \cap C^-$, qui sont non-vides. Donc V n'est pas connexe. □

22. C'est la définition 7.88 de la topologie métrique.

On procède en deux étapes, en montrant d'abord qu'il existe des points en « dessous » et au « dessus » de 0, puis en essayant de les relier. Comme V est un voisinage de 0, il existe un ouvert U du cône centré en 0 inclus à V . Donc par définition de la topologie induite, et puisque les boules forment une base de la topologie de $\mathbb{R}^3$, il existe une boule B centrée en 0 dont U est la trace sur C , telle que $0 \in (B \cap C) \subset V$. On choisit $p = (p_x, p_y, p_z) \in (B \cap C)$, et en considérant $p' = (p_x, p_y, -p_z)$ on a ainsi trouvé deux points qui vérifient $p_z > 0$ et $p'_z < 0$ (au besoin, on les échange).

(1) Supposons que $V \setminus \{0\}$ soit connexe par arc. Donc il existe un chemin

$$\gamma : [0; 1] \rightarrow V \setminus \{0\} : t \mapsto (\gamma_x(t), \gamma_y(t), \gamma_z(t))$$

qui relie p à p' et qui vérifie $\gamma_z(0) = p_z > 0$ et $\gamma_z(1) = -p_z < 0$. Or $\gamma_z(t)$ est une fonction continue (car γ est continu), donc par le théorème des valeurs intermédiaires, il existe $\bar{t}$ qui vérifie $\gamma_z(\bar{t}) = 0$. Or le seul point de C dont la cote (coordonnée en z) soit nulle est le sommet 0 qui n'est pas dans $V \setminus \{0\}$, d'où la contradiction.

Soient deux espaces topologiques E et F , et $f : E \rightarrow F$ un homéomorphisme. Pour toute partie A de E , l'espace $E \setminus A$ est homéomorphe au sous-espace $F \setminus f(A)$ via la restriction $f|_{E \setminus A}$.

Lemme 10.59.

Soient deux espaces topologiques E et F , et $f : E \rightarrow F$ un homéomorphisme. E est connexe par arc si et seulement si F l'est.

Démonstration. On montre en réalité que l'image d'un connexe par arc par une application continue est un connexe par arc, ce qui implique chaque sens de l'équivalence de l'énoncé.

Soient p et q des points de F . Il existe un chemin reliant un antécédent de p et un antécédent de q (dans E). L'image de ce chemin est un chemin reliant p et q (dans F) puisque composé d'applications continues. $\square$

Lemme 10.60.

Une sphère de $\mathbb{R}^n$ est connexe par arc si $n > 1$

Démonstration. On voit qu'un cercle est connexe par arc car on a un paramétrage en sinus et cosinus. Pour une sphère S de centre a en dimension $n > 2$, on se donne p et q sur S et on définit P le plan affine passant par a , p et q . Alors $P \cap S$ est un cercle, donc on peut relier p à q par un chemin dans cette intersection.

Pour voir sur une formule que $P \cap S$ est un cercle, on peut écrire $x - a = \lambda(a - p) + \mu(a - q)$ l'équation (en x) du plan P , et $|x - a|^2 = R^2$ l'équation (en x) de la sphère. En injectant, on obtient une équation du second degré en λ, μ qui se révèle être l'équation d'un cercle à une transformation affine près. $\square$

Lemme 10.61.

Un ouvert connexe par arc dans $\mathbb{R}^n$ ($n \geq 2$) reste connexe par arc même si on lui enlève un point.

Démonstration. En effet, soit U un tel ouvert connexe par arc, et p un point de U . Soient x et y sur $U \setminus \{p\}$. Il existe un chemin γ de x à y . Si le chemin ne passe pas par p , c'est gagné. Si il passe par p , on choisit une boule B fermée (de rayon non-nul) centrée en p qui ne contient ni x ni y . On note

$$E = \gamma^{-1}(B) \subset [0; 1]$$

c'est un ensemble compact (fermé, par continuité de γ , et borné) dont on regarde le maximum $\bar{t}$ et le minimum $\underline{t}$.

Il reste enfin à définir un chemin entre p et q par morceaux

- (1) Les points p et $\gamma(\underline{t})$ sont reliés par γ ,
- (2) Par connexité par arc, il existe un chemin sur la sphère qui relie $\gamma(\underline{t})$ à $\gamma(\bar{t})$,
- (3) et enfin $\gamma(\bar{t})$ et q sont reliés via γ ;

ce qui achève la construction d'un chemin continu entre p et q . $\square$

Pour conclure l'exercice, par l'absurde, on prend un voisinage connexe et ouvert V de 0 dans le cône, homéomorphe à un ouvert connexe U de $\mathbb{R}^2$. Or $V \setminus \{0\}$ n'est pas connexe par arc, alors que l'ouvert dont on retire un point reste connexe par arc. C'est impossible, donc l'homéomorphisme n'existe pas, et le cône n'est pas une variété de dimension 2.

10.3.14 Des exemples

Exemple 10.62.

Nous étudions l'exemple suivant :

$$A_1 = \{(x, y) \in \mathbb{R}^2 \mid 2y^2 + 4y + 2 < x \leq \sqrt{4 - y^2}, y \in [-1.5, 0.5]\}. \quad (10.74)$$

On commence par tracer la parabole $x = 2y^2 + 4y + 2$, la circonférence $x^2 + y^2 = 4$ et les droites $y = -1.5$ et $y = 1/2$. On voit tout de suite que l'aire délimitée par les quatre courbes est donnée par l'union de deux parties. Dans la première $\sqrt{4 - y^2} \leq x \leq 2y^2 + 4y + 2$, $y \in [0, 0.5]$ et dans l'autre $2y^2 + 4y + 2 \leq x \leq \sqrt{4 - y^2}$, $y \in [-1.5, 0]$. L'ensemble A_1 est contenu dans la deuxième, 10.1. L'intérieur de A_1 est donné par $\text{Int}(A_1) = \{(x, y) \in \mathbb{R}^2 \mid 2y^2 + 4y + 2 < x < \sqrt{4 - y^2}, y \in]-1.5, 0[\}$, et sa frontière est l'union de 3 morceaux de courbe ℓ_1, ℓ_2, ℓ_3 :

$$\begin{aligned} \ell_1 &= \{(x, y) \mid x = 2y^2 + 4y + 2, y \in [-1.5, 0]\} \\ \ell_2 &= \{(x, y) \mid x = \sqrt{4 - y^2}, y \in [-1.5, 0]\} \\ \ell_3 &= \{(x, y) \mid x \in [0.5, \sqrt{7/4}], y = -1.5\}. \end{aligned} \quad (10.75)$$

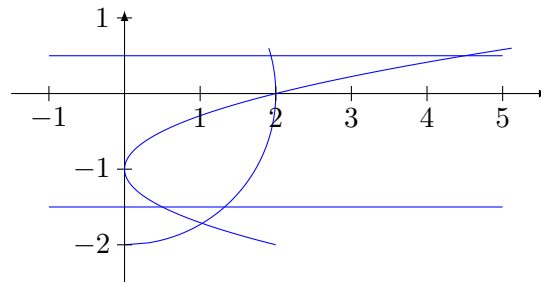


FIGURE 10.1 –

△

Exemple 10.63.

Nous étudions

$$A_3 = \mathbb{N} \times \mathbb{Q} = \{(x, y) \in \mathbb{R}^2 \mid x \in \mathbb{N}, y \in \mathbb{Q}\}. \quad (10.76)$$

L'ensemble A_3 n'est pas ouvert, ni fermé, ni borné dans la topologie de $\mathbb{R}^2$. En fait, comme on a vu dans les exercices du cours, $\mathbb{Q}$ a intérieur vide et sa fermeture est $\mathbb{R}$. L'ensemble $\mathbb{N}$, par contre est fermé et non borné. On peut remarquer que tous les points de $\mathbb{N}$ sont points isolés. La fermeture de A_3 est alors $\mathbb{N} \times \mathbb{R}$ et son intérieur est vide. On peut dessiner la fermeture de cet ensemble comme une famille de droites verticales $x = n$, pour tout n dans $\mathbb{N}$. △

Exemple 10.64.

Nous étudions l'ensemble

$$A_3 = \{(t, 2t) \in \mathbb{R}^2 \mid t \in [0, 1]\}. \quad (10.77)$$

L'ensemble A_3 est un petit segment de droite. Son intérieur est vide parce que toute boule centrée en un point de la droite intersecte l'extérieur de la droite. Son adhérence et sa frontière sont A_3 lui-même parce que nous considérons les valeurs de t dans $[0, 1]$ qui est un intervalle fermé. Si l'intervalle avait été ouvert, l'adhérence et la frontière auraient été trouvés en fermant :

$$\overline{\{(t, 2t) \text{ tels que } t \in [0, 1[\}} = \{(t, 2t) \text{ tels que } t \in [0, 1]\} \quad (10.78)$$

Étant donné que son adhérence est égal à lui-même, cet ensemble est fermé (et donc pas ouvert). Il est également borné parce qu'il est contenu dans une boule de rayon 3. △

Exemple 10.65.

Nous étudions l'ensemble

$$A_4 = \mathbb{Q} \times \mathbb{Q} = \{(x, y) \in \mathbb{R}^2 \mid x \in \mathbb{Q}, y \in \mathbb{Q}\}. \quad (10.79)$$

Dans $\mathbb{R}$ nous savons que $\bar{\mathbb{Q}} = \mathbb{R}$, $\text{Int}(\mathbb{Q}) = \emptyset$ et $\partial\mathbb{Q} = \mathbb{R}$ parce que toute boule centrée en un rationnel contient un irrationnel, et inversement, toute boule centrée en un irrationnel contient un rationnel. Dans $\mathbb{R}^2$ nous avons le même phénomène parce dans la boule $B((p, q), r)$ avec $(p, q) \in \mathbb{Q} \times \mathbb{Q}$, se trouvent en particulier les points de la forme (p, x) avec $x \in B(q, r) \subset \mathbb{R}$. Évidemment, certains de ces x ne sont pas dans $\mathbb{Q}$ et par conséquent, la boule $B((p, q), r)$ contient les points $(p, x) \notin \mathbb{Q} \times \mathbb{Q}$.

De la même manière, si (x, y) est un point de $\mathbb{R}^2$, dans toute boule centrée en (x, y) , il y aura un élément de $\mathbb{Q}^2$.

Par conséquent, $\text{Int}(\mathbb{Q} \times \mathbb{Q}) = \emptyset$, $\overline{\mathbb{Q} \times \mathbb{Q}} = \mathbb{R} \times \mathbb{R}$ et $\partial(\mathbb{Q} \times \mathbb{Q}) = \mathbb{R}^2$.

Il n'est ni ouvert ni fermé (parce qu'il n'est égal ni à son intérieur ni à sa fermeture). Il n'est pas borné non plus parce qu'il existe des nombres rationnels arbitrairement grands. $\triangle$

Exemple 10.66.

Nous étudions l'ensemble

$$A_5 = \{(x, y) \in \mathbb{R}^2 \mid x \in]0, 1[, \sin \frac{1}{x} < y < 3\}. \quad (10.80)$$

La fonction $x \mapsto \sin(\frac{1}{x})$ est une des fonctions dont le graphe doit être connu. La figure 10.2 montre la situation. Comme d'habitude, il est fortement recommandé de refaire le dessin soi-même.

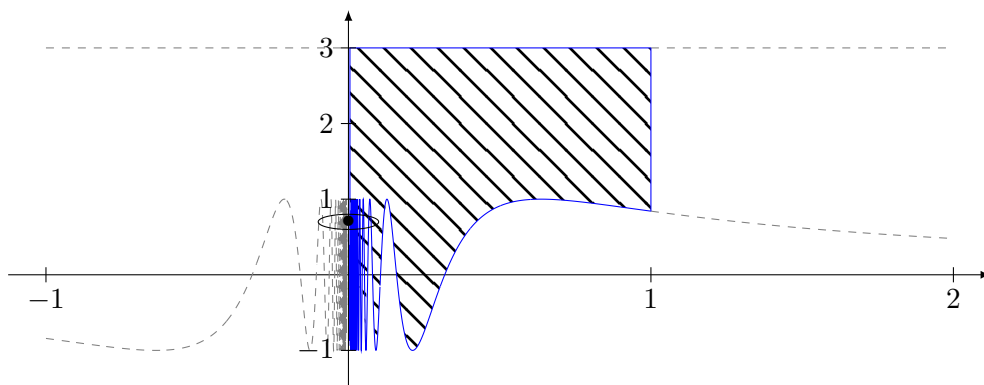


FIGURE 10.2 – Les points qui sont sur l'axe vertical entre 0 et 3 sont sur la frontière, mais pas dans l'ensemble A_5 .

L'ensemble A_5 est ouvert parce que les conditions $x \in]0, 1[$ et $\sin \frac{1}{x} < y < 3$ sont des conditions « ouvertes » au sens où si un point les vérifie, alors on peut trouver une boule dans laquelle ces conditions restent vérifiées. Cela prouve que $\text{Int}(A_5) = A_5$.

La fermeture de A_5 contient en outre les points tels que $\sin \frac{1}{x} = y$ entre $x = 0$ et $x = 1$ (les bornes étant incluses) ainsi que les points des trois segments de droites suivants :

$$\begin{aligned} &\{(0, y) \text{ tels que } y \in [-1, 3]\} \\ &\{(x, 3) \text{ tels que } x \in [0, 1]\} \\ &\{(1, y) \text{ tels que } y \in [\sin(1), 3]\}. \end{aligned} \quad (10.81)$$

La frontière est composée de ces trois segments et du graphe de la fonction $\sin \frac{1}{x}$ entre 0 et 1.

L'ensemble A_5 est borné parce qu'il est contenu par exemple dans la boule centrée en $(0, 0)$ et de rayon 10. Il est ouvert et donc pas fermé. $\triangle$

Exemple 10.67.

Nous étudions l'ensemble

$$A_6 = \bigcup_{n \in \mathbb{N}_0} \left\{ \left(\frac{1}{n}, y \right) \mid y \in [0, 1] \right\}. \quad (10.82)$$

L'ensemble A_6 est une union infinie de segments de droites verticaux, voir figure 10.3

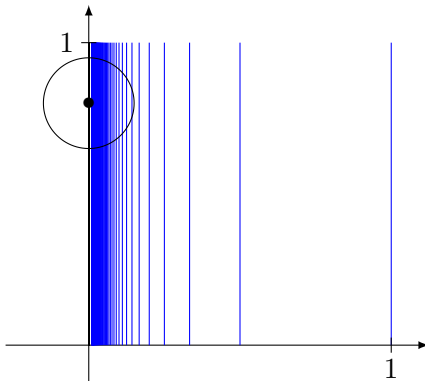


FIGURE 10.3 – Le segment sur l'axe vertical entre $y = 0$ et $y = 1$ fait partie de l'adhérence et de la frontière, mais pas de l'ensemble A_6 lui-même.

L'intérieur est vide parce qu'autour de tout réel de la forme $\frac{1}{n}$, il y a un réel qui n'est pas de cette forme. En ce qui concerne la frontière et l'adhérence, il s'agit de l'union de tous ces segments plus le segment en $x = 0$.

En effet, la boule de rayon r autour du point $(0, y)$ le point $(\frac{1}{n}, y)$ avec n assez grand pour que $\frac{1}{n} < r$. $\triangle$

10.3.15 Topologie de la droite réelle complétée

Nous introduisons l'ensemble $\bar{\mathbb{R}} = \mathbb{R} \cup \{\pm\infty\}$. À présent les symboles $+\infty$ et $-\infty$ n'ont aucune signification particulière; il s'agit seulement de deux éléments que nous ajoutons à $\mathbb{R}$ pour former un ensemble que nous notons $\bar{\mathbb{R}}$.

Pas plus tard qu'immédiatement nous leur donnons une signification en définissant une topologie sur $\bar{\mathbb{R}}$. Les ouverts sur $\bar{\mathbb{R}}$ sont

- (1) tous les ouverts de $\mathbb{R}$,
- (2) les intervalles de la forme $]-\infty, a[$ pour tous les $a \in \mathbb{R}$,
- (3) les intervalles de la forme $]a, +\infty[$ pour tous les $a \in \mathbb{R}$,
- (4) la topologie engendrée par toutes ces parties de $\bar{\mathbb{R}}$.

Par construction, les boules de $\mathbb{R}$ et les intervalles $]-\infty, a[$ et $]a, +\infty[$ forment une base de topologie pour $\bar{\mathbb{R}}$.

Si f est une fonction $f: \mathbb{R} \rightarrow \mathbb{R}$, que signifie $\lim_{x \rightarrow \infty} f(x)$? Il s'agit de considérer la fonction élargie

$$\begin{aligned} \tilde{f}: \bar{\mathbb{R}} &\rightarrow \bar{\mathbb{R}} \\ x &\mapsto \begin{cases} f(x) & \text{si } x \in \mathbb{R} \\ 0 & \text{si } x = \pm\infty. \end{cases} \end{aligned} \quad (10.83)$$

Ensuite, c'est la définition topologie usuelle de la limite. Notons que les limites en a ne dépendent pas de la valeur effective de f en a , donc le prolongement par 0 est sans conséquences. Nous pouvions tout aussi bien prolonger par 4.

Le même raisonnement tient pour donner un sens à $\lim_{x \rightarrow a} f(x) = \pm\infty$.

10.3.16 Quelques mots à propos de la droite réelle complétée

Définition 10.68.

La **droite réelle complétée** est l'ensemble $\mathbb{R} \cup \{\pm\infty\}$ où $\pm\infty$ sont deux nouveaux éléments. Nous la notons $\overline{\mathbb{R}}$ pour des raisons que nous verrons à peine plus bas.

Cette définition ne servirait à rien si nous n'y mettions pas une topologie pour positionner les éléments $\pm\infty$ par rapport à ceux qui existaient déjà dans $\mathbb{R}$.

Définition 10.69 (Topologie sur $\overline{\mathbb{R}}$).

La topologie sur $\overline{\mathbb{R}}$ est celle sur $\mathbb{R}$ à laquelle nous ajoutons les voisinages de $\pm\infty$ de la façon suivante. Une partie V de $\overline{\mathbb{R}}$ est un voisinage de $+\infty$ s'il existe $m > 0$ tel que $]m, +\infty] \subset V$.

Le lemme suivant justifie la notation $\overline{\mathbb{R}}$ pour la droite réelle complétée²³.

Lemme 10.70.

L'adhérence²⁴ de $\mathbb{R}$ dans $\overline{\mathbb{R}}$ est $\overline{\mathbb{R}}$.

Démonstration. Il suffit de prouver que $+\infty$ et $-\infty$ sont dans l'adhérence de $\mathbb{R}$. Nous le faisons pour $+\infty$. Ce n'est pas très compliqué : si A est un ouvert contenant $+\infty$, il contient une partie de la forme $]a, +\infty]$, et donc contient des éléments de $\mathbb{R}$. $\square$

Pour la suite nous utilisons la notation (pratique en probabilité)

$$\{f < a\} = \{x \in S \text{ tel que } f(x) < a\}. \quad (10.84)$$

10.4 Continuité

La définition de fonction continue est la définition 7.75. Dans le cas d'une fonction $f: \mathbb{R} \rightarrow \mathbb{R}$, elle devient ceci.

Proposition 10.71.

Soient $A \subset \mathbb{R}$ et $a \in A$. La fonction $f: A \rightarrow \mathbb{R}$ est **continue en a** si et seulement si pour tout $\epsilon > 0$, il existe un $\delta > 0$ tel que si $x \in B(a, \delta) \cap A$ alors $|f(x) - f(a)| \leq \epsilon$.

Nous allons maintenant étudier quelques conséquences de la continuité sur $\mathbb{R}$.

- (1) D'abord on voit que la continuité n'a été définie qu'en un point. On peut dire que la fonction f est continue en tel point donné, mais nous n'avons pas dit ce qu'est une fonction continue dans son ensemble.
- (2) Le théorème 7.79 nous précise que si I est un intervalle de $\mathbb{R}$, la fonction f est continue sur I si et seulement si elle est continue en chaque point de I .
- (3) Comme la définition de f continue en a fait intervenir $f(x)$ pour tous les x pas trop loin de a , il faut au moins déjà que f soit définie sur ces x . En d'autres termes, dire que f est continue en a demande que f existe sur un intervalle autour de a .
Ceci couplé à la définition précédente laisse penser qu'il est surtout intéressant d'étudier les fonctions qui sont continues sur un intervalle.
- (4) L'intuition comme quoi une fonction continue doit pouvoir être tracée sans lever la main correspond aux fonctions continues sur des intervalles. Au moins sur l'intervalle où elle est continue, elle est traçable en un morceau.

Exemple 10.72.

Il est très possible d'être continue en un seul point. Par exemple la fonction

$$f(x) = x(1 - \mathbb{1}_{\mathbb{Q}}(x)) \quad (10.85)$$

23. Mais ne justifie pas le qualificatif « complété » parce que l'espace métrique $\mathbb{R}$ était déjà complet.

24. Définition 7.24.

où $\mathbb{1}_{\mathbb{Q}}$ est la fonction indicatrice de $\mathbb{Q}$ dans $\mathbb{R}$. $\triangle$

Proposition 10.73.

Si $f: \mathbb{R} \rightarrow \mathbb{R}$ est continue au point $a \in \mathbb{R}$ et si $f(a) \neq 0$, alors il existe un voisinage de a sur lequel f ne s'annule pas.

Démonstration. Si f s'annulait sur tout voisinage de a (mais pas en a lui-même), nous aurions, pour tout n un réel

$$x_n \in B\left(a, \frac{1}{n}\right) \setminus \{a\} \quad (10.86)$$

tel que $f(x_n) = 0$. Cela donnerait une suite $x_n \rightarrow a$ avec $f(x_n) \rightarrow 0$, ce qui contredit la continuité de f en a en vertu de la proposition 7.857.160 sur la continuité séquentielle en un point. $\square$

Notons que ce résultat se généralise beaucoup : si f est continue et pas égale à r en a , alors elle continue à n'être pas égale à r dans un voisinage de a .

10.4.1 Opération sur la continuité

Nous allons démontrer maintenant une série de petits résultats qui permettent de simplifier la démonstration de la continuité de fonctions.

Théorème 10.74.

Si la fonction f est continue au point a , alors la fonction λf est également continue en a .

Démonstration. Soit $\epsilon > 0$. Nous avons besoin d'un $\delta > 0$ tel que pour chaque x à moins de δ de a , la fonction λf soit à moins de ϵ de $(\lambda f)(a) = \lambda f(a)$. Étant donné que la fonction f est continue en a , on sait déjà qu'il existe un δ_1 (nous notons δ_1 afin de ne pas confondre ce nombre dont on est sûr de l'existence avec le δ que nous sommes en train de chercher) tel que

$$(|x - a| \leq \delta_1) \Rightarrow |f(x) - f(a)| \leq \epsilon_1.$$

Hélas, ce δ_1 n'est pas celui qu'il faut parce que nous travaillons avec λf au lieu de f , ce qui fait qu'au lieu d'avoir $|f(x) - f(a)|$, nous avons $|\lambda f(x) - \lambda f(a)| = |\lambda| \cdot |f(x) - f(a)|$. Ce que δ_1 fait avec (λf) , c'est

$$(|x - a| \leq \delta_1) \Rightarrow |(\lambda f)(x) - (\lambda f)(a)| \leq |\lambda| \epsilon_1.$$

Ce que nous apprend la continuité de f , c'est que pour chaque choix de ϵ_1 , on a un δ_1 qui fait cette implication. Comme cela est vrai pour chaque choix de ϵ_1 , essayons avec $\epsilon_1 = \epsilon/|\lambda|$ pour voir ce que ça donne. Nous avons donc un δ_1 qui fait

$$(|x - a| \leq \delta_1) \Rightarrow |(\lambda f)(x) - (\lambda f)(a)| \leq |\lambda| \epsilon_1 = \epsilon.$$

Ce δ_1 est celui qu'on cherchait. $\square$

Théorème 10.75.

Si f et g sont deux fonctions continues en a , alors la fonction $f + g$ est également continue en a .

Démonstration. La continuité des fonctions f et g au point a fait en sorte que pour tout choix de ϵ_1 et ϵ_2 , il existe δ_1 et δ_2 tels que

$$(|x - a| \leq \delta_1) \Rightarrow |f(x) - f(a)| \leq \epsilon_1.$$

et

$$(|x - a| \leq \delta_2) \Rightarrow |g(x) - g(a)| \leq \epsilon_2.$$

La quantité que nous souhaitons analyser est $|f(x) + g(x) - f(a) - g(a)|$. Tout le jeu de la démonstration de la continuité est de triturer cette expression pour en tirer quelque chose en termes de ϵ_1 et ϵ_2 . Si nous supposons avoir pris $|x - a|$ plus petit en même temps que δ_1 et que δ_2 , nous avons

$$|f(x) + g(x) - f(a) - g(a)| \leq |f(x) - f(a)| + |g(x) - g(a)| \leq \epsilon_1 + \epsilon_2$$

en utilisant la formule générale $|a+b| \leq |a|+|b|$. Maintenant si on choisit ϵ_1 et ϵ_2 tels que $\epsilon_1 + \epsilon_2 < \epsilon$, et les δ_1, δ_2 correspondants, on a

$$|f(x) + g(x) - f(a) - g(a)| \leq \epsilon,$$

pourvu que $|x - a|$ soit plus petit que δ_1 et δ_2 . Le bon δ à prendre est donc le minimum de δ_1 et δ_2 qui eux-mêmes sont donnés par un choix de ϵ_1 et ϵ_2 tels que $\epsilon_1 + \epsilon_2 \leq \epsilon$. $\square$

Pour résumer ces deux théorèmes, on dit que si f et g sont continues en a , alors la fonction $\alpha f + \beta g$ est également continue en a pour tout $\alpha, \beta \in \mathbb{R}$.

Proposition 10.76.

Soient des parties Ω_f et Ω_g dans $\mathbb{R}$. Soient $f: \Omega_f \rightarrow \mathbb{R}$ ainsi que $g: \Omega_g \rightarrow \mathbb{R}$ telles que

- (1) g est continue en a et vaut $g(a) = \ell$.
- (2) f est continue en ℓ et vaut $f(\ell) = b$.
- (3) $g(\Omega_g) \subset \Omega_f$.

Alors $f \circ g$ est continue en a .

Démonstration. Soit $\epsilon > 0$. La continuité de f dit que il existe $\eta > 0$ tel que

$$y \in B(\ell, \eta) \cap \Omega_f \Rightarrow |f(y) - f(\ell)| < \epsilon. \quad (10.87)$$

La continuité de g donne $\delta > 0$ tel que

$$x \in B(a, \delta) \cap \Omega_g \Rightarrow |g(x) - g(a)| < \eta. \quad (10.88)$$

Si $x \in B(a, \delta) \cap \Omega_g$, alors $g(x) \in B(\ell, \eta) \cap \Omega_f$. Donc

$$|(f \circ g)(x) - f(\ell)| < \epsilon. \quad (10.89)$$

Mais $f(\ell) = (f \circ g)(a)$. Tout cela est la continuité de $f \circ g$ en a . $\square$

Parmi les propriétés immédiates de la continuité d'une fonction, nous avons ceci qui est souvent bien utile.

Corolaire 10.77.

Si la fonction f est continue en a et si $f(a) > 0$, alors f est positive sur un intervalle autour de a .

Démonstration. Prenons $\epsilon < f(a)$ et voyons²⁵ ce que la continuité de f en a nous offre : il existe un δ tel que

$$(|x - a| \leq \delta) \Rightarrow |f(x) - f(a)| \leq \epsilon < f(a).$$

Nous en retenons que sur un intervalle (de largeur δ), nous avons $|f(x) - f(a)| \leq f(a)$. Par hypothèse, $f(a) > 0$, donc si $f(x) < 0$, alors la différence $f(x) - f(a)$ donne un nombre encore plus négatif que $-f(a)$, c'est-à-dire que $|f(x) - f(a)| > f(a)$, ce qui est contraire à ce que nous venons de démontrer. D'où la conclusion que $f(x) > 0$. $\square$

10.4.2 La fonction la moins continue du monde

Parmi les exemples un peu sales de fonctions non continues, il y a celle-ci :

$$\chi_{\mathbb{Q}}(x) = \begin{cases} 1 & \text{si } x \in \mathbb{Q} \\ 0 & \text{sinon.} \end{cases}$$

25. ici, nous insistons sur le fait que nous prenons ϵ strictement plus petit que $f(a)$.

Par exemple, $\chi_{\mathbb{Q}}(0) = 1$, et²⁶ $\chi_{\mathbb{Q}}(\pi) = \chi_{\mathbb{Q}}(\sqrt{2}) = 0$. Malgré que $\chi_{\mathbb{Q}}(0) = 1$, il n'existe *aucun* voisinage de 1 sur lequel la fonction reste proche de 1, parce que tout voisinage va contenir au moins un irrationnel. À chaque millimètre, cette fonction fait une infinité de bonds !

Cette fonction n'est donc continue nulle part.

À partir de là, nous pouvons construire la fonction suivante qui n'est continue qu'en un point :

$$f(x) = x\chi_{\mathbb{Q}}(x) = \begin{cases} x & \text{si } x \in \mathbb{Q} \\ 0 & \text{sinon.} \end{cases}$$

Cette fonction est continue en zéro. En effet, prenons $\delta > 0$; il nous faut un ϵ tel que $|x| \leq \epsilon$ implique $f(x) \leq \delta$ parce que $f(0) = 0$. Bon ben prendre simplement $\epsilon = \delta$ nous contente. Cette fonction est donc très facilement continue en zéro.

Et pourtant, dès que l'on s'écarte un tant soit peu de zéro, elle fait des bonds une infinité de fois par millionième de millimètre ! Cette fonction est donc la plus discontinue du monde en tous les points sauf un (zéro) où elle est une fonction continue !

10.4.3 Approche topologique

Nous avons vu que sur tout ensemble métrique, nous pouvons définir ce qu'est un ouvert : c'est un ensemble qui contient une boule ouverte autour de chacun de ses points. Quand on est dans un ensemble ouvert, on peut toujours un peu se déplacer sans sortir de l'ensemble.

Le théorème suivant est une très importante caractérisation des fonctions continues (de $\mathbb{R}$ dans $\mathbb{R}$) en termes de topologie, c'est-à-dire en termes d'ouverts.

Théorème 10.78.

Si I est un intervalle ouvert contenu dans $\text{dom } f$, alors f est continue sur I si et seulement si pour tout ouvert $\mathcal{O}$ dans $\mathbb{R}$, l'image inverse $f|_I^{-1}(\mathcal{O})$ est ouvert.

Par abus de langage, nous exprimons souvent cette condition par « une fonction est continue si et seulement si l'image inverse de tout ouvert est un ouvert ».

Démonstration. Dans un premier temps, nous allons transformer le critère de continuité en termes de boules ouvertes, et ensuite, nous passerons à la démonstration proprement dite. Le critère de continuité de f au point x dit que

$$\forall \delta > 0, \exists \epsilon > 0 \text{ tel que } (|x - a| < \epsilon) \Rightarrow |f(x) - f(a)| < \delta. \quad (10.90)$$

Cette condition peut être exprimée sous la forme suivante :

$$\forall \delta > 0, \exists \epsilon \text{ tel que } a \in B(x, \epsilon) \Rightarrow f(a) \in B(f(x), \delta),$$

ou encore

$$\forall \delta > 0, \exists \epsilon \text{ tel que } f(B(x, \epsilon)) \subset B(f(x), \delta). \quad (10.91)$$

Jusque ici, nous n'avons fait que du jeu de notations. Nous avons exprimé en termes de topologie des inégalités analytiques. La condition (10.91) est le plus souvent utilisée comme définition de la continuité d'une fonction en x , lorsque le contexte ne demande pas de définitions plus générales. Si tel est le choix, il faut pouvoir retrouver (10.90) à partir de (10.91).

Passons maintenant à la démonstration proprement dite du théorème.

D'abord, supposons que f est continue sur I , et prenons $\mathcal{O}$, un ouvert quelconque. Le but est de prouver que $f|_I^{-1}(\mathcal{O})$ est ouvert. Pour cela, nous prenons un point $x_0 \in f|_I^{-1}(\mathcal{O})$ et nous allons trouver un ouvert autour ce point contenu dans $f|_I^{-1}(\mathcal{O})$. Nous écrivons $y_0 = f(x_0)$. évidemment, $y_0 \in \mathcal{O}$, donc on a une boule autour de y_0 qui est contenue dans $\mathcal{O}$, soit donc $\delta > 0$ tel que

$$B(y_0, \delta) \subset \mathcal{O}.$$

26. Pour prouver que $\sqrt{2}$ n'est pas rationnel, c'est pas trop compliqué, mais pour prouver que π ne l'est pas non plus, il faudra encore manger de la soupe.

Par hypothèse, f est continue en x_0 , et nous pouvons donc y appliquer le critère (10.91). Il existe donc $\epsilon > 0$ tel que

$$f(B(x_0, \epsilon)) \subset B(f(x_0), \delta) \subset \mathcal{O}.$$

Cela prouve que $B(x_0, \epsilon) \subset f|_I^{-1}(\mathcal{O})$.

Dans l'autre sens, maintenant. Nous prenons $x_0 \in I$ et nous voulons prouver que f est continue en x_0 , c'est-à-dire que pour tout δ nous cherchons un ϵ tel que $f(B(x_0, \epsilon)) \subset B(f(x_0), \delta)$. Oui, mais $B(f(x_0), \delta)$ est ouverte, donc par hypothèse, $f|_I^{-1}(B(f(x_0), \delta))$ est ouvert, inclus dans I et contient x_0 . Donc il existe un ϵ tel que

$$B(x_0, \epsilon) \subset f|_I^{-1}(B(f(x_0), \delta)),$$

et donc tel que

$$f(B(x_0, \epsilon)) \subset B(f(x_0), \delta),$$

ce qu'il fallait prouver. $\square$

Lemme 10.79.

L'image d'un ensemble connexe par une fonction continue est connexe.

Démonstration. Nous allons encore faire la contraposée. Soit A une partie de $\mathbb{R}$ telle que $f(A)$ ne soit pas connexe. Nous allons prouver que A elle-même n'est pas connexe. Dire que $f(A)$ n'est pas connexe, c'est dire qu'il existe $\mathcal{O}_1$ et $\mathcal{O}_2$, deux ouverts disjoints qui recouvrent $f(A)$. Je prétends que $f^{-1}(\mathcal{O}_1)$ et $f^{-1}(\mathcal{O}_2)$ sont ouverts, disjoints et qu'ils recouvrent A .

- Ces deux ensembles sont ouverts parce qu'ils sont images inverses d'ouverts par une fonction continue (théorème 10.78).
- Si $x \in f^{-1}(\mathcal{O}_1) \cap f^{-1}(\mathcal{O}_2)$, alors $f(x) \in \mathcal{O}_1 \cap \mathcal{O}_2$, ce qui contredirait le fait que $\mathcal{O}_1$ et $\mathcal{O}_2$ sont disjoints. Il n'y a donc pas d'éléments dans l'intersection de $f^{-1}(\mathcal{O}_1)$ et de $f^{-1}(\mathcal{O}_2)$.
- Si $f^{-1}(\mathcal{O}_1)$ et $f^{-1}(\mathcal{O}_2)$ ne recouvrent pas A , il existe un x dans A qui n'est dans aucun des deux. Dans ce cas, $f(x)$ est dans $f(A)$, mais n'est ni dans $\mathcal{O}_1$, ni dans $\mathcal{O}_2$, ce qui contredirait le fait que ces deux derniers recouvrent $f(A)$.

Nous déduisons que A n'est pas connexe. Et donc le lemme. $\square$

Théorème 10.80 (Théorème des valeurs intermédiaires).

Soit f , une fonction continue sur $[a, b]$, et supposons que $f(a) < f(b)$. Alors pour tout y tel que $f(a) \leq y \leq f(b)$, il existe un $x \in [a, b]$ tel que $f(x) = y$.

Démonstration. Nous savons que $[a, b]$ est connexe parce que c'est un intervalle (proposition 10.47). Donc $f([a, b])$ est connexe (lemme 10.79) et donc est un intervalle (à nouveau la proposition 10.47). Étant donné que $f([a, b])$ est un intervalle, il contient toutes les valeurs intermédiaires entre n'importe quels deux de ses éléments. En particulier toutes les valeurs intermédiaires entre $f(a)$ et $f(b)$. $\square$

Corolaire 10.81.

L'image d'un intervalle par une fonction continue est un intervalle.

Démonstration. Soient I un intervalle, $\alpha < \beta \in f(I)$ et $\gamma \in]\alpha, \beta[$. Nous considérons $a, b \in I$ tels que $\alpha = f(a)$ et $\beta = f(b)$. Par le théorème des valeurs intermédiaires 10.80, il existe $t \in]a, b[$ tel que $f(t) = \gamma$. Par conséquent $\gamma \in f(I)$. $\square$

Corolaire-Définition 10.82 (Existence de la racine carrée).

*Si $x \geq 0$ alors il existe un unique $y \geq 0$ tel que $y^2 = x$. Ce nombre est noté $\sqrt{x}$ et est nommé **racine carrée** de x .*

Démonstration. La fonction $f: t \mapsto t^2$ est continue et strictement croissante. Nous avons $f(0) = 0$ et ²⁷ $f(x+1) > x$. Donc le théorème des valeurs intermédiaires 10.80 nous assure qu'il existe un unique $y \in [0, x+1]$ tel que $f(y) = x$. $\square$

Lemme 10.83.

La fonction racine carrée est strictement croissante.

Démonstration. Supposons que $x < y$. Si $\sqrt{x} > \sqrt{y}$, alors la croissance de la fonction carré donne $x > y$ qui est contraire à l'hypothèse.. $\square$

10.4.4 Module sur les nombres complexes

Lemme-Définition 10.84.

Si $z \in \mathbb{C}$, alors $z\bar{z}$ est un réel positif.

Nous définissons le **module** sur $\mathbb{C}$ par²⁸

$$|z| = \sqrt{z\bar{z}}. \quad (10.92)$$

Démonstration. Prouvons que $z\bar{z}$ est un réel positif. En effet si $z = a + bi$ alors

$$z\bar{z} = (a + bi)(a - bi) = a^2 - abi + abi + b^2 = a^2 + b^2 \geq 0. \quad (10.93)$$

$\square$

Proposition 10.85.

Pour tout nombres complexes $z = a + bi$ et z' , nous avons

- (1) $z\bar{z} = a^2 + b^2$;
- (2) $\bar{\bar{z}} = z$;
- (3) $|z| = |\bar{z}|$;
- (4) $|zz'| = |z||z'|$;
- (5) $|z_1 + z_2| \leq |z_1| + |z_2|$

Démonstration. En plusieurs points.

Pour (1) Calcul direct :

$$z\bar{z} = (a + bi)(a - bi) = a^2 - abi + abi + b^2 = a^2 + b^2. \quad (10.94)$$

Pour (2) On a :

$$\bar{\bar{z}} = \overline{(a - bi)} = a + bi. \quad (10.95)$$

Pour (3) Même calcul que pour (1).

Pour (4) Vu que les deux membres de l'égalité à prouver sont positifs, il est suffisant de prouver l'égalité des carrés (lemme 10.83). Nous avons

$$zz' = (a + bi)(a' + b'i) = aa' - bb' + i(ab' + ba'), \quad (10.96)$$

donc

$$|zz'|^2 = (aa' - bb')^2 + (ab' + ba')^2 \quad (10.97a)$$

$$= (aa')^2 + (bb')^2 - 2aa'bb' + (ab')^2 + (ba')^2 + 2ab'ba' \quad (10.97b)$$

$$= a^2(a'^2 + b'^2) + b^2(b'^2 + a'^2) \quad (10.97c)$$

$$= (a^2 + b^2)(a'^2 + b'^2). \quad (10.97d)$$

D'autre part,

$$(|z||z'|)^2 = |z|^2|z'|^2 = (a^2 + b^2)(a'^2 + b'^2). \quad (10.98)$$

27. Faites deux cas suivant $x \geq 1$ ou non si vous le voulez, moi je prends $x + 1$.

28. Définition de la racine carré : 10.82.

Pour (5) Nous posons $z_1 = a_1 + b_1i$ et $z_2 = a_2 + b_2i$. Ensuite nous calculons, en utilisant (10.98) :

$$(|z_1| + |z_2|)^2 = |z_1|^2 + |z_2|^2 + 2|z_1||z_2| = a_1^2 + b_1^2 + a_2^2 + b_2^2 + 2\sqrt{(a_1^2 + b_1^2)(a_2^2 + b_2^2)}. \quad (10.99)$$

et

$$|z_1 + z_2|^2 = |(a_1 + a_2) + i(b_1 + b_2)|^2 \quad (10.100a)$$

$$= (a_1 + a_2)^2 + (b_1 + b_2)^2 \quad (10.100b)$$

$$= a_1^2 + a_2^2 + 2a_1a_2 + b_1^2 + b_2^2 + 2b_1b_2. \quad (10.100c)$$

En faisant la différence,

$$(|z_1| + |z_2|)^2 - |z_1 + z_2|^2 = 2\sqrt{(a_1^2 + b_1^2)(a_2^2 + b_2^2)} - 2(a_1a_2 + b_1b_2). \quad (10.101)$$

Pour prouver que cette différence est positive, nous comparons les carrés des deux termes :

$$A = (a_1^2 + b_1^2)(a_2^2 + b_2^2) \quad (10.102a)$$

$$B = (a_1a_2 + b_1b_2)^2. \quad (10.102b)$$

Nous avons :

$$A = a_1^2a_2^2 + a_1^2b_2^2 + b_1^2a_2^2 + b_1^2b_2^2 \quad (10.103)$$

et

$$B = a_1^2a_2^2 + b_1^2b_2^2 + 2a_1a_2b_1b_2. \quad (10.104)$$

Et un petit calcul montre enfin que

$$A - B = a_1^2b_2^2 + b_1^2a_2^2 - 2a_1a_2b_1b_2 = (a_1b_2 - b_1a_2)^2 \geq 0. \quad (10.105)$$

□

Lemme 10.86.

Nous avons $|\operatorname{Re}(z)| \leq |z|$ et nous avons l'égalité si et seulement si $z \in \mathbb{R}$.

Démonstration. En plusieurs points.

L'inégalité Par croissance de la fonction racine carré nous avons, en posant $z = a + bi$:

$$|\operatorname{Re}(z)| = |a| = \sqrt{|a|^2} \leq \sqrt{|a|^2 + |b|^2} = |z|. \quad (10.106)$$

Égalité dans un sens Si $|\operatorname{Re}(z)| = |z|$, alors toutes les inégalités dans (10.106) sont des égalités.

En particulier

$$\sqrt{|a|^2} = \sqrt{|a|^2 + |b|^2}. \quad (10.107)$$

Par stricte croissance de la fonction racine carré, nous déduisons que $|b|^2 = 0$ et donc que $b = 0$.

Égalité dans l'autre sens Si $z \in \mathbb{R}$, alors $\operatorname{Re}(z) = z$, et nous avons l'égalité.

□

Lemme 10.87.

Soient $a, b \in \mathbb{C}$. Nous avons $|a + b| = |a| + |b|$ si et seulement si $a\bar{b} = 0$.

Démonstration. Nous avons toujours l'égalité

$$|a + b|^2 = |a|^2 + |b|^2 + 2\operatorname{Re}(a\bar{b}). \quad (10.108)$$

Dans un premier sens nous supposons $|a + b| = |a| + |b|$. Donc

$$\sqrt{|a|^2 + |b|^2 + 2\operatorname{Re}(a\bar{b})} = \sqrt{|a|^2 + |b|^2 + 2|a||b|}, \quad (10.109)$$

et donc que $\operatorname{Re}(a\bar{b}) = |a||b|$. Vu que $|a\bar{b}| = |a||b|$ (proposition 10.85(4)), nous avons

$$\operatorname{Re}(a\bar{b}) = |a\bar{b}|. \quad (10.110)$$

Nous sommes dans le cas d'égalité du lemme 10.86. Donc $a\bar{b} \in \mathbb{R}$. Et il est manifestement positif parce qu'égal à $|a||b|$.

Dans l'autre sens, nous supposons que $a\bar{b} = 0$. En particulier $a\bar{b} \in \mathbb{R}$ et $\operatorname{Re}(a\bar{b}) = |a||b|$. Nous avons alors

$$|a + b| = \sqrt{|a|^2 + |b|^2 + 2\operatorname{Re}(a\bar{b})} = |a| + |b|. \quad (10.111)$$

□

Lemme 10.88.

À propos du module.

(1) Si $x, y \in \mathbb{C}$ nous avons

$$|x + y| \leq |x| + |y|. \quad (10.112)$$

(2) Il y a égalité si et seulement si $x\bar{y} \geq 0$.

Démonstration. En plusieurs points.

L'inégalité Nous considérons deux nombres complexes x et y . Nous avons

$$|x + y| = \sqrt{|x|^2 + |y|^2 + x\bar{y} + \bar{x}y}. \quad (10.113)$$

Maintenant, $x\bar{y} + y\bar{x} = 2\operatorname{Re}(xy)$ et $\operatorname{Re}(z) \leq |z|$ et la racine carrée est croissante²⁹. Donc

$$|x + y| = \sqrt{|x|^2 + |y|^2 + x\bar{y} + \bar{x}y} \leq \sqrt{|x|^2 + |y|^2 + 2|x\bar{y}|} = \sqrt{|x|^2 + |y|^2 + 2|x||y|} = |x| + |y|. \quad (10.114)$$

Le cas d'égalité C'est le lemme 10.87.

□

Lemme 10.89.

Si deux nombres complexes $a, b \in \mathbb{C}$ vérifient $a\bar{b} \in \mathbb{R}$, alors on est dans un des deux cas suivants :

- $b = 0$
- il existe $\lambda \in \mathbb{R}$ tel que $a = \lambda b$.

De façon équivalente, il existe $\alpha, \beta \in \mathbb{R}$ non tous deux nuls tels que $\alpha a + \beta b = 0$.

Démonstration. Nous écrivons $a = a_1 + ia_2$ et $b = b_1 + ib_2$ avec $a_i, b_i \in \mathbb{R}$. Nous supposons $b \neq 0$. Nous effectuons la multiplication $a\bar{b} = (a + ib_2)(b_1 - ib_2)$ et nous annulons la partie imaginaire :

$$a_2b_1 - a_1b_2 = 0. \quad (10.115)$$

Si $b_1 = 0$ alors $a_1b_2 = 0$ avec $b_2 \neq 0$, ce qui implique $a_1 = 0$. Donc $a = ia_2$, $b = ib_2$. Résultat obtenu.

Si $b_1 \neq 0$ alors

$$a_2 = \frac{a_1b_2}{b_1}, \quad (10.116)$$

et nous avons du coup

$$a = \frac{a_1}{b_1}b. \quad (10.117)$$

Mission accomplie.

Nous prouvons à présent la formulation équivalente. Si $b = 0$ il suffit de prendre $\alpha = 0$. Si $a = \lambda b$ il faut prendre $\alpha = \beta/\lambda$.

Dans l'autre sens, si $\alpha \neq 0$ alors $a = -(\beta/\alpha)b$ et si $\alpha = 0$ alors $\beta \neq 0$ et il reste $b = 0$. □

29. Lemme 10.83.

Proposition 10.90.

La paire $(\mathbb{C}, |\cdot|)$ est un espace vectoriel normé³⁰.

Démonstration. Nous devons prouver les différents points de la définition 7.118.

- (1) $|z| \geq 0$ parce que la racine carrée prend ses valeurs dans $\mathbb{R}^+$.
- (2) Si $|z| = 0$, alors, en notant $z = a + bi$ nous avons $a^2 + b^2 = 0$. La somme de deux positifs est nulle que quand les deux sont nuls. Donc $a = b = 0$.
- (3) Si $\lambda \geq 0$, alors $(\lambda z)\overline{\lambda z} = \lambda^2 z\bar{z}$ et nous avons

$$|\lambda z| = \sqrt{\lambda^2 z\bar{z}} = |\lambda| \sqrt{z\bar{z}} = |\lambda| |z|. \quad (10.118)$$

- (4) L'inégalité $|x + y| \leq |x| + |y|$ est le lemme 10.88.

□

Proposition 10.91.

Si z_1 et z_2 sont des nombres complexes, alors

$$|z_1 z_2| = |z_1| |z_2|. \quad (10.119)$$

Nous avons aussi, pour tout $n \in \mathbb{N}$,

$$|z^n| = |z|^n. \quad (10.120)$$

Démonstration. D'abord $(a + bi)(c + di) = ac - db + (ad + bc)i$, de telle sorte que

$$|(a + bi)(c + di)|^2 = (ac - bd)^2 + (ad + bc)^2. \quad (10.121)$$

Mais en calculant d'autre part $|a + bi|^2 |c + di|^2$, nous tombons sur la même valeur.

Une simple récurrence permet de conclure que $|z^n| = |z|^n$. □

Voilà. Vous êtes déjà content d'apprendre que l'on peut démontrer $|z^n| = |z|^n$ sans faire appel à la forme trigonométrique des nombres complexes.

Lemme 10.92.

Pour tout $z \in \mathbb{C}$ nous avons $z\bar{z} = \bar{z}z = |z|^2$.

10.4.5 Continuité de la racine carrée, invitation à la topologie induite

Pourquoi nous intéresser particulièrement à cette fonction ? Parce qu'elle a une sale condition d'existence : son domaine de définition n'est pas ouvert. Or dans tous les théorèmes de continuité d'approche topologique que nous avons vus, nous avons donné des conditions *pour tout ouvert*. Nous nous attendons donc à avoir des difficultés avec la continuité de $\sqrt{x}$ en zéro.

Prenons I , n'importe quel intervalle ouvert dans $\mathbb{R}^+$, et voyons que la fonction³¹

$$\begin{aligned} f: \mathbb{R}^+ &\rightarrow \mathbb{R}^+ \\ x &\mapsto \sqrt{x} \end{aligned} \quad (10.122)$$

est continue sur I . Remarque déjà que si I est un ouvert dans $\mathbb{R}^+$, il ne peut pas contenir zéro. Avant de nous lancer dans notre propos, nous prouvons un lemme qui fera tout le travail³².

Lemme 10.93.

Soit $\mathcal{O}$, un ouvert dans $\mathbb{R}^+$. Alors $\mathcal{O}^2 = \{x^2 \text{ tel que } x \in \mathcal{O}\}$ est également ouvert.

30. Définition d'une norme : 7.118.

31. La racine carrée est définie en 10.82.

32. C'est toujours ingrat d'être un lemme : on fait tout le travail et c'est toujours le théorème qui est nommé.

Démonstration. Un élément de $\mathcal{O}^2$ s'écrit sous la forme x^2 pour un certain $x \in \mathcal{O}$. Le but est de trouver un ouvert autour de x^2 qui soit contenu dans $\mathcal{O}^2$. Étant donné que $\mathcal{O}$ est ouvert, on a une boule centrée en x contenue dans $\mathcal{O}$. Nous appelons δ le rayon de cette boule :

$$B(x, \delta) \subset \mathcal{O}.$$

Étant donné que cet ensemble est connexe, nous savons par le lemme 10.79 que $B(x, \delta)^2$ est également connexe (parce que la fonction $x \mapsto x^2$ est continue). Son plus grand élément est $(x + \delta)^2 = x^2 + \delta^2 + 2x\delta > x^2 + \delta^2$, et son plus petit élément est $(x - \delta)^2 = x^2 + \delta^2 - 2x\delta$.

Ce qui serait pas mal, c'est que ces deux bornes entourent x^2 ; de cette façon elles définiraient un ouvert autour de x^2 qui soit dans $\mathcal{O}^2$. Hélas, c'est pas gagné que $x^2 + \delta^2 - 2x\delta$ soit plus petit que x^2 .

Heureusement, en fait c'est vrai parce que d'une part, du fait que $\mathcal{O} \subset \mathbb{R}^+$, on a $x > 0$, et d'autre part, pour que $\mathcal{O}$ soit positif, il faut que $\delta < x$. Donc on a évidemment que $\delta < 2x$, et donc que

$$x^2 + \delta^2 - 2x\delta = x^2 + \delta \underbrace{(\delta - 2x)}_{<0} < x^2.$$

Donc nous avons fini : l'ensemble

$$B(x, \delta)^2 =]x^2 + \delta^2 - 2x\delta, x^2 + \delta^2 + 2x\delta[\subset \mathcal{O}^2$$

est un intervalle qui contient x^2 , et donc qui contient une boule ouverte centrée en x^2 . □

Maintenant nous pouvons nous attaquer à la continuité de la racine carrée sur tout ouvert positif en utilisant le théorème 10.78. Soit $\mathcal{O}$ n'importe quel ouvert de $\mathbb{R}$, et prouvons que $f|_I^{-1}(\mathcal{O})$ est ouvert. Par définition,

$$f|_I^{-1}(\mathcal{O}) = \{x \in I \text{ tel que } \sqrt{x} \in \mathcal{O}\}. \quad (10.123)$$

Maintenant c'est un tout petit effort que de remarquer que $f|_I^{-1}(\mathcal{O}) = \mathcal{O}^2 \cap I$. De là, on a gagné parce que $\mathcal{O}^2$ et I sont des ouverts. Or l'intersection de deux ouverts est ouvert.

Nous n'en avons pas fini avec la fonction $\sqrt{x}$. Nous avons la continuité de la racine carrée pour tous les réels strictement positifs. Il reste à pouvoir dire que la fonction est continue en zéro malgré qu'elle ne soit pas définie sur un ouvert autour de zéro.

Il est possible de dire que la racine carrée est continue en 0, malgré qu'elle ne soit pas définie sur un ouvert autour de 0... en tout cas pas un ouvert au sens que tu as en tête. Nous allons rentabiliser un bon coup notre travail sur les espaces métriques.

Nous pouvons définir la notion de boule ouverte sur n'importe quel espace métrique A en disant que

$$B(x, r) = \{y \in A \text{ tel que } d(x, y) < r\}.$$

Définition 10.94.

Soit $f: A \rightarrow B$, une application entre deux espaces métriques. Nous disons que f est **continue** au point $a \in A$ si $\forall \delta > 0, \exists \epsilon > 0$ tel que

$$f(B(a, \epsilon)) \subset B(f(a), \delta). \quad (10.124)$$

Tu reconnais évidemment la condition (10.91). Nous l'avons juste recopiée. Tu remarqueras cependant que cette définition généralise immensément la continuité que l'on avait travaillé à propos des fonctions de $\mathbb{R}$ vers $\mathbb{R}$. Maintenant tu peux prendre n'importe quel espace métrique et c'est bon.

Nous n'allons pas faire un tour complet des conséquences et exemples de cette définition. Au lieu de cela, nous allons juste montrer en quoi cette définition règle le problème de la continuité de la racine carrée en zéro.

La fonction que nous regardons est

$$\begin{aligned} f: \mathbb{R}^+ &\rightarrow \mathbb{R}^+ \\ x &\mapsto \sqrt{x}. \end{aligned} \quad (10.125)$$

Mais cette fois, nous ne la voyons pas comme étant une fonction dont le domaine est une partie de $\mathbb{R}$, mais comme fonction dont le domaine est $\mathbb{R}^+$ vu comme un espace métrique en soi. Quelles sont les boules ouvertes dans $\mathbb{R}^+$ autour de zéro ? Réponse : la boule ouverte de rayon r autour de zéro dans $\mathbb{R}^+$ est :

$$B(0, r)_{\mathbb{R}^+} = \{x \in \mathbb{R}^+ \text{ tel que } d(x, 0) < r\} = [0, r[.$$

Cet intervalle est un ouvert. Aussi incroyable que cela puisse paraître !

Testons la continuité de la racine carrée en zéro dans ce contexte. Il s'agit de prendre $A = \mathbb{R}^+$, $B = \mathbb{R}^+$ et $a = 0$ dans la définition 10.94. Nous avons que $B(\sqrt{0}, \delta) = B(0, \delta) = [0, \delta[$ pour la topologie de $\mathbb{R}^+$.

Il s'agit maintenant de trouver un ϵ tel que $f(B(0, \epsilon)) \subset [0, \delta[$. Par définition, nous avons que

$$f(B(0, \epsilon)) = [0, \sqrt{\epsilon}[,$$

le problème revient donc à trouver ϵ tel que $\sqrt{\epsilon} \leq \delta$. Prendre $\epsilon < \delta^2$ fait l'affaire.

Donc voilà. Au sens de la topologie induite³³, de $\mathbb{R}$ vers $\mathbb{R}^+$, nous pouvons dire que la fonction racine carrée est partout continue.

10.4.6 Second degré

Nous résolvons à présent le polynôme du second degré.

Proposition 10.95 ([234]).

Soit la fonction

$$\begin{aligned} f: \mathbb{R} &\rightarrow \mathbb{R} \\ x &\mapsto ax^2 + bx + c \end{aligned} \quad (10.126)$$

avec $a \neq 0$. Nous notons $\Delta = b^2 - 4ac$.

(1) Nous avons la formule

$$f(x) = a\left(x + \frac{b}{2a}\right)^2 + c - \frac{b^2}{4a}. \quad (10.127)$$

(2) Si $a > 0$, alors f a un minimum global en $x_m = -b/2a$.

(3) Si $a < 0$, alors f a un maximum global en $x_M = -b/2a$.

(4) Si $\Delta < 0$ alors f ne possède pas de racines réelles.

(5) Si $\Delta = 0$, alors f possède une unique racine $x_0 = -b/2a$.

(6) Si $\Delta > 0$ alors f possède exactement deux racines distinctes données par

$$x_1 = \frac{-b + \sqrt{\Delta}}{2a} \quad x_2 = \frac{-b - \sqrt{\Delta}}{2a}. \quad (10.128)$$

Démonstration. En plusieurs parties.

Pour (1) C'est un calcul immédiat.

Pour (2) Nous partons de la formule du point (1). Vu que $c - \frac{b^2}{4a}$ est constant, minimiser f revient à minimiser $x \mapsto \left(x + \frac{b}{2a}\right)^2$. Comme cette dernière fonction est toujours positive, elle a un minimum global là où elle est nulle, c'est à dire en $x_m = -b/2a$.

Pour (3) Idem que pour (2).

33. Définition 7.17.

Pour la suite nous effectuons quelques manipulations à partir de (10.127). Nous avons $f(x) = 0$ lorsque

$$\left(x + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2}. \quad (10.129)$$

Pour (4) À gauche de (10.129) nous avons un nombre toujours positif ou nul. À droite, $4a^2 > 0$.
Donc si $b^2 - 4ac < 0$, l'égalité est impossible et il n'y a pas de x vérifiant $f(x) = 0$.

Pour (5) Si $b^2 - 4ac = 0$, alors la condition (10.129) devient

$$\left(x + \frac{b}{2a}\right)^2 = 0, \quad (10.130)$$

et donc $x = -b/2a$ est l'unique solution.

Pour (6) Si $b^2 - 4ac > 0$, nous pouvons prendre la racine carrée³⁴ des deux côtés de (10.129), et la condition devient

$$x + \frac{b}{2a} = \pm \sqrt{\frac{b^2 - 4ac}{4a^2}}, \quad (10.131)$$

ce qui donne

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}. \quad (10.132)$$

Ce sont là les deux seuls candidats pour vérifier $f(x) = 0$.

Un calcul direct montre que

$$f\left(\frac{-b + \sqrt{b^2 - 4ac}}{2a}\right) = 0 \quad (10.133)$$

et que

$$f\left(\frac{-b - \sqrt{b^2 - 4ac}}{2a}\right) = 0. \quad (10.134)$$

Donc ce sont bien des racines de f et ce sont les seules. Notez aussi qu'elles sont distinctes parce que $\Delta \neq 0$.

□

34. Définition 10.82.