Le Frido 2019,
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 2020. 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 niveau recherche sur

   `https://laurent.claessens-donadello.eu/pdf/giulietta.pdf`

3. Et bien entendu les sources LaTeX

   `https://github.com/LaurentClaessens/mazhe`

ISBN : 979-10-97085-18-6

Thèmes

Ceci est une sorte d'index thématique.

Thème 1 : 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 15.20 sur un espace mesuré avec une tribu, définition 15.1.

(2) Une mesure extérieure est la définition 15.13

(3) Une algèbre de partie : définition 15.16. Une mesure sur une algèbre de parties : définition 15.14. L'intérêt est que si on connait une mesure sur une algèbre de parties, elle se prolonge en une mesure sur la tribu engendrée par le théorème de prolongement de Hahn 15.68.

(4) Un λ-système : définition 15.30.

(5) Une mesure complexe : définition 15.198.

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

$$f\colon \big(X, \mathcal{L}\text{eb}(X)\big) \to \big(\mathbb{R}, \mathcal{B}\text{or}(\mathbb{R})\big).$$

Voir les points 15.106 et 15.150 pour les conventions à ce propos.

À propos d'applications mesurables :

(1) Une fonction continue est borélienne, théorème 15.49.

À propos de tribu induite :

(1) Définition 15.6.

(2) Les boréliens induits sont bien les boréliens de la topologie induite : $\mathcal{B}\text{or}(Y) = \mathcal{B}\text{or}(X)_Y$, théorème 15.50.

Thème 2 : théorie de la mesure

Mesure À propos de mesure.

(1) Mesure positive, mesure finie et σ-finie, c'est la définition 15.20.

(2) Le produit de tribus est donné par la définition 15.112,

(3) Produit d'une mesure par une fonction, définition 15.187.

(4) le produit d'espaces mesurés est donné par la définition 15.208.

(5) Mesure de Lebesgue sur $\mathbb{R}$, définition 15.127.

(6) Une partie de $\mathbb{R}$ non mesurable au sens de Lebesgue : l'exemple 15.141.

(7) Mesure de Lebesgue sur $\mathbb{R}^N$, définition 15.210.

(8) Mesure à densité, définition 15.187.

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 $f\colon S \to [0, +\infty]$ est une fonction mesurable, le théorème fondamental d'approximation 15.105 donne une suite croissante de fonctions étagées qui converge vers f.

(2) Les fonctions simples sont denses dans L^p, proposition 28.44.

(3) Encadrement d'un borélien A par un fermé F et un ouvert V par le lemme 15.201 : $F \subset A \subset V$ avec $\mu(V \backslash F) < \epsilon$.

(4) Approximation L^p de la fonction caractéristique d'un borélien par une fonction continue par le théorème 15.203.

Thème 3 : intégration À propos d'intégration.

(1) Intégrale associée à une mesure, définition 15.151

(2) L'existence d'une primitive pour toute fonction continue est le théorème 13.308.

(3) La définition d'une primitive est la définition 13.135.

(4) Primitive et intégrale, proposition 15.232.

(5) Intégrale impropre, définition 15.245.

L'ordre dans lequel les choses sont faites.

— Nous commençons par considérer des fonctions $f\colon \Omega \to [0, +\infty]$ dans la définition 15.151.

— Nous donnerons ensuite quelque propriétés restreintes au fonctions à valeurs positives, par exemple

(1) La convergence monotone 15.160,

(2) Lemme de Fatou 15.164.

(3) (presque) linéarité pour les fonctions positives, théorème 15.165.

— La définition pour les fonctions à valeurs dans $\mathbb{R}$ puis $\mathbb{C}$ est 15.168.

— Pour les fonctions à valeurs dans un espace vectoriel, c'est la définition 15.176.

Quelque résultats :

(1) Si $A, B \subset \Omega$ sont des parties disjointes, alors $\int_{A\cup B} f = \int_A f + \int_B f$, proposition 15.173.

<++>

Thème 4 : suites et séries

Suites Les suites réelles sont en général dans la proposition 8.11 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 8.23. Cela sert pour les séries alternées, théorème 12.80, qui sert pour étudier la série de Taylor de $\ln(x+1)$, voir le lemme 16.73 et ce qui l'entoure.

(2) La définition de la convergence absolue est la définition 12.59.

(3) Une suite réelle croissante et majorée converge, proposition 8.18.

(4) Toute suite dans un compact admet une sous-suite convergente, théorème 8.19.

(5) Pour tout réel, il existe une suite croissante de rationnels qui y converge, proposition 8.4.

Série Les séries sont en général dans la section 12.5.

(1) Quelques séries usuelles en 12.6.3 : série harmonique, géométrique, de Riemann, et la mythique arithmético-géométrique.

(1a) La série harmonique diverge : $\sum_k \frac{1}{k} = \infty$, exemple 12.74.

(1b) La série géométrique : $\sum_{k=0}^{N} q^k = \frac{1-q^{N+1}}{1-q}$, exemple 12.75.

(1c) Une autre cool série : $\sum_{k=1}^{N} \frac{1}{k(k+1)} = \frac{N}{N+1}$, lemme 12.79.

(2) Critère des séries alternées, théorème 12.80.

(3) Convergence d'une série implique convergence vers zéro du terme général, proposition 12.66.

Sommes infinies Nous pouvons dire plusieurs choses à propos d'une somme infinie.

(1) Une somme indexée par un ensemble quelconque est la définition 12.99.

(2) La définition de la somme d'une infinité de termes est donnée par la définition 12.56.

(3) 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

(3a) si la série converge absolument, on peut modifier l'ordre des termes sans modifier la convergence ni la somme (commutativité, proposition 12.97).

(4) 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 12.108.

Thème 5 : 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 13.359.

(2) Une majoration du reste est dans le théorème 16.34

(3) De classe C^2 sur $\mathbb{R}^n$, proposition 13.366.

(4) Avec un reste donné par un point dans $]x, a[$, proposition 13.370.

(5) Avec reste intégral, proposition 21.149 et théorème 21.146 pour le cas simple $\mathbb{R} \to \mathbb{R}$.

(6) Le polynôme de Taylor généralise à l'utilisation de toutes les dérivées disponibles le résultat de développement limité donné par la proposition 13.112.

(7) Pour les fonctions holomorphes, il y a le théorème 27.30 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 (35.93).

(2) On utilise pas mal de Taylor dans les résultats liant extrema et différentielle/hessienne. Par exemple la proposition 18.70.

Quelque développements Voici quelque développements limités à savoir. Ils sont calculables en utilisant la formule de Taylor-Young (proposition 13.375).

$$e^x = \sum_{k=0}^{n} \frac{x^k}{k!} + x^n\alpha(x) \qquad \text{ordre } n, \text{proposition 16.68}$$

$$\cos(x) = \sum_{k=0}^{p} \frac{(-1)^k x^{2k}}{(2k)!} + x^{2p+1}\alpha(x) \qquad \text{ordre } 2p+1, \text{proposition 19.69}$$

$$\sin(x) = \sum_{k=0}^{p} \frac{(-1)^k x^{2k+1}}{(2k+1)!} + x^{2p+2}\alpha(x) \qquad \text{ordre } 2p+1, \text{proposition 19.69}$$

$$\ln(1+x) = \sum_{k=1}^{n} \frac{(-1)^{k+1}}{k} x^k + \alpha(x)x^n \qquad \text{ordre } n, \text{proposition 16.72}$$

$$\ln(1+x) = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} x^k \qquad \text{exact proposition 16.74}$$

$$\ln(2) = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} \qquad \text{exact proposition 16.74}$$

$$(1+x)^l = \sum_{k=0}^{l} \binom{l}{k} x^k \qquad \text{exact si } l \text{ est entier.}$$

$$(1+x)^\alpha = 1 + \sum_{k=1}^{n} \frac{\alpha(\alpha-1)\dots(\alpha-k+1)}{k!} x^k + x^n\alpha(x) \qquad \text{ordre } n.$$

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

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 6 : séries de Fourier

— Formule sommatoire de Poisson, proposition 30.11.

— Inégalité isopérimétrique, théorème 29.21.

— Fonction continue et périodique dont la série de Fourier ne converge pas, proposition 29.18.

— 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 29.5.

(2) Convergence au sens $L^2\Big([0,2\pi]\Big)$ dans le théorème 28.108.

(3) Si f est continue, périodique et si sa série de Fourier converge uniformément, théorème 29.13.

(4) Si f est périodique et la série des coefficients converge absolument pour tout x, proposition 29.14.

(5) Si f est périodique et de classe C^1, théorème 29.15.

Il est cependant faux de croire que la continuité et la périodicité suffisent à obtenir une convergence, comme le montre dans la proposition 29.18.

Thème 7 : normes

Définition Espace vectotiel normé : définition 7.106.

Équivalence de norme (1) Définition de l'équivalence de norme 12.3.

(2) La proposition 12.5 sur l'équivalence des normes $\|.\|_2$, $\|.\|_1$ et $\|.\|_\infty$ dans $\mathbb{R}^n$.

(3) En général pour les normes $\|.\|_p$, il y a des inégalités dans 13.350 et 18.96 ; voir aussi le thème 7.

(4) La proposition 18.106 donne l'inégalité $\|x\|_q \leqslant n^{\frac{1}{q}-\frac{1}{p}}\|x\|_p$ dès que $0 < q < p$.

(5) Toutes les normes sur un espace vectoriel de dimension finie sont équivalentes, théorème 12.6.

(6) Montrer que le problème $a - b$ est stable dans l'exemple 35.26.

(7) La proposition 12.22 donnant $\rho(A) \leqslant \|A\|$ utilise l'équivalence de toutes les normes sur un espace vectoriel de dimension finie.

Norme opérateur et d'algèbre voir le thème 41.

Thème 8 : topologie produit

(1) La définition de la topologie produit est 7.9.

(2) Pour les espaces vectoriels normés, le produit est donné par la définition 12.41.

(3) L'équivalence entre la topologie de la norme produit et la topologie produit est le lemme 12.42.

Thème 9 : espaces métriques, normés

(1) Un espace métrique est un espace muni d'une distance, définition 7.87.

(2) La distance entre un point et un ensemble est la définition 7.100.

(3) Le théorème-définition 7.88 donne la topologie sur un espace métrique en disant que les boules ouvertes sont une base de la topologie (définition 7.54).

(4) La définition de la convergence d'une suite est la définition 7.25.

(5) Dans un espace vectoriel normé, une application est continue si et seulement si elle est bornée, proposition 12.25.

(6) Un espace vectoriel topologique qui possède en tout point une base dénombrable de topologie accepte une distance, théorème 9.33.

Thème 10 : gaussienne

(1) Le calcul de l'intégrale

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

est fait de deux façons dans l'exemple 15.262. Dans les deux cas, le théorème de Fubini 15.259 est utilisé.

(2) Le lemme 30.17 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 30.20 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 30.22

Thème 11 : compacts

Propriétés générales Quelques propriétés de compacts.

(1) La définition d'un ensemble compact est la définition 7.43.
(2) Les compacts sont les fermés bornés par le théorème 8.9.
(3) Le théorème de Borel-Lebesgue 8.6 dit qu'un intervalle de $\mathbb{R}$ est compact si et seulement si il est de la forme $[a, b]$.
(4) Théorème des fermés emboîtés dans le cas compact, corollaire 7.53. À ne pas confondre avec celui dans le cas des espaces métrique, théorème 9.51.
(5) L'image d'un compact par une fonction continue est un compact, théorème 7.86.
(6) Suites dans un compact
  (6a) Toute suite dans un compact admet une sous-suite convergente, théorème 8.19.
  (6b) Dans $\mathbb{R}^n$, toute suite dans un compact admet une sous-suite convergente, théorème 8.36. La démonstration de ce théorèma 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.
  (6c) Un espace métrique est compact si et seulement si toute suite contient une sous-suite convergente. C'est le théorème de Bolzano-Weierstrass 7.97. La démonstration de ce théorème est indépendante.
(7) Une fonction continue sur un compact est bornée et attein ses bornes, théorème 7.99.
(8) Une fonction continue sur un compact y est uniforément continue, théorème de Heine 13.89.

Produits de compacts À propos de produits de compacts. C'est un compact dans tous les cas métriques[1].

(1) Les produits d'espaces métriques compacts sont compacts ; c'est le théorème de Tykhonov. Nous verrons ce résultat dans les cas suivants.
  — $\mathbb{R}$, lemme 8.8.
  — Produit fini d'espaces métriques compacts, théorème 9.66.
  — Produit dénombrable d'espaces métriques compacts, théorème 9.68.

Thème 12 : densité

(1) Densité des polynômes dans $\left(C^0([0,1]), \|.\|_\infty\right)$, théorème de Bernstein 37.133.
(2) Densité des polynômes dans $\left(C^0(I), \|.\|_\infty\right)$ lorsque $I = [a, b]$, corollaire 37.134.
(3) Densité de $\mathscr{D}(\mathbb{R}^d)$ dans $L^p(\mathbb{R}^d)$ pour $1 \leqslant p < \infty$, théorème 28.47.
(4) Densité de $\mathscr{S}(\mathbb{R}^d)$ dans l'espace de Sobolev $H^s(\mathbb{R}^d)$, proposition 32.15.
(5) Densité de $\mathscr{D}(\mathbb{R}^d)$ dans l'espace de Sobolev $H^s(\mathbb{R}^d)$, proposition 32.17.
Cela est utilisé pour le théorème de trace 32.19.
(6) Les applications étagées dans les applications mesurables (qui plus est avec limite croissante), théorème fondamental d'approximation 28.50.
(7) Les fonctions continues à support compact dans $L^2(I)$, théorème 28.51.
(8) Les polynômes trigonométriques sont denses dans $L^p(S^1)$ pour $1 \leqslant p < \infty$. Deux démonstrations indépendantes par le théorème 29.6 et le théorème 28.70.

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 18.121.

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

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

— Le lemme 13.299 le donne pour la racine carré.

— Le théorème 13.305 donne la densité des polynômes dans les fonctions continues sur un compact.

— Le théorème 13.302 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 13.303 donne le même résultat pour la densité dans $C(X, \mathbb{C})$.

— Le lemme 29.1 est une version pour les polynômes trigonométriques.

— Le lemme 13.299 est une cas particulier du théorème 13.305, mais nous en donnons une démonstration indépendante afin d'isoler la preuve de la généralisation 13.303. Une version pour les polynômes trigonométriques sera donnée dans le lemme 29.1.

Le théorème de Stone-Weierstrass est utilisé pour prouver la densité des polynômes trigonométriques dans les fonctions continues sur S^1, voir la proposition 28.87.

Thème 13 : espaces de fonctions En ce qui concerne les densités, voir le thème 12.

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

(1) La topologie des semi-normes est la définition 9.74.

(2) La définition 31.10 donne les topologies sur $C^\infty(\Omega)$, $\mathscr{D}(K)$ et $\mathscr{D}(\Omega)$.

(3) La topologie $*$-faible sur $\mathscr{D}'(\Omega)$ est donnée par la définition 31.17.

L'espace $L^2\big([0, 2\pi]\big)$ 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 28.72.

(2) Le produit scalaire $\langle f, g\rangle$ est donné en (28.331) et la base trigonométrique est (28.332).

(3) La densité des polynômes trigonométriques dans $L^p(S^2)$ est le théorème 28.70 ou le théorème 29.6, au choix.

(4) Une conséquence de cette densité est que le système trigonométrique est une base hilbertienne de L^2 par le lemme 28.107.

L'espace L^2 est discuté en analyse fonctionnelle, dans la section 28.4 et les suivantes parce que l'étude de L^2 utilise entre autres l'inégalité de Hölder 28.33.

Le fait que L^2 soit une espace de Hilbert est utilisé dans la preuve du théorème de représentation de Riesz 28.128.

Thème 14 : fonctions Lipschitz

(1) Définition : 13.254.

(2) La notion de Lipschitz est utilisée pour définir la stabilité d'un problème, définition 35.25.

Thème 15 : formule des accroissements finis Il en existe plusieurs formes :

(1) Une version adaptée aux espaces de dimension finie est le théorème 13.252.

(2) Pour les fonctions $\mathbb{R} \to \mathbb{R}$ en le théorème 13.129.

(3) Une généralisation pour les intervalles non bornés : théorème 13.130.

(4) Espaces vectoriels normés, théorème 12.151

Thème 16 : limite et continuité

(1) Limite d'une fonction en un point : définition 7.62. Il n'y a pas unicité en général comme le montre l'exemple 7.29 dans un espace non séparé.

(2) La proposition 9.83 donne l'unicité de la limite dans le cas des espaces duaux pour la topologie $*$-faible. La proposition 7.65 nous dira qu'il y a unicité dès que l'espace d'arrivée est séparé.

(3) Définition de la continuité d'une fonction en un point et sur une partie de l'espace de départ : définiton 7.66.

(4) Continuité sur une partie si et seulement si continue en chaque point, c'est le théorème 7.69.

(5) Voir l'exemple 13.64 traité en détail.

Thème 17 : différentiabilité

(1) Définition générale de la différentielle sur des espaces vectoriels normés : la proposition 12.133.

(2) Nous parlons de différentielle en dimension finie et donnons une interprétation géométrique en 13.20.1.

(3) La recherche d'extrema d'une fonction sur $\mathbb{R}^n$ passe par la seconde différentielle, proposition 18.70.

(4) Lien entre différentielle seconde (hessienne) et convexité en la proposition 18.94 et le corollaire 18.96.

(5) La différentielle est liée aux dérivées partielles par les formules données au lemme 13.195

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

Thème 18 : points fixes

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

Théorème de Picard 18.34 donne un point fixe comme limite d'itérés d'une fonction Lipschitz. Il aura pour conséquence le théorème de Cauchy-Lipschitz 18.40, l'équation de Fredholm, théorème 18.39 et le théorème d'inversion locale dans le cas des espaces de Banach 18.48.

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 21.30.

(1b) Dans $\mathbb{R}^n$ en version continue, en s'appuyant sur le cas C^∞ et en faisant un passage à la limite, théorème 21.31.

(1c) Dans $\mathbb{R}^2$ via l'homotopie, théorème 27.19. Oui, c'est très loin. Et c'est normal parce que ça va utiliser la formule de l'indice qui est de l'analyse complexe [2].

Théorème de Markov-Kakutani 21.36 qui donne un point fixe à une application continue d'un convexe fermé borné dans lui-même. Ce théorème donnera la mesure de Haar 21.37 sur les groupes compacts.

Théorème de Schauder 21.32 qui est une version valable en dimension infinie du théorème de Brouwer.

(2) Pour les équations différentielles

(2a) Le théorème de Schauder a pour conséquence le théorème de Cauchy-Arzela 21.33 pour les équations différentielles.

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

(2b) Le théorème de Schauder 21.32 permet de démontrer une version du théorème de Cauchy-Lipschitz (théorème 18.40) 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 35.47.
- La convergence quadratique de la méthode de Newton est donnée par le théorème 35.53.
- En calcul numérique, section 35.5
- Méthode de Newton comme méthode de point fixe, sous-section 35.6.2.

(4) D'autres utilisation de points fixes.
- Processus de Galton-Watson, théorème 39.48.
- Dans le théorème de Max-Milgram 26.59, le théorème de Picard est utilisé.

Thème 19 : théorèmes de Stokes, Green et compagnie

(1) Forme générale, théorème 21.73.

(2) Rotationnel et circulation, théorème 25.8.

Le théorème de Stokes peut être utilisé pour montrer le théorème de Brower, proposition 21.30.

Thème 20 : permuter des limites

Fonctions définies par une intégrale Les théorèmes sur les fonctions définies par une intégrale, section 18.4. Nous avons entre autres

(1) $\partial_i \int_B f = \int_B \partial_i f$, avec B compact, proposition 18.25.

(2) Si f est majorée par une fonction ne dépendant pas de x, nous avons le théorème 18.15.

(3) Si l'intégrale est uniformément convergente, nous avons le théorème 18.16 qui donne la continuité de $F(x) = \int_\Omega f(x,\omega)d\mu(\omega)$.

(4) Pour dériver $\int_B g(t,z)dt$ avec B compact dans $\mathbb{R}$ et $g\colon \mathbb{R}\times\mathbb{C}\to\mathbb{C}$, il faut aller voir la proposition 27.17.

(5) En ce qui concerne le x dans la borne, le théorème 15.232 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 15.233 en est une conséquence.

Conegence monotone Théorème de la convergence monotone, théorème 15.160.

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 comptage [3]. Nous utilisons cette technique pour permute une somme et une intégrale dans l'équation (27.131).
- le théorème de Fubini-Tonelli 15.256 demande que la fonction soit mesurable et positive ;
- le théorème de Fubini 15.259 demande que la fonction soit intégrable (mais pas spécialement positive) ;
- le corollaire 15.258 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, théorème 13.297.

(2) Permuter limite et dérivées partielles, théorème 13.298.

(3) Permuter limite et différentielle, théorème 16.6.

Quelque remarques sur les techniques de démonstration.

3. Mesure de comptage, définition 15.227.

(1) Le résultat fondamental 13.297 est démontré sans recourrir à des intégrales. Une preuve alternative, plus courte, avec des intégrales est donnée en 15.240.
(2) Les résultats un peu plus élaborés 13.298 et 16.6 sont prouvés avec des intégrales, mais devraient pouvoir être adaptés.

Somme et dérivée Permuter somme et différentielle, théorème 16.6.

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 15.20(2).

Thème 21 : applications continues et bornées

(1) Une application linéaire non continue : exemple 12.34 de $e_k \mapsto ke_k$. Les dérivées partielles sont calculées en (26.135).
(2) Une autre application linéaire non continue en l'exemple 12.35 : la dérivation sur les polynômes.
(3) Une application linéaire est bornée si et seulement si elle est continue, proposition 12.25.

Thème 22 : inégalités

Inégalité de Jensen (1) Une version discrète pour $f\big(\sum_i \lambda_i x_i\big)$, la proposition 18.100.
(2) Une version intégrale pour $f\big(\int \alpha d\mu\big)$, la proposition 28.31.
(3) Une version pour l'espérance conditionnelle, la proposition 37.52.

Inégalité pour les normes ℓ^p (1) Hölder pour L^p : $\|fg\|_1 \leqslant \|f\|_p \|g\|_q$, proposition 28.33.
(2) Hölder pour ℓ^p : $\|x\|_q \leqslant n^{\frac{1}{q}-\frac{1}{p}}\|x\|_p$, proposition 18.106.
<++>

Inégalité de Minkowsky (1) Pour une forme quadratique q sur $\mathbb{R}^n$ nous avons $\sqrt{q(x+y)} \leqslant \sqrt{q(x)} + \sqrt{q(y)}$. Proposition 11.281.
(2) Si $1 \leqslant p < \infty$ et si $f, g \in L^p(\Omega, \mathcal{A}, \mu)$ alors $\|f+g\|_p \leqslant \|f\|_p + \|g\|_p$. Proposition 28.37.
(3) L'inégalité de Minkowsky sous forme intégrale s'écrit sous forme déballée

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

ou sous forme compacte

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

Transformée de Fourier Pour tout $f \in L^1(\mathbb{R}^n)$ nous avons $\|\hat{f}\|_\infty \leqslant \|f\|_1$, lemme 30.8.

Inégalité des normes Inégalité de normes : si $f \in L^p$ et $g \in L^1$, alors $\|f * g\|_p \leqslant \|f\|_p \|g\|_1$, proposition 28.56.

Thème 23 : connexité

(1) Définition 7.38
(2) Une partie de $\mathbb{R}$ est connexe si et seulement si elle est un intervalle, proposition 8.34.
(3) Le groupe $\mathrm{SL}(n, \mathbb{K})$ est connexe par arcs : proposition 14.17.
(4) Le groupe $\mathrm{GL}(n, \mathbb{C})$ est connexe par arcs : proposition 14.18.
(5) Le groupe $\mathrm{GL}(n, \mathbb{C})$ est connexe par arcs, proposition 14.18.
(6) Le groupe $\mathrm{GL}(n, \mathbb{R})$ a exactement deux composantes connexes par arcs, proposition 14.19.
(7) Le groupe $\mathrm{O}(n, \mathbb{R})$ n'est pas connexe, lemme 14.13.
(8) Les groupe $\mathrm{U}(n)$ et $\mathrm{SU}(n)$ sont connexes par arcs, lemme 14.14.
(9) Le groupe $\mathrm{SO}(n)$ est connexe mais ce n'est pas encore démontré, proposition 14.15.
(10) Connexité des formes quadratiques de signature donnée, proposition 18.112.

Thème 24 : suite de Cauchy, espace complet Nous parlons d'espaces topologiques complets. À ne pas confondre avec un espace mesuré complet, définition 15.56.

(1) Corps complet : définition 1.73(6), espace métrique complet : définition 9.22.
(2) La définition 9.21 donne la notion de suite de Cauchy dans un espace métrique.
(3) La définition 9.19 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 9.25.
(5) La proposition 9.26 donne l'équivalence entre les suites de Cauchy et les suites τ-Cauchy dans le cas des espaces vectoriels topologiques *normés*.
(6) L'exemple 9.25 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 18.125 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 9.39(2).
(9) Toute suite convergente dans un espace métrique est de Cauchy, propostion 9.27.

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 pout une distance et pas pour une autre. Souvent, cependant la distance à considérer est donnée par le contexte.

(1) Les réels $\mathbb{R}$, théorème 9.39.
(2) Un espace vectoriel normé sur un corps complet est complet, proposition 9.43.
(3) La proposition 13.282 donne quelques espaces complets. Soit X un espace topologique métrique (Y, d) un espace espace métrique complet. Alors les espaces
   (3a) $\left(C_b^0(X,Y), \|.\|_\infty\right)$
   (3b) $\left(C_0^0(X,Y), \|.\|_\infty\right)$
   (3c) $\left(C_0^k(X,Y), \|.\|_\infty\right)$
   sont complets.
(4) Le lemme 13.283 dit que $\left(C^0(A,B), \|.\|_\infty\right)$ est complet dès que A est compact et B est complet.
(5) L'espace $\mathscr{D}(K)$ est complet tant pour la topologie des semi-normes que pour la topologie métrique (qui sont les mêmes). C'est la proposition 31.14.
(6) L'espace $\mathscr{S}(\Omega)$ est complet et métrisable par la proposition 31.56.
(7) L'espace $L^p(\Omega, \mathcal{A}, \mu)$ par le théorème 28.40.

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 13.305 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 $\left(C^p(X,Y), \|.\|_\infty\right)$ soit complet en général.

Thème 25 : application réciproque

(1) Définition 7.76.
(2) Dans le cas des réels, des exemples sont donnés en 13.7.
(3) Continuité, proposition 7.78.
(4) Théorème de la bijection 13.61 (qui contient aussi de la continuité).
(5) Dérivabilité, proposition 13.119.

Thème 26 : 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 15.179 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 28.59.

(3) Et encore un pour L^p dans la proposition 28.132.
(4) Si $\int f\chi = 0$ pour tout χ à support compact alors $f = 0$ presque partout, proposition 31.1.
(5) La proposition 28.22 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 18.2.

Thème 27 : 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-Arzela 21.33 pour les équations différentielles.
(2) Le théorème de Schauder 21.32 permet de démontrer une version du théorème de Cauchy-Lipschitz (théorème 18.40) sans la condition Lipschitz
(3) Le théorème de Cauchy-Lipschitz 18.40 est utilisé à plusieurs endroits :
   — Pour calculer la transformée de Fourier de $e^{-x^2/2}$ dans le lemme 30.17.
(4) Théorème de stabilité de Lyapunov 33.34.
(5) Le système proie-prédateur de Lotka-Volterra 33.35
(6) Équation de Schrödinger, théorème 33.41.
(7) L'équation $(x - x_0)^\alpha u = 0$ pour $u \in \mathscr{D}'(\mathbb{R})$, théorème 31.64.
(8) La proposition 33.37 donne un résultat sur $y'' + qy = 0$ à partir d'une hypothèse de croissance.
(9) Équation de Hill $y'' + qy = 0$, proposition 33.39.

Thème 28 : injections

(1) L'espace de Sobolev $H^1(I)$ s'injecte de façon compacte dans $C^0(\bar{I})$, proposition 32.6.
(2) L'espace de Sobolev $H^1(I)$ s'injecte de façon continue dans $L^2(I)$, proposition 32.6.
(3) L'espace $L^2(\Omega)$ s'injecte continument dans $\mathscr{D}'(\Omega)$ (les distributions), proposition 31.20.

Thème 29 : logarithme

(1) Le logarithme pour les réels strictement positifs $\ln\colon]0,\infty[\to \mathbb{R}$ est donné en la définition 16.58.
(2) Les principales propriétés sont dans la proposition 16.60 : $\ln(xy) = \ln(x) + \ln(y)$ etc.
(3) La proposition 16.74 donne la série

$$\ln(1+x) = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} x^k. \tag{-2.2}$$

(4) L'exemple 21.148 donne l'encadrement $0.644 \leqslant \ln(2) \leqslant 0.846$.
(5) La proposition 16.94 dit que toute matrice complexe admet un logarithme. En particulier une série explicite est donné pour le logarithme d'un bloc de Jordan.
(6) Sur les complexes, le logarithme $\ln\colon \mathbb{C}^* \to \mathbb{C}$ est la définition 27.54. 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 16.83.

Thème 30 : inversion locale, fonction implicite

Des énoncés (1) Inversion locale dans $\mathbb{R}^n$: théorème 18.47. Pour un Banach c'est le théorème 18.48.
(2) Fonction implicite dans un Banach : théorème 18.49.

Des utilisations (1) Utilisé pour montrer que le flot d'une équation différentielle est un C^p-difféomorphisme local, voir 33.30.
(2) Pour le théorème de Von Neumann 18.62.

Thème 31 : convexité L'essentiel des résultats sur les fonctions convexes sont dans la section 18.11. On a surtout :

(1) Définition des fonctions convexes : 18.76 et 18.92 en dimension supérieure.
(2) En termes de différentielles, 18.93 pour la différentielle première et 18.96 pour la hessienne.
(3) Une courbe paramétrée convexe est la définition 22.87.
(4) L'enveloppe convexe d'une courbe fermée simple et convexe : 22.89.
(5) Courbure et convexité d'une courbe paramétrée : section 22.12.4.
(6) Une courbe paramétrée convexe est localement le graphe d'une fonction convexe par le lemme 22.88.
(7) La convexité est utilisée dans la méthode du gradient à pas optimal de la proposition 18.109.

En terme de parties convexes, on :

(1) Définition 10.24 d'une partie convexe d'un espace vectoriel.
(2) Une boule est convexe, exemple 10.25.

Thème 32 : fonction puissance Il y a beaucoup de choses à dire...

Définition Nous considérons, pout $a > 0$, la fonction $g_a : \mathbb{R} \to \mathbb{R}$ 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 1.59.
(2) a^n pour $n \in \mathbb{Z}$ en la définition 13.309.
(3) $a^{1/n}$ pour $n \in \mathbb{Z}$ en la définition 13.311.
(4) a^q pour $q \in \mathbb{Q}$ en la définition 13.311.
(5) $\sqrt[n]{x}$ en la définition 13.313.
(6) La fonction g_a est Cauchy-continue sur $\mathbb{Q}$, c'est la proposition 13.324.
(7) a^x pour $a > 0$ et $x \in \mathbb{R}$ en la définition 13.326.
(8) a^z pour $a > 0$ et $z \in \mathbb{C}$ en la définition 19.19.

Quelque propriétés (1) Pour tout $q \in \mathbb{Q}$, il y a un $\sqrt{q}$ dans $\mathbb{R}$, proposition 1.130.
(2) Si $a > 0$ et $x, y \in \mathbb{R}$ nous avons $(a^x)^y = (a^y)^x = a^{xy}$ par la proposition 13.337.
(3) La fonction puissance est strictement croissante (en ses deux arguments), proposition 13.332.

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 fonctions puissance est strictement croissante, proposition 13.332
(2) La fonction a^x est dérivable et sa dérivée vérifie $g'_a(x) = g_a(x)g'_a(0)$, proposition 13.340.
(3) La formule de dérivation pour $x \mapsto x^q$ avec $q \in \mathbb{Q}$ est la proposition 13.349.
(4) La dérivation de $x \mapsto x^\alpha$ avec $\alpha \in \mathbb{R}$ est la proposition 15.242. 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 16.66).

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

$$f(x + y) = f(x)f(y) \tag{-2.3}$$

en la définition 13.342.

(1) Équivanlence entre l'équation fonctionnelle et l'équation différentielle, proposition 13.347.

(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 13.342 et les choses qui suivent.

(3) L'équation fonctionnelle pour une fonction continue $f\colon \mathbb{R} \to S^1$ est traitée dans la proposition 13.353.

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 16.57).
— Définir $e = \exp(1)$.
— Définir, pour x irrationnel, $a^x = \exp(x\ln(a))$.
— Prouver que $e^x = \exp(x)$ pour tout x.

Thème 33 : dualité Ne pas confondre dual algébrique et dual topologique d'un espace vectoriel.

(1) Définition de la base duale 4.113.

Dual topologique et algébrique Ils sont définis par 4.112. 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 9.81.

Nous comparons les topologies faibles et de la norme en la section 12.11.

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

(1) Le théorème de représentation de Riesz 26.17 pour les espaces de Hilbert.
(2) La proposition 28.128 pour les espaces $L^p\big([0,1]\big)$ avec $1 < p < 2$.
(3) Le théorème de représentation de Riesz 28.130 pour les espaces L^p en général.

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

Thème 34 : opérations sur les distributions

(1) Convolution d'une distribution par une fonction, définition par l'équation (31.96).
(2) Dérivation d'une distribution, proposition-définition 31.22.
(3) Produit d'une distribution par une fonction, définition 31.21.

Thème 35 : transformée de Fourier

(1) Définition sur L^1, définition 30.1.
(2) La transformée de Fourier d'une fonction $L^1(\mathbb{R}^d)$ est continue, proposition 30.7.
(3) L'espace de Schwartz est stable par transformée de Fourier. L'application $\mathcal{F}\colon \mathscr{S}(\mathbb{R}^d) \to \mathscr{S}(\mathbb{R}^d)$ est une bijection linéaire et continue. Proposition 30.14

Thème 36 : convolution

(1) Définition 28.52, et principales propriétés sur $L^1(\mathbb{R})$ dans le théorème 28.53.
(2) Inégalité de normes : si $f \in L^p$ et $g \in L^1$, alors $\|f * g\|_p \leqslant \|f\|_p \|g\|_1$, proposition 28.56.
(3) $\varphi \in L^1(\mathbb{R})$ et $\psi \in \mathscr{S}(\mathbb{R})$, alors $\varphi * \psi \in \mathscr{S}(\mathbb{R})$, proposition 28.155.
(4) Les suites régularisantes : $\lim_{n\to\infty} \rho_n * f = f$ dans la proposition 30.19.
(5) Convolution d'une distribution par une fonction, définition par l'équation (31.96).

Thème 37 : méthode de Newton

(1) Nous parlons un petit peu de méthode de Newton en dimension 1 dans 35.6.
(2) La méthode de Newton fonctionne bien avec les fonctions convexes par la proposition 35.55.
(3) La méthode de Newton en dimension n est le théorème 35.61.
(4) Un intervalle de convergence autour de α s'obtient par majoration de $|g'|$, proposition 35.47.
(5) Un intervalle de convergence quadratique s'obtient par majoration de $|g''|$, théorème 35.53.
(6) En calcul numérique, section 35.6.

Thème 38 : méthodes de calcul

(1) Théorème de Rothstein-Trager 21.95.
(2) Algorithme des facteurs invariants 4.106.
(3) Méthode de Newton, théorème 35.61
(4) Calcul d'intégrale par suite équirépartie 29.8.

Thème 39 : espaces vectoriels

(1) Existence d'une base. Pour un espace vectoriel quelconque, proposition 4.20.
(2) Théorème de la base incomplète. Pour un espace vectoriel quelconque, théorème 4.21.

<++>

Thème 40 : définie positive

(1) Une application bilinéaire est définie positive lorsque $g(u,u) \geqslant 0$ et $g(u,u) = 0$ si et seulement si $u = 0$ est la définition 11.4.
(2) Un opérateur ou une matrice est défini positif si toutes ses valeurs propres sont positives, c'est la définition 11.191.
(3) Pour une matrice symétrique, définie positive si et seulement si $\langle Ax, x\rangle > 0$ pour tout x. C'est le lemme 11.196.
(4) Une application linéaire est définie positive si et seulement si sa matrice associée l'est. C'est la proposition 11.195.

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

Thème 41 : norme matricielle, norme opérateur et rayon spectral Quelque définitions

(1) Définition de la norme opérateur : définition 12.10.
(2) Définition du rayon spectral 12.15.

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 12.27 assure que $\|A\|_2 = \sqrt{\rho(A^tA)}$.
(2) Lien entre valeurs propres et norme opérateur : le lemme 12.28 pour les matrices symétriques strictement définies positives donne $\|A\|_2 = \lambda_{max}$.
(3) Pour toute norme algébrique nous avons $\rho(A) \leqslant \|A\|$, proposition 12.22.
(4) Dans le cadre du conditionnement de matrice. Voir en particulier la proposition 35.108 qui utilise le théorème 12.27.
(5) Rayon spectral et convergence de méthode itérative, proposition 35.144.

Pour la norme opérateur nous avons les résultats suivants.

(1) La majoration $\|Au\| \leqslant \|A\|\|u\|$ est le lemme 12.17.

(2) Définition d'une algèbre : 3.71 et pour une norme d'algèbre : 12.14.

(3) La norme opérateur est une norme d'algèbre, lemme 12.20.

(4) Pour des espaces vectoriels normés, être borné est équivalent à être continu : proposition 12.25.

(5) Le lemme à propos d'exponentielle de matrice 16.117 donne :

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

La norme opérateur est utilisée pour donner une norme sur les produits tensoriels, définition 12.129.

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 42.

Thème 42 : série de matrices

(1) Rayon spectral et norme opérateur : thème 41.

(2) Exponentielle de matrices : thème 56.

(3) Série entière de matrices : section 16.12.

(4) Pour la série $\sum_k A^k = (1-A)^{-1}$.

— Pour un espace de Banach : proposition 12.158.

— Pour les matrices nilpotentes : proposition 11.162.

— En lien avec le rayon spectral (si et seulement si $\rho(A) < 1$) dans la proposition 16.113.

— Le lemme 16.28 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 35.164 pour prouver qu'une M-matrice irréductible vérifie $A^{-1} > 0$.

Thème 43 : rang

(1) Définition 4.38.

(2) Le théorème du rang, théorème 4.39

(3) Prouver que des matrices sont équivalentes et les mettre sous des formes canoniques, lemme 4.104 et son corollaire 4.105.

(4) Tout hyperplan de $\mathbb{M}(n,\mathbb{K})$ coupe $\mathrm{GL}(n,\mathbb{K})$, corollaire 4.105. Cela utilise la forme canonique sus-mentionnée.

(5) Le lien entre application duale et orthogonal de la proposition 4.121 utilise la notion de rang.

(6) Le lemme 11.252 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 11.253.

Thème 44 : extension de corps et polynômes

(1) Définition d'une extension de corps 6.51.

(2) Pour l'extension du corps de base d'un espace vectoriel et les propriétés d'extension des applications linéaires, voir la section 11.14.

(3) Extension de corps de base et similitude d'application linéaire (ou de matrices, c'est la même chose), théorème 11.255.

(4) Extension de corps de base et cyclicité des applications linéaires, corollaire 11.254.

(5) À propos d'extensions de $\mathbb{Q}$, le lemme 6.155.

(6) Corps de rupture : définition 6.102 existence par la proposition 6.109. Il n'y a pas unicité.

(7) Corps de décomposition : définition 6.118. Attention : le plus souvent nous parlons de corps de décomposition d'un seul polynôme. Cette définition est un peu surfaite. Existence par la proposition 6.119 qui le donne même comme extension par toutes les racines, et unicité à isomorphisme près par le théorème 6.121, énoncé de façon plus simple (mais pas indépendante !) en la proposition 6.122.

Un trio de résutats 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 3.102).

(2) Dans un anneau, un idéal I est maximam 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 3.163).

Thème 45 : décomposition de matrices

(1) Décomposition de Bruhat, théorème 14.37.

(2) Décomposition de Dunford, théorème 11.216.

(3) Décomposition polaire 14.31 et la proposition 18.58 pour la régularité.

Thème 46 : systèmes d'équations linéaires

— Algorithme des facteurs invariants 4.106.

— 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 choisit. Propositions 18.108 pour l'existence et 18.109 pour la méthode.

Thème 47 : formes bilinéaires et quadratiques

(1) Les formes bilinéaires sont définies en 11.1.

(2) Forme quadratique, définition 11.199

(3) Une isométrie d'une forme bilinéaire est affine ou linéaire, théorème 11.269.

(4) Forme bilinéaire dégénérée, définition 11.266.

(5) Une forme bilinéaire est non-dénénérée si et seulement si sa matrice associée est inversible, c'est la proposition 11.268.

(6) Une isométrie d'une forme bilinéaire est linéaire ou affine par le théorème 11.269.

Thème 48 : arithmétique modulo, théorème de Bézout

(1) Pour $\mathbb{Z}^*$ c'est le théorème 3.13.

(2) Théorème de Bézout dans un anneau principal : corollaire 3.111.

(3) Théorème de Bézout dans un anneau de polynômes : théorème 6.40.

(4) En parlant des racines de l'unité et des générateurs du groupe unitaire dans le lemme 20.4. Au passage nous y parlerons de solfège.

(5) La proposition 3.15 qui donne tout entier assez grand comme combinaisons de a et b à coefficients positifs est utilisée en chaînes de Markov, voir la définition 39.42 et ce qui suit.

(6) PGCD et PPCM sont dans la définition 1.46.

(7) Calcul effectif du PGCD puis des coefficients de Bézout : sous-sections 3.3.4.1 et 3.3.4.2.

Thème 49 : 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) $A[X]$, définition 3.145 ; 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 3.147.

(2) Liens entre $\mathbb{K}[\alpha]$, $\mathbb{K}[X]$, $\mathbb{K}(\alpha)$ et $\mathbb{K}(X)$ lorsque α est transcendant, proposition 6.82. Et la proposition 6.85 pour le cas où α est algébrique.

(3) 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 3.155.

(4) $\mathbb{K}(X)$, le corps des fractions de $\mathbb{K}[X]$, définition 6.72. Si $R = P/Q$ dans $\mathbb{K}(X)$, l'évaluation est $R(\alpha) = P(\alpha)Q(\alpha)^{-1}$, définition 6.73.

(5) $\mathbb{K}(\alpha)_{\mathbb{L}}$ est le plus petit corps de $\mathbb{L}$ contenant $\mathbb{K}$ et α, définition 6.74.

(6) À propos de polynômes à plusieurs variables.

— Anneau de polynômes : $A[X_1, \dots, X_n]$ est la définition 3.182.

— Corps engendré : $\mathbb{K}(\alpha_1, \dots, \alpha_n)$ est la définition 6.115.

— Corps des fractions rationnelles : $\mathbb{K}(X_1, \dots, X_n)$ est la définition 6.116.

Coefficients dans un anneau commutatif (1) Les polynômes à coefficients dans un anneau commutatif sont à la section 3.13.

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 6.36.

(2) Le théorème 6.36 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 6.49.

Polynôme primitif (1) Un polynôme est irréductible sur A si et seulement si irréductible et primitif sur le corps des fractions, corollaire 3.179.

Polynôme d'endomorphisme C'est la section 11.8.

Racines et factorisation (1) Si $\mathbb{A}$ est un anneau, la proposition 3.173 factorise une racine.

(2) Si $\mathbb{A}$ est un anneau, la proposition 3.175 factorise une racine avec sa multiplicité.

(3) Si $\mathbb{A}$ est un anneau, le théorème 3.177 factorise plusieurs racines avec leurs multiplicités.

(4) Le théorème 3.177 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 6.83.

(6) Le théorème 6.99 annule un polynôme de degré n ayant $n+1$ racines distinctes.

(7) La proposition 6.158 nous annule un polynôme à plusieurs variables lorsqu'il a trop de racines.

(8) En analyse complexe, le principe des zéros isolés 27.20 annule en gros toute série entière possédant un zéro non isolé.

(9) Polynômes irréductibles sur $\mathbb{F}_q$.

Thème 50 : zoologie de l'algèbre Nous listons ici un peu tous les termes qui arrivent en algèbre.

Éléments Pour les éléments, nous avons :

(0a) Élément irréductible en 3.88.

(0b) Élément premier en 3.113.

Anneaux Pour les anneaux, nous avons :

(0a) Anneau factoriel en 3.92.

(0b) Anneau principal en 3.96.

(0c) Anneau intègre en 1.54.

(0d) Anneau noetherien en 3.119.

Idéaux Pour les idéaux, nous avons :

(0a) Idéal principal en 3.95.

(0b) Idéal premier en 3.97.

Thème 51 : invariants de similitude

(1) Théorème 11.241.

(2) Pour prouver que la similitude d'applications linéaires résiste à l'extension du corps de base, théorème 11.255.

(3) Pour prouver que la dimension du commutant d'un endomorphisme de E est de dimension au moins $\dim(E)$, lemme 11.252.

(4) Nous verrons dans la remarque 11.242 à propos des invariants de similitude que toute matrice est semblable à la matrice bloc-diagonale constituées des matrices compagnon (définition 11.236) de la suite des polynômes minimals.

Thème 52 : diagonalisation Des résultats qui parlent diagonalisation

(1) Définition d'un endomorphisme diagonalisable : 11.164.

(2) Conditions équivalentes au fait d'être diagonalisable en termes de polynôme minimal, y compris la décomposition en espaces propres : théorème 11.167.

(3) Diagonalisation simultanée 11.170, pseudo-diagonalisation simultanée 11.274.

(4) Diagonalisation d'exponentielle 16.95 utilisant Dunford.

(5) Décomposition polaire théorème 14.31. $M = SQ$, S est symétrique, réelle, définie positive, Q est orthogonale.

(6) Décomposition de Dunford 11.216. $u = s + n$ où s est diagonalisable et n est nilpotent, $[s, n] = 0$.

(7) Réduction de Jordan (bloc-diagonale) 11.244.

(8) L'algorithme des facteurs invariants 4.106 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 11.189. Via le lemme de Schur complexe 11.176.

(2) Théorème spectral autoadjoint (c'est le même, mais vu sans matrices), théorème 11.287

(3) Théorème spectral hermitien, lemme 11.183.

(4) Théorème spectral, matrice normales, théorème 11.186.

Pour les résultats de décomposition dont une partie est diagonale, voir le thème 45 sur les décompositions.

Thème 53 : endomorphismes cycliques

(1) Définition 11.138.

(2) Son lien avec le commutant donné dans la proposition 11.250 et le théorème 11.253.

(3) Utilisation dans le théorème de Frobenius (invariants de similitude), théorème 11.241.

Thème 54 : déterminant

(1) Déterminant d'une matrice : définition 4.68.

(2) Déterminant d'un endomorphisme 11.50.

(3) Principales propriétés algébriques du déterminant : la proposition 11.52.

(4) Déterminant et manipulations de lignes et colonnes, section 4.3.10 et les propositions qui précèdent à partir du lemme 4.70 qui dit que $\det(A) = \det(A^t)$.

(5) Les n-formes alternées forment un espace de dimension 1, proposition 11.45.

(6) Déterminant d'une famille de vecteurs 11.46.

(7) Calcul d'un déterminant de taille 2×2 : équation (4.88).

(8) Interprétations géométriques

(8a) 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 11.38.

ii. En particulier le lemme 11.39 nous dit comment un déterminant donne un vecteur orthogonal à une famille donnée de vecteurs.

(8b) Déterminant et aires, volumes

i. Déterminant et mesure de Lebesgue : théorème 15.251.

ii. Aire du parallélogramme : proposition 19.56.

iii. Volume du parallélépipède avec le produit mixte et le déterminant 3×3, 19.57.

Tant que nous en sommes dans les interprétations géométrique, 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 (21.186) : $dS = \|T_u \times T_v\|$ qui est la norme du produit vectoriel des vecteurs tangents à la paramétrisation.

Nous voyons dans l'équation (21.183) 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 de la paramétrisation.

(9) Le déterminant de Vandermonde est à la proposition 11.54. Il est utilisé à divers endroits :

(9a) Pour prouver que u est nilpotente si et seulement si $\mathrm{Tr}(u^p) = 0$ pour tout p (lemme 11.160)

(9b) Pour prouver qu'un endomorphisme possédant $\dim(E)$ valeurs propres distinctes est cyclique (proposition 11.250).

Thème 55 : polynôme d'endomorphismes

(1) Endomorphismes cycliques et commutant dans le cas diagonalisable, proposition 11.250.

(2) Racine carré d'une matrice hermitienne positive, proposition 14.26.

(3) Théorème de Burnside sur les sous-groupes d'exposant fini de $\mathrm{GL}(n, \mathbb{C})$, théorème 11.262.

(4) Décomposition de Dunford, théorème 11.216.

(5) Algorithme des facteurs invariants 4.106.

Thème 56 : 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 16.37.

— Nous démontrons qu'elle vérifie l'équation différentielle $y' = y$, $y(0) = 1$ (théorème 16.54).
— 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 16.58).
— Les fonctions trigonométriques (sinus et cosinus) sont définies par leurs séries. Il est alors montré que $e^{ix} = \cos(x) + i\sin(x)$.

Complexes (1) Le fait que $e^{i\theta}$ donne tous les nombres complexes de norme 1 est la proposition 19.60.

(2) Le groupe des racines de l'unité est donné par l'équation (20.1).

Algèbre normée commutative Pour la définition c'est la proposition 16.37 et pour la régularité C^∞ c'est la proposition 16.41.

Idem non commutatif Il y a une tentative de théorème 16.42, 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) Les sections 12.10 et 16.4.4 parlent d'exponentielle de matrices.
(2) L'exponentielle donne lieu à une fonction de classe C^∞, proposition 16.114.
(3) Le lemme à propos d'exponentielle de matrice 16.117 donne :

$$\|e^{tA}\| \leqslant P\big(|t|\big) \sum_{i=1}^{r} e^{t\,\mathrm{Re}(\lambda_i)}.$$

(4) La proposition 16.95 : 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.
(5) La section 16.12.3 parle des fonctions exponentielle et logarithme pour les matrices. Entre autres la dérivation et les séries.
(6) Pour résoudre des équations différentielles linéaires : sous-section 33.6.1.
(7) La proposition 16.94 dit que l'exponentielle est surjective sur $\mathrm{GL}(n,\mathbb{C})$.
(8) La proposition 12.161 : si u est un endomorphisme, alors $\exp(u)$ est un polynôme en u.
(9) Calcul effectif : sous-section 16.12.4.
(10) Proposition 14.22 : si $A \in \mathbb{M}(n,\mathbb{C})$ alors $e^{\mathrm{Tr}(A)} = \det(e^A)$.
(11) Les séries entières de matrices sont traitées autour de la proposition 16.111.

Thème 57 : types d'anneaux Définition d'anneau : définition 1.37.

(1) $\mathbb{Z}$ est intègre, exemple 3.75, principal et euclidien (proposition 3.132).
(2) $\mathbb{Z}[X]$ n'est pas principal (voir (3)).
(3) Si A est un anneau intègre qui n'est pas un corps, alors $A[X]$ n'est pas principal, lemme 3.133.
(4) L'anneau des fonctions holomorphes sur un compact donné est principal, proposition 27.24.
(5) L'anneau $\mathbb{Z}[i\sqrt{3}]$ n'est pas factoriel, exemple 3.94.
(6) L'anneau $\mathbb{Z}[i\sqrt{5}]$ n'est ni factoriel ni principal, exemple 3.123.
(7) Tous les idéaux de $\mathbb{Z}/6\mathbb{Z}$ sont principaux, mais $\mathbb{Z}/6\mathbb{Z}$ n'est pas principal. Exemple 3.106.

Thème 58 : sous-groupes

(1) Théorème de Burnside sur les sous-groupes d'exposant fini de $\mathrm{GL}(n,\mathbb{C})$, théorème 11.262.
(2) Sous-groupes compacts de $\mathrm{GL}(n,\mathbb{R})$, lemme 14.38 ou proposition 14.39.

Thème 59 : groupe symétrique

(1) Définition 2.60.

(2) La signature $\epsilon\colon S_n \to \{-1,1\}$ est l'unique homomorphisme surjectif de S_n sur $\{-1,1\}$, proposition 2.73(1).

(3) La table des caractères du groupe symétrique S_4 est donné dans la section 17.5.

(4) Le groupe symétrique S_4 est le groupe des symétries affines du tétraèdre régulier, proposition 19.12.

(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 60 : action de groupe

(1) Définition d'une action de groupe sur un ensemble : 2.43.

(2) Action du groupe modulaire sur le demi-plan de Poincaré, théorème 24.93.

(3) La formule de Burnside (théorème 2.56) 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, 19.9.2.1 et 19.9.2.2.

(5) Le groupe symétrique S_n agit sur l'anneau $\mathbb{K}[T_1,\dots,T_n]$, lemme 6.150.

Thème 61 : 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 11.262.

(6) $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$, corollaire 20.34.

Thème 62 : produit semi-direct de groupes

(1) Définition 2.76.

(2) Le corollaire 2.78 donne un critère pour prouver qu'un produit NH est un produit semi-direct.

(3) L'exemple 19.96 donne le groupe des isométries du carré comme un produit semi-direct.

(4) Le théorème 5.25 classifie les groupes d'ordre pq (p, q premiers distincts) à grands coups de produit semi-directs.

(5) Le théorème 19.1 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.

(6) La proposition 19.3 donne une décomposition du groupe orthogonal $\mathrm{O}(n) = \mathrm{SO}(n) \times_\rho C_2$ où $C_2 = \{\mathrm{Id}, R\}$ où R est de déterminant -1.

(7) La proposition 10.57 donne $\mathrm{Aff}(\mathbb{R}^n) = T(n) \times_\rho \mathrm{GL}(n,\mathbb{R})$ où $\mathrm{Aff}(\mathbb{R}^n)$ est le groupe des applications affines bijectives de $\mathbb{R}^n$.

Thème 63 : théorie des représentations

(1) Définition 4.128.

(2) Table des caractères du groupe diédral, section 19.15.

(3) Table des caractères du groupe symétrique S_4, section 17.5.

Thème 64 : isométries Il y a $(\mathbb{R}^n, \|.\|)$ et $\mathbb{R}^n, d$.

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

Ne pas confondre une isométrie d'un espace affine avec une isométrie d'un espace euclidien. Les isométrie d'un espace euclidien préservent le produit scalaire et fixent donc l'origine (lemme 11.16). Les isométrie des espaces affines par contre conservent les distances (définition 10.58) et peuvent donc déplacer l'origine de l'espace vectoriel sur lequel il est modelé ; 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 Quelque résultats généraux et en vrac à propos d'isométries.

(1) Définition d'une isométrie pour une forme bilinéaire, 11.204. Pour une forme quadratique : définition 11.203.

(2) Définition du groupe orthogonal 11.81, et le spécial orthogonal $\mathrm{SO}(n)$ en la définition 11.84. Le groupe $\mathrm{SO}(2)$ est le groupe des rotations, par corollaire 19.137.

(3) La rotation $R_A(\theta)$ d'un angle θ autour du point $A \in \mathbb{R}^2$ est donnée par la définition 19.126.

(4) La proposition 19.138 donne à toute rotation $R_0(\theta)$ une matrice de la forme connue. C'est autour de cela que nous définissons les angles, définition 19.156.

(5) Le groupe orthogonal est le groupe des isométries de $\mathbb{R}^n$, proposition 11.83.

(6) Les isométries de l'espace euclidien sont affines, 11.269.

(7) Les isométries de l'espace euclidien comme produit semi-direct : $\mathrm{Isom}(\mathbb{R}^n) \simeq T(n) \times_\rho \mathrm{O}(n)$, théorème 19.1.

(8) Isométries du cube, section 5.7.

(9) Nous parlons des isométries affines du tétraèdre régulier dans la proposition 19.12.

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

(1) Générateurs du groupe diédral, proposition 19.94.

(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 19.164.

(3) Le théorème 19.166 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 quelque énoncés à ce propos.

(1) Définition d'une réflexion dans $\mathbb{R}^2$ 19.120.

(2) La caractérisation en termes de projection orthogonale est le lemme 19.109 ; en terme de médiatrice c'est le lemme 19.112.

(3) Définition d'un hyperplan 11.256.

(4) En dimension 2, une rotation est définie comme composée de deux réflexions en la définition 19.117.

(5) En dimension 2, les réflexion ont un déterminant -1 par le lemme 19.130.

(6) Les isométries du plan $(\mathbb{R}^2, d)$ sont données dans le théorème 19.163, et sont au plus 3 réflexions par le théorème 19.161.

(7) Décomposition des isométries de $\mathbb{R}^n$ en réflexions par le lemme 19.79.

(8) En particulier, les éléments de $\mathrm{SO}(3)$ sont des compositions de deux réflexions par le corollaure 19.81.

(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 19.83.

Sous-groupe fini (1) Les sous-groupes finis des isométries de $(\mathbb{R}^2, d)$ sont cycliques, théorème 19.164.

(2) Les sous-groupes finis de SO(3) sont listés dans 19.188.

(3) Les sous groupes finis de SO(2) sont cycliques, lemme 19.141.

Thème 65 : caractérisation de distributions en probabilités

(1) La probabilité conjointe est la définition 37.19.

(2) La fonction de répartition est la définition 37.53.

(3) La fonction caractéristique est la définition 37.55.

Thème 66 : théorème central limite

(1) Pour les processus de Poisson, théorème 41.5.

Thème 67 : 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 30.13 sur $\mathscr{S}(\mathbb{R}^d)$

(2) Lemme 32.10 pour L^2.

L'autre lemme de transfert est en théorie des tribus, le résultat $\sigma\big(f^{-1}(\mathcal{C})\big) = f^{-1}\big(\sigma(\mathcal{C})\big)$ du lemme 15.47. Celui-ci est d'ailleurs plutôt nommé « lemme de transport ».

Thème 68 : 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 37.31.

Les autres sont listées ci-dessous.

Probabilité conditionnelle .

Plusieurs probabilités conditionnelles.

— D'un événement en sachant un autre : la définition 37.29 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 37.47 qui défini la variable aléatoire

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

Dans le cas continu, c'est la définition 37.48 :

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

— 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 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 $E(X|\mathcal{F}) = \texttt{proj}_K(X)$ où K est le sous-ensemble de $L^2(\Omega, \mathcal{A}, P)$ des fonctions $\mathcal{F}$-mesurables (théorème 37.31). Cela au sens des projections orthogonales.

— d'une variable aléatoire par rapport à une autre. La définition 37.33 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 raccourcis pour dire « sachant la tribu engendrée par X ».

Thème 69 : dénombrements

— Coloriage de roulette (19.9.2.1) et composition de colliers (19.9.2.2).

— Nombres de Bell, théorème 16.124.

— Le dénombrement des solutions de l'équation $\alpha_1 n_1 + \dots \alpha_p n_p = n$ utilise des séries entières et des décomposition de fractions en éléments simples, théorème 20.29.

Thème 70 : enveloppes

(1) L'ellipse de John-Loewner donne un ellipsoïde de volume minimum autour d'un compact dans $\mathbb{R}^n$, théorème 18.117.

(2) Le cercle circonscrit à une courbe donne un cercle de rayon minimal contenant une courbe fermée simple, proposition 22.86.

(3) Enveloppe convexe du groupe orthogonal 14.36.

(4) Enveloppe convexe d'une courbe fermée plane comme intersection des demi-plans tangents, proposition 22.92.

Thème 71 : équations diophantiennes

(1) Équation $ax + by = c$ dans $\mathbb{N}$, équation (3.58).

(2) Dans 3.3.8, nous résolvons $ax + by = c$ en utilisant Bézout (théorème 3.13).

(3) L'exemple 3.137 donne une application de la pure notion de modulo pour $x^2 = 3y^2 + 8$. Pas de solutions.

(4) L'exemple 3.138 résout l'équation $x^2 + 2 = y^3$ en parlant de l'extension $\mathbb{Z}[i\sqrt{2}]$ et de stathme.

(5) Les propositions 3.142 et 3.144 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 décomposition de fractions en éléments simples, théorème 20.29.

(7) La proposition 1.50 donne une bijection $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ en résolvant dans $\mathbb{N}$ (entre autres) l'équation $k = y^2 + x$ pour k fixé.

Thème 72 : techniques de calcul Il y en a pour tous les gouts.

Primitives et intégrales Toute la section 18.12 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 19.190) ou autres fonctions trigonométriques. Ils sont donc placés beaucoup plus bas que la théorie.

— Méthode du développement asymptotique, sous-section 19.13.2.

— Méthode des coordonnées polaires, sous-section 19.13.1.

— Utilisation du théorème de la fonction implicite, dans l'exemple 19.192.

Conventions et notations

Il y a quelque conventions et notations par-ci par-là. En voici une liste.

— Matrice, application linéaires et changement de bases, c'est la section 11.11.

<++>

Table des matières

Index

Liste des notations

$N \lhd G$ Le sous-groupe N est normal dans G, page 141

Algèbre

$[\mathbb{L} : \mathbb{K}]$ degré d'une extension de corps, page 304

$\mathcal{L}(E, F)$ Ensemble des applications linéaires de E dans F, page 223

$\mathbb{K}(A)$ corps contenant $\mathbb{K}$ et A, page 317

$\mathbb{K}[A]$ anneau contenant $\mathbb{K}$ et A, page 317

$\mathbb{N}_0$ les naturels non nuls : $\mathbb{N}_0 = \mathbb{N}\backslash\{0\}$, page 109

$\mathcal{M}_{n\times m}$ l'ensemble des matrices $n \times m$, page 223

∇f gradient de la fonction f, page 734

$\mathtt{proj}_V$ projection de $V \times W$ sur V, page 575

$\mathrm{Span}(A)$ l'ensemble des combinaisons linéaires finies d'éléments de A, page 215

$C^1(U, \mathbb{R}^n)$ Les applications une fois continument dérivables, page 747

$df_a(u)$ Application de la différentielle de f sur le vecteur u, page 719

$f^{(n)}$ La n-ième dérivée de la fonction f, page 799

$o(x)$ fonction tendant rapidement vers zéro, page 801

(p) idéal engendré par p, page 179

$\mathbb{F}_p$ lorsque p est premier, page 289

$\mathbb{F}_{p^n}$ corps fini à p^n éléments, page 1308

$\mathrm{Frac}(\mathbb{A})$ Le corps des fractions de l'anneau $\mathbb{A}$, page 118

$\mathrm{Fun}(X, Y)$ les applications de X vers Y, page 112

$\mathrm{S}(E)$ Les opérateurs autoadjoints de E, page 472

U_n Le groupe des racines n^{e}de l'unité., page 1291

$\mathrm{res}(P, Q)$ résultat des polynômes P et Q, page 464

$\sqrt{A}$ racine d'une matrice hermitienne positive, page 835

$\theta_\alpha(P)$ la multiplicité de α par rapport à P, page 211

$A[X]$ tous les polynômes de degré fini à coefficients dans A, page 207

$A_n[X]$ les polynômes à coefficients dans A et de degré inférieur à n, page 208

$C(P)$ matrice compagnon, page 528

$D \mid P$ D divise P, page 209

$E_\lambda(u)$ Espace propre de u, page 483

Ensembles de matrices

Géométrie

Chaînes de Markov

Probabilités et statistique

Théorie des groupes

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 LaTeX (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 20.6.

(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 $\mathscr{D}(\Omega)$.

(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'analyse. http://linuxfr.org/nodes/110155/comments/1675813

(11) Bertrand Desmons pour plusieurs patchs 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`.

(15) cdrcprds pour une réponse à une question d'algèbre, démonstration à l'appui à propos de pgcd.

(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 26.60 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 13.297 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) Provatiscus 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

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 11.3 (bien qu'ils ne le savent pas).

(6) Xavier Mauquoy pour l'énoncé et la preuve du théorème 3.36.

(7) David Revoy pour les dessins de Pepper&Carrot de la couverture.

J'ai souvent donné entre parenthèse 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 hypertexte vers des sites, des blogs, etc. Tous ces gens ont fait du bon boulot. Sans toute cette « communauté », l'internet serait mort [1].

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 éloquente 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 le 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 [2], 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 inclue en la section 0.6. Voir 0.3 pour plus de détails.

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 Certaine notes en bas de page sont écrite dans une fonte spéciale [3].

1. 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.
2. Par exemple pour les théorèmes pour lesquels je n'ai pas lu ni a fortiori écrit de preuves.
3. Les notes comme celle-ci signifient qu'il y a quelque chose dont je ne suis pas sûr.

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 :

Problèmes et choses à faire

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 usuelle 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 8.1.13 ; dans tous les autres cas, la définition prise ici est celle qu'il vous faut.

(2) Un compact est un 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 $\ln : \mathbb{C}^* \to \mathbb{C}$ 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 discutable. 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 27.66.

(4) Le mot « corps » n'implique pas la commutativité, et nous n'utilisons pas la terminologie « anneau à division ». Voir la remarque 1.62 et la discussion 6.1.

0.5 Sage est là pour vous aider

Il existe de nombreux logiciels de mathématique. Notre préféré est Sage pour une raison très précise : en tant que langage de programmation, Sage est python qui est un langage généraliste. La syntaxe et la structure de Sage ne sont pas *ad hoc* pour faire de math, 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.

0.5.1 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 [4], et nous vous conseillons particulièrement le livre [2].

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

4. http://www.sagemath.org

0.5.2 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 besoin [5]. Voici une liste (non exhaustive) de ce que Sage peut faire pour vous.

(1) Calculer des limites de fonctions, exemples 44.1 et 44.2.

(2) Tracer des graphes de fonctions, exemple 44.2.

(3) Tracer des courbes en trois dimensions, voir exemple 13.144. 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 44.3.

(5) Résoudre des systèmes d'équations linéaires. Voir les exemples 44.4 et 44.5. Lire aussi la documentation.

(6) Tout savoir d'une forme quadratique, voir exemple 44.6.

(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 extrema de la fonctions (sous réserve d'être capable de résoudre certaines équations), voir les exemples 44.7 et 44.8.

(8) Indiquer une infinité de solutions à une équation en utilisant des paramètres. L'exemple 44.9 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 44.10.

(10) Calculer des approximations numériques comme dans l'exemple 44.11.

(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 20.65.

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 0.1.
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 16.109 pour le logarithme de nombres négatifs. Et aussi ceci :

```
1
2  SageMath version 7.3, Release Date: 2016-08-04
3  Type "notebook()" for the browser-based notebook interface.
4  Type "help()" for help.
5
6 sage: limit(1/x,x=0)
7 Infinity
8 sage: limit(1/x**2,x=0)
9 +Infinity
```

tex/sage/sageSnip017.sage

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

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

$$\lim_{x\to 0} \frac{1}{x} = \infty \tag{0.1}$$

ainsi que

$$\lim_{x\to 0} \frac{1}{x^2} = +\infty. \tag{0.2}$$

Voir aussi la compactification en un point d'Alexandroff 7.61.

0.6 Comment contribuer et aider ?

Ces notes ne sont pas relues de façon systématique. Aucune garantie. Merci de me signaler toute faute ou remarque : le relecteur c'est toi. Voici une petite liste de questions que je me pose ou de choses écrites dont je ne suis pas certain. Si vous avez un avis ou une réponse à un des points, merci de vous faire connaitre.

Les questions ouvertes sont divisées en trois niveaux de difficulté :

(1) Niveau facile : un étudiant de licence devrait pouvoir le faire.

(2) Niveau moyen : un candidat à l'agrégation de mathématique devrait pouvoir le faire.

(3) Demande probablement de connaissances avancées en mathématique ; au moins être tout à fait à l'aise avec le niveau d'agrégation.

Quel que soit votre niveau, vous pouvez faire ceci :

(1) M'écrire pour me signaler toutes les fautes que vous voyez, même si vous n'êtes pas sûr.

(2) Si vous n'êtes pas expert, me signaler tous le endroits qui vous semblent obscurs. Vu que ces notes sont destinées à *apprendre*, les avis des non experts sont très importants.

(3) Mettre une copie de (ou un lien vers) ces notes sur votre site.

0.6.1 Des preuves qui manquent

Vous trouverez un peu partout des énoncés sans preuves. Certaines sont surement 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.

0.6.2 Mes questions de géométrie

0.6.2.1 Facile

(1) Donner une interprétation en termes de plans, droites ou je ne sais quoi de géométrique au 4-cycle parmi les permutations des sommets du tétraèdre. D'où sort géométriquement la matrice (19.29) ?

0.6.2.2 Moyen

(1) Démontrer la proposition 10.3 qui donne les relations de Chasles pour un espace affine.

(2) En géométrie projective, dans la sphère de Riemann $\hat{\mathbb{C}} = P_1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$ est-ce qu'il existe une notion de cercle dont le centre est ∞ ? Voir le point 24.65.

(3) Géométrie projective. Tout le monde semble définir le birapport en identifiant $P(\mathbb{K}^2)$ à $\hat{\mathbb{K}} = \mathbb{K} \cup \{\infty\}$. Bien entendu, personne ne semble s'être attribué la mission d'expliciter la dépendance du birapport en le choix de l'identification. Je le fais à la définition 24.40.

Mais cette définition dépend du choix d'identification $\varphi\colon P(\mathbb{K}^2) \to \hat{\mathbb{K}}$, comme le montre l'exemple 24.42. J'ai donc défini des classes d'identifications possibles $A(\varphi)$ en 24.38. Et je démontre la proposition 24.43 que si $\varphi_a \in A(\varphi)$ alors les birapports construits à partir de φ et φ_a sont identiques.

Question : pourquoi personne ne semble faire ce travail ? En quoi l'identification φ_0 que tout le monde utilise est plus canonique qu'une autre ? Est-ce que l'on peut décrire simplement les classes $A(\varphi)$? Le groupe qui conserve le birapport associé à φ est-il isomorphe au groupe qui conserve le birapport associé à φ' ? Quels que soient φ et φ' ?

Suis-je la seule personne au monde à m'être demandé si le birapport était un objet canonique ?

(4) En géométrie projective, dans $P_1(\mathbb{C}) = \hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$, si ℓ est une droite dans $\mathbb{C}$, est-ce que la droite correspondante dans $\hat{\mathbb{C}}$ contient le point ∞ ? Moi j'ai envie de dire que ∞ est sur toutes les droites. Voir le problème 24 et la remarque 24.63.

(5) Géométrie affine, barycentre. Les mauvaise langues diraient que tout cela est du snobisme autour de la paresse d'écrire $\overrightarrow{xy}$ au lieu de $y - x$. Est-ce qu'il y a des cas où toute l'étude des espaces affines et des barycentres en particulier apportent *réellement* plus qu'une facilité d'écriture par rapport à travailler dans le cadre vectoriel pur ?

0.6.3 Mes questions d'algèbre

0.6.3.1 Facile

0.6.3.2 Moyen

(1) Pour donner un peu de consistance à l'exemple 3.135, il faudrait décrire les éléments irréductibles de $\mathbb{Z}[i\sqrt{2}]$.

0.6.3.3 Difficile

(1) Que penser de 6.78 qui dit que l'extension de corps $\mathbb{K}(\alpha)$ dépend en réalité du corps ambiant dans lequel on calcule l'extension ?

Est-ce qu'il existe des exemples moins triviaux et plus utiles que celui que je donne ?

(2) Pour quelle classe d'anneaux et de polynômes le quotient $A[X]/(P)$ est-il un corps ?

0.6.3.4 Non classées

(1) Est-ce qu'il existe une structure raisonnable d'espace vectoriel sur $\mathbb{Z}$? Est-ce qu'il existe des corps discrets infinis ?

Dans cette question, j'ai derrière la tête que dans un espace vectoriel topologique nous avons une notion de suite de Cauchy, définition 9.19. Donc dans ce cas la notion d'espace complet est une notion topologique. Or il y a l'exemple 9.25 qui donne deux distances sur $\mathbb{N}$, qui donnent la même topologique, mais l'un étant complet, l'autre non.

Si il y avait une structure vectorielle sur $\mathbb{N}$, cela créerait une contradiction. Au moins au sens où la définition 9.19 de suite de Cauchy « topologique » ne redonne pas la même que la notion « métrique » de la définition usuelle 9.21.

(2) La « décomposition en facteurs premiers » dans $\mathbb{Z}[i\sqrt{2}]$ que je donne dans l'exemple 3.135 est-elle correcte ? En particulier le lemme 3.136 ?

(3) Est-ce que la fin de la démonstration 20.25 avec cette histoire d'ensemble $\{\xi_k^q$ tel que $q \in \mathbb{N}\}$ fini est compréhensible ?

(4) Les représentations *irréductibles* sont les modules *indécomposables*. Quid des modules irréductibles ? C'est pas un peu dingue de ne pas utiliser le mot « irréductible » pour désigner les mêmes choses dans le cas des modules et celui des représentations ?

(5) Rendre rigoureuse la remarque (11.239) qui dit que les matrices dont le polynôme minimal est égal au polynôme caractéristique sont denses dans les matrices.

(6) La partie initiation de récurrence ($r = 2$) de la preuve de la proposition 10.36 à propos de convexe et de barycentre est-elle correcte ? Ce passage de l'espace affine à l'espace vectoriel sous-jacent me paraît un peu facile.

(7) Est-ce que l'énoncé et la démonstration de la proposition 6.96 sont corrects ? Si a et b sont des racines de P, alors $\mu_a\mu_b$ divise P (si $\mu_a \neq \mu_b$). Cette proposition est utilisée dans la démonstration de l'irréductibilité des polynômes cyclotomiques (proposition 20.23).

(8) À quoi sert l'hypothèse « autre que $\mathbb{F}_2$ » dans le lemme 20.75 ? Peut-être dans la notion de déterminant parce qu'en caractéristique 2, l'antisymétrie d'une forme linéaire n'implique le fait qu'elle soit alternée.

(9) L'inversibilité de la somme de Gauss (proposition 20.41) est-elle bien démontrée ?

(10) Des commentaires sur l'exemple 6.130 qui montre que $X^p - X + 1$ est irréductible sur $\mathbb{F}_p$.

(11) Les idéaux de A/I sont en bijection avec les idéaux de A contenant I. Justification de l'équation (3.87).

(12) À propos d'extensions algébriques, est-ce que la proposition 6.85 est correcte ? Est-ce qu'implicitement, il n'y a pas un sur-corps de $\mathbb{K}$ dans lequel il faut travailler ?

(13) À propos de construction à la règle et au compas. Pour l'addition d'angles, l'exemple 20.82 explique comment on construit la somme de deux angles. Le problème est que cette construction se fait par intersection de deux cercles. Une des deux intersections donne $\alpha+\beta$ et l'autre donne $\alpha-\beta$. Comment par construction peut-on choisir le bon point ?

(14) À propos de chiffrement RSA, quelle est la probabilité que le message M ne soit pas premier avec p ? Est-ce que Alice (qui est celle qui chiffre avec la clef de Bob) peut le vérifier ? Que penser des points que j'énumère à la page 1297 au dessus du problème 23 ?

(15) Isomorphisme du corps $\mathbb{R}$. Que penser de la remarque 6.5 ?

0.6.4 Mes questions d'analyse

0.6.4.1 Facile

0.6.4.2 Moyen

(1) Est-ce que l'énoncé du théorème de Müntz 18.7 est correct ? Voir en particulier la remarque 18.8 à propos de la présence du monôme 1 dans la liste.

(2) À propos de formule sommatoire de Poisson, est-ce que l'exemple 30.12 est bien fait ? En particulier la formule (30.44) est-elle correcte et bien justifiée ?

(3) Que penser de la remarque 26.38 qui dit qu'on doit avoir un théorème de complétion de partie orthonormale en une base orthonormale pour un espace de Hilbert ? C'est vrai ?

(4) Préciser l'énoncé et donner une démonstration de la proposition 12.107 qui traite de sommes dénombrables.

(5) Explosion en temps fini. C'est le corollaire 33.18. Dans le cas où $\lim_{t\to t_{max}} \|y(t)\| = \infty$ alors la dérivée de y n'est pas non plus bornée. Correct ?

(6) Est-ce qu'il y a moyen de définir la mesure produit (de deux espaces mesurés) sans passer par l'intégrale ?

Le théorème-définition 15.207 donne le produit de mesures par la formule

$$(\mu_1 \otimes \mu_2)(A) = \int_{\Omega_1} \mu_2\big(A_2(x)\big)d\mu_1(x) = \int_{\Omega_2} \mu_1\big(A_1(y)\big)d\mu_2(y). \tag{0.3}$$

On peut faire plus abstrait ?

Sans une telle définition, l'ordre imposé est :

— mesure

— intégrale

— mesure produit.

En particulier, quand on voit l'intégrale, la mesure de Lebesgue sur $\mathbb{R}^n$ n'est pas encore définissable.

Il serait bien de pouvoir faire :

— mesure

— mesure de Lebesgue sur $\mathbb{R}$

— mesure produit

— mesure de Lebesgue sur $\mathbb{R}^n$

— intégrale.

(7) La proposition 13.340 prouve que la fonction $x \mapsto a^x$ $(a > 0)$ est dérivable. Pour ce faire, le concept de primitive est utilisé (pas jusqu'aux intégrales, cependant). Ça me semble incroyable qu'il faille ça pour prouver une dérivabilité.

Prouver que la limite

$$\lim_{\epsilon \to 0} \frac{a^\epsilon - 1}{\epsilon} \tag{0.4}$$

existe et n'est pas infinie sans recourir aux intégrales, aux primitives.

0.6.4.3 Difficile

(1) Soit $n \in \mathbb{N}$, $A \in \mathbb{R}$ et $x_0 \in \mathbb{Q}$. Nous considérons la suite[3]

$$x_{k+1} = \frac{1}{n}\left((n+1)x_k + \frac{A}{x_k^{n-1}}\right). \tag{0.5}$$

Prouver que :

— C'est une suite de Cauchy

— $x_k^n \to A$.

Il me faudrait une démonstration de cela sans passer par la méthode de Newton. Par exemple via le binôme de Newton.

Mon but serait de définir $a^{1/n}$ pour tout $n \in \mathbb{N}$ sans passer par de l'analyse (ou en tout cas pas en passant par le concept de fonction continue). Pour l'instant, c'est la définition 13.311 qui définit $a^{1/n}$. Cela se base sur un argument de fonction continue strictement croissante pour obtenir une bijection.

(2) Est-ce que la proposition 9.26 qui donne le critère $d(x_p, x_q) \leqslant \epsilon$ pour être une suite de Cauchy est valide dans un espace topologique métrique au lieu de normé ? Dans quels cas a-t-on

$$d(a, b) = d(a + u) + d(b + u) \tag{0.6}$$

lorsque d est une distance qui n'est pas spécialement induite d'une norme ?

(3) Soit V, un espace vectoriel normé. Soit $v \in V$. Est-ce qu'il existe un élément $\varphi \in V'$ (application linéaire continue) telle que $\varphi(v) = 1$ et $\|\varphi\| = 1$?

(4) Que penser de 15.154 qui tente d'expliquer pourquoi on ne définit pas l'intégrale d'une fonction non mesurable, malgré que le supremum qui la définirait existe forcément ?

(5) Changement de variables. À quel point la proposition 15.254 est-elle équivalente au théorème usuel ?

0.6.4.4 Non classées

0.6.5 Mes questions de probabilité et statistiques.

0.6.5.1 Facile

0.6.5.2 Moyen

(1) Soit une variable aléatoire X à valeurs réelles. Est-ce que la tribu engendrée par X est d'une façon ou d'une autre engendrée par les « courbes de niveau » de X ? C'est-à-dire par les $X^{-1}(\{t\})$ pour les $t \in \mathbb{R}$.

C'est ce qui semble ressortir de l'exemple de 37.2.10. Et intuitivement, je trouve que ça irait bien ...

0.6.5.3 Difficile

0.6.5.4 Non classées

0.6.6 Mes questions de LaTeX et programmation

0.6.6.1 Facile

(1) Comment faire en sorte que les mots commençant par « é » soient avec les « e » dans l'index, et non avant les « a » ?

0.6.6.2 Moyen

(1) Comment mettre $A[X]$ dans le titre d'un `enumerate` ?

Mon environnement `subproof` est un enumerate, et je voudrais parler de temps en temps de $A[X]$ dans ses titres, mais LaTeX plante à cause du crochet fermant. Voir la démonstration du lemme 3.133. Pour obtenir l'effet, j'ai créé un `newcommand` de `\foo` qui fait $A[X]$.

Il y a aussi ce problème pour le titre de l'exemple 3.135.

(2) Revoir le mécaniste de l'index thématique. Il faudrait pouvoir les trier avec des titres. Mais attention : il doit arriver avant la table des matières.

(3) L'environnement `example` est un sale hack pour placer le triangle. Faire mieux. Recopier l'environnement théorème pour lui changer son carré en triangle ?

0.6.6.3 Difficile

Je ne sais pas comment faire, et à mon avis il faudra innover.

(1) 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`.

(2) 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`.

0.6.7 Numérique

0.6.7.1 Moyen

(1) L'erreur de cancellation provoquée par la différence $a - \tilde{a}$ lorsque a et $\tilde{a}$ n'a pas de conséquences sur l'ordre de grandeur de la réponse. Seulement des conséquences sur la valeur des chiffres significatifs. Vrai ou faux ?

Voir la remarque 35.20.

0.7 Comment contribuer et aider (math) ?

0.7.0.1 Questions d'analyse

(1) À propos de suites de Cauchy dans un espace vectoriel topologique et dans un espace métrique, est-ce que le théorème 9.36 est correct ?

Soit V un espace vectoriel topologique métrisable [6], alors il admet une métrique d compatible avec la topologie telle que une suite dans V est d-Cauchy si et seulement si elle est τ-Cauchy.

Dans cet ordre d'idée, il faut des exemples de :

— un espace vectoriel topologique métrisable et une métrique d compatible avec la topologie, mais dont les suites d-Cauchy ne sont pas celles τ-Cauchy. Et en particulier dont la complétude est différente que celle de la « bonne » métrique donnée par la théorème 9.33.

— Et aussi un exemple pour la remarque 9.37.

(2) L'exemple 18.23 parle d'inverser une intégrale et une dérivée au sens des distributions pour prouver que la dérivée de $\int_0^x g(t)dt$ par rapport à x est g. Rendre cela rigoureux.

(3) À propos du théorème de récurrence de Poincaré 15.83, l'application ϕ doit être mesurable ? Répondre à la question posée sur la page de discussion de l'article sur wikipédia.

Toujours à propos du théorème de récurrence de Poincaré, il me semble qu'il y a un énoncé qui insiste sur la compacité de l'espace des phases et une démonstration utilisant la propriété de sous-recouvrement fini. Je serais content de retrouver cela. (ce serait sans doute mettable dans la leçon sur l'utilisation de la compacité)

(4) Dans [4], on parle de la proposition 31.42 à sa page 10. Comment est-ce qu'on justifie le passage

$$\int_{\mathbb{R}^d} T\big(y \mapsto \varphi(x)\psi(x-y)\big)dx = T\Big(y \mapsto \int_{\mathbb{R}^d} \varphi(x)\psi(x-y)dx\Big). \tag{0.7}$$

Sylvie Benzoni précise que « ceci demanderai quelques justifications ». Où trouver lesdites justifications ? Il s'agit de permuter une distribution et une intégrale.

(5) Peut-on permuter une application linéaire et continue avec une somme pas spécialement dénombrable ? En supposant que $\sum_{i\in I} f(v_i)$ existe, la proposition 12.108 semble dire que oui. Est-ce correct ?

Peut-on avoir un exemple de partie sommable $\{v_i\}_{i\in I}$ et d'application linéaire continue f telle que la partie $\{f(v_i)\}$ ne soit pas sommable ?

Peut-être ceci dans un espace de Hilbert. $v_i = \frac{1}{i^2}e_i$ puis $f(e_i) = i^3 e_i$.

(6) Soit une partie orthonormale *pas spécialement dénombrable* $\{u_i\}_{i\in I}$ d'un espace de Hilbert (pas spécialement séparable). Si

$$x = \sum_{i\in I} x_i u_i, \tag{0.8}$$

6. i.e. admet une base dénombrable de topologique, voir la proposition 9.34

puis-je prendre le produit scalaire avec u_k et le permuter avec la somme pour déduire que $x_k = \langle x, u_k \rangle$?

C'est ce que je fais dans la proposition 26.25.

(7) Théorème de point fixe et équation différentielle. Que penser de l'exemple 18.45 qui itère la contraction de Cauchy-Lipschitz pour résoudre $y'(t) = y(t)$, $y(0) = 1$? Est-ce que c'est générique comme comportement ? Est-ce que la convergence est efficace dans des cas moins triviaux ?

0.7.1 Question de numérique

(1) Différences finies. Il faut une analyse de consistance, stabilité et convergence du schéma à 9 points pour le laplacien donné par (36.146). Je crois qu'il est d'ordre 6, mais je n'en suis vraiment pas sûr.

0.8 Taper du code pour le Frido

Dans cette section nous donnons quelques indications sur la façon de taper du code LaTeX pour le Frido.

Tout commence par télécharger les sources à l'adresse

https://github.com/LaurentClaessens/mazhe

0.8.1 Pour compiler le document vous même

Lisez le fichier `COMPILATION.md`.

0.8.2 Nommage des fichiers `tex`

J'ai pris l'habitude de préfixer les noms par un nombre. Par exemple `139_EspacesVecto`. Le fait est qu'il est plus simple, pour ouvrir le ficher, de taper `139<TAB>` que de se souvenir si « EspacesVecto » est écrit avec une majuscule, en français, en anglais, ...

De plus un chapitre contenant plusieurs fichiers, nous nous retrouvons rapidement avec beaucoup de fichiers nommés `EspacesVecto1`, `EspacesVecto2`, etc.

Vous trouverez le prochain numéro disponible dans `réserve.tex`.

0.8.3 Inclure des exemples de code

Pour inclure du code Sage, nous utilisons la commande `\lstinputlisting`. Ici encore, le fichier `réserve.tex` contient le prochain disponible.

0.8.4 Pour les exercices

ATTENTION : dans un futur proche, je vais supprimer tous les exercices et les mettre sous forme d'exemples. Une des raisons est de supprimer la dépendance en le paquet personnel `exocorr` qui rend compliqué la compilation du Frido par des tierces personnes.

Les exercices sont tapés dans les fichiers déjà pré-remplis `src_exocorr/exo*.tex`. Les corrections sont dans le fichier `src_exocorr/corr*.tex` correspondant. Ces fichiers ne sont pas inclus directement, mais via la macro `\Exo`.

Le fichier `réserve.tex` contient le prochain disponible.

Exemple Vous voulez créer un exercice.

— Allez voir dans `réserve.tex` la prochaine ligne `Exo` disponible.

— Mettons que ce soit `\Exo{mazhe-0018}`

— Supprimez cette ligne de `réserve.tex`, et mettez la où vous voulez voir paraitre votre exercice.

— Tapez votre exercice dans le fichier `src_exocorr/exomazhe-0018.tex` et votre correction dans le fichier `src_exocorr/corrmazhe-0018.tex`. Ces fichiers sont déjà créés et pré-remplis. Ne changez pas le code qui y est.

0.9 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.

0.9.1 Licence libre

Je crois que c'est clair.

0.9.2 pdflatex

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

0.9.3 utf8

Je crois que c'est clair.

0.9.4 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.

0.9.5 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.

0.9.6 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, blablabla ». 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).

0.9.7 Des listes de liens internes

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

0.9.8 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.

En faisant

```
pytex lst_frido.py --verif
```

vous aurez une liste des références vers le bas. Cette liste doit être vide ! Ce programme cherche tous les `\ref` et `\eqref` ainsi que les `\label` correspondants et vous prévient lorsque le `\label` est après le `\ref`.

Si vous pensez qu'une référence pointée doit être acceptée (par exemple parce c'est dans une des listes de liens internes), alors vous ajoutez son hash dans la liste du fichier `commons.py`. Si il s'agit vraiment d'une référence vers un résultat que vous utilisez, alors vous devez déplacer des choses. Soit votre résultat vers le bas, soit celui que vous utilisez vers le haut. Parfois cela demande de déplacer ou redécouper des chapitres entiers... Si il n'y a vraiment pas moyen, bravo, vous venez de prouver que la mathématique est logiquement inconsistante.

0.9.9 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 $\mathbb{Z} \times \mathbb{Z}\backslash 0$; 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 ».

0.10 Vérifier si vous n'avez pas fait de bêtises

Lorsqu'on fait de lourdes modifications (déplacement de parties, fusion de théorèmes, etc) il est toujours possible de faire des bêtises d'au moins deux types : créer des références vers le futur et supprimer des parties (genre couper-coller en oubliant le coller). Pour s'en prémunir, le script suivant lance quelques compilations et vérifications :

```
./testing.sh
```

Aucune erreur ne devrait être signalée.

Attention : ce script fait quelques manipulations à base de `git stash` et crée une nouvelle branche (nom aléatoire assez long) pour tester votre dernière modification sans créer de commit.

0.11 Acceptation des contribution

TD ;DR : pratiquement aucun patch n'est refusé.

Le premier critère d'acceptation d'une contribution est évidemment la correction mathématique.

0.11.1 Attention aux expressions rationnelles

Si vous trouvez une faute d'orthographe, rien ne vous empêche de faire une recherche de la même faute pour la corriger d'un seul coup dans 25 fichiers. Faites toutefois attention à des remplacements automatiques sur base d'expressions rationnelles telles que

```
des [a-z]*[^s]
```

qui serait supposé détecter des erreurs de pluriel. Je vous laisse trouver au moins 5 cas sans fautes qui satisfont cette expression.

Utilisez de telles expressions pour *trouver* des fautes, pas pour les corriger.

0.11.2 Pas de modifications massives, automatiques pour des raisons cosmétiques

Il est un type de contributions que je ne vais plus accepter, ce sont les modifications massives et automatiques de *tous* les fichiers pour des raisons de « propreté » du code. Exemples :

— Supprimer automatiquement tous les espaces en bout de lignes,

— Supprimer automatiquement toutes les lignes vides en fin de fichier

— Remplacer `\ref` par `~\ref`

— Remplacer `\[` par `\begin{equation}`

— Remplacer `\og` par « (avec ou sans espaces devant ou derrière)

— ...

Ce type de substitutions automatiques créent des patch gigantesques qui prennent un temps astronomique à relire pour un bénéfice pas tellement évident.

Pire : ils ont des effets de bords pas toujours évident à détecter ou à prévoir.

N'oubliez pas que le Frido n'est pas que du LaTeX. Il est aussi divers script de pré et post-compilation (y compris qui hackent des fichiers intermédiaires entre deux passes de LaTeX). Ces scipts, écrits par votre très humble et très obéissant serviteur, ne sont pas parfaits et les parseurs reposent sur certaines hypothèses. Donc des choses qui ne devraient ne rien changer du point de vue de LaTeX peuvent avoir des conséquences.

Bien entendu, si vous êtes en train de taper des math et que ce genre de « malpropreté » du code vous gêne, vous pouvez corriger dans les fichiers que vous modifiez.

Chapitre 1

Construction des ensembles de nombres

1.1 Quelques éléments sur les ensembles

1.1.1 Petit mot d'introduction

1.1.
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.

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.

Une petite définition cependant, que l'on utilisera :

Définition 1.2.
Deux ensembles A et B sont ***disjoints*** *si leur intersection est vide*[1] *; en d'autres termes, s'il n'existe aucun élément commun à A et B.*

1.3.
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. Remarquez que les mots « intersection » et « vide » sont de ceux que nous avons décidé de ne pas définir.

1.4.
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 Ensemble ordonné

Définition 1.5.
Soient deux ensembles E et F. Une application $f : E \to F$ 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) ***bijective*** *si elle est à la fois injective et surjective.*

La méthode la plus courante pour démontrer qu'une application $f : E \to F$ 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 $1/(x - y)$.

1.6.
L'**axiome du choix** que nous acceptons peut s'énoncer comme ceci[5] : 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 1.7.
Une ***relation d'ordre*** *sur un ensemble E est une relation binaire (notée $\leqslant$) sur E telle que pour tous $x, y, z \in E$,*

réflexivité *: $x \leqslant x$*

antisymétrie *: $x \leqslant y$ et $y \leqslant x$ implique $x = y$*

transitivité *: $x \leqslant y$ et $y \leqslant z$ implique $x \leqslant z$.*

Définition 1.8.
Un ensemble ordonné est ***totalement ordonné*** *si deux éléments sont toujours comparables : si $x, y \in E$ alors nous avons soit $x \leqslant y$ soit $y \leqslant x$. Si les éléments ne sont pas tous comparables, nous disons que l'ordre est* ***partiel****.*

Définition 1.9.
Soit un ensemble ordonné $(E, \leqslant)$ 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 $m \leqslant x$.*

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

Les notions de ***maximum*** *et de* ***majorant*** *sont définis 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 1.10.
Un ensemble ordonné est ***bien ordonné*** *si toute partie non vide possède un plus petit élément : si A est une partie de E, alors $\exists x \in A, \forall y \in A, x \leqslant y$.*

1.11.
Quelques remarques.

(1) L'inégalité stricte (définie par : $x < y$ si et seulement si $x \leqslant y$ et $x \neq y$) n'est pas une relation d'ordre parce qu'elle n'est pas réflexive.

(2) Nous verrons dans la remarque 1.110 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 : $x \leqslant y$ ou $y \leqslant x$.

Exemple 1.12
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 $Y \subset X$. △

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

Définition 1.13.
*Soit un ensemble totalement ordonné $(E, \leqslant)$. 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*

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

1.1.3 Lemme de Zorn

Définition 1.14 (Ensemble inductif[6])**.**
*Un ensemble est **inductif** si tout sous-ensemble totalement ordonné admet un majorant.*

Lemme 1.15 (Lemme de Zorn)**.**
Tout ensemble ordonné inductif non vide admet un maximum.

Le point intéressant de ce lemme est que le majorant soit un maximum, c'est-à-dire qu'il appartienne à l'ensemble.

Définition 1.16.
*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).*

Lemme 1.17 ([1] [2])**.**
Soit un ensemble E. Si I et J sont deux parties de E telles que $I \cup J$ soit infini. Alors soit I soit J (soit le deux) est infini.

La proposition suivante sera utilisée en théorie de la mesure, dans l'exemple 15.61. Ça utilise l'axiome du choix sous la forme du lemme de Zorn.

Proposition 1.18 ([7, 8])**.**
Si S est un ensemble infini alors il existe une bijection $\varphi\colon \{1, 2\} \times S \to S$.

1.1.4 Complémentaire

Définition 1.19.
*Soit E, un ensemble et A, une partie de E (c'est-à-dire un sous-ensemble de E). Le **complémentaire** de l'ensemble A, dans E, noté $\complement A$ est l'ensemble des éléments de E qui ne font pas partie de A :*

$$\complement A = E \backslash A = \{x \in E \text{ tel que } x \notin A\}. \tag{1.1}$$

Nous allons aussi régulièrement noter le complémentaire de A par A^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, $E \backslash (E \backslash A) = A$,

2. Écrivez moi si vous connaissez une preuve de ceci.

(2) $\complement(A \cap B) = \complement A \cup \complement B$,

(3) $\complement(A \cup B) = \complement A \cap \complement B$,

(4) $A \backslash B = A \cap \complement B$.

Définition 1.21 (différence symétrique)**.**
Si A et B sont des ensembles, l'ensemble $A\Delta B$ est la ***différence symétrique*** *d'ensembles :*

$$A\Delta B = (A \cup B)\backslash(A \cap B). \tag{1.2}$$

C'est l'ensemble des éléments étant soit dans A soit dans B mais pas dans les deux.

Lemme 1.22.
Si A et B sont des ensembles nous avons

(1) $A^c \Delta B^c = A\Delta B$.

(2) $(A\Delta B)\Delta B = A$.

Démonstration. D'abord nous avons l'égalité $X^c \backslash Y^c = Y \backslash X$. Cela se prouve de façon classique en séparant deux cas selon que B soit inclus dans A ou non.

De là nous avons la première assertion :

$$A^c \Delta B^c = (A^c \cup B^c)\backslash(A^c \cap B^c) = (A \cap B)^c \backslash (A \cup B)^c = (A \cup B)\backslash(A \cap B) = A\Delta B. \tag{1.3}$$

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

$$(A\Delta B)\Delta B = (A \cup B)\backslash(B \backslash A) = A. \tag{1.4}$$

□

1.1.5 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 $x \sim z$.*

Exemple 1.24
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 1.25
Soit f une application entre deux ensembles E et F. Nous définissons une relation d'équivalence sur E par

$$x \sim y \Leftrightarrow f(x) = f(y). \tag{1.5}$$

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

$$\begin{aligned} g\colon E/\sim &\to F \\ [x] &\mapsto f(x) \end{aligned} \tag{1.6}$$

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

$$f = g \circ \pi. \tag{1.7}$$

△

1.2 Les naturels

Toutes les constructions sont faites dans [9]. Les résultats énoncés ici sont utilisés plus bas et servent de guide à un éventuel contributeur qui voudrait écrire une partie sur la construction de $\mathbb{N}$ et $\mathbb{Z}$. Nous espérons que des preuves se trouvent dans [9]. En tout cas, le lecteur est invité à ne pas les prendre pour évidents.

1.2.1 La construction

Cette section est vide, insuffisamment détaillée ou incomplète. Votre aide est la bienvenue ! Comment faire ?

1.2.2 Quelques résultats de cardinalité

Je vous conseille fortement de ne pas considérer ces résultats comme évidents avant d'avoir lu quelque articles de Wikipédia sur la construction des naturels en théorie des ensembles.

Proposition 1.26.
L'ensemble $\mathbb{N}$ est infini[3].

Cette proposition est à peu près prise comme définition d'un ensemble fini dans [10] qui donne également une preuve de l'équivalence avec notre définition. Rien de tout cela n'est évident [4]

Proposition-définition 1.27.
Si I est un ensemble fini, il existe un unique $N \in \mathbb{N}$ tel que I soit en bijection avec $\{0, \dots, N\}$.
*Dans ce cas, le nombre $N+1$ est le **cardinal** de I.*

Nous ne définissons pas ce qu'est le cardinal d'un ensemble infini ; c'est très compliqué et ça ne nous servira pas.

Définition 1.28.
*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 1.16, c'est qu'un ensemble fini n'est ni dénombrable ni non dénombrable [5].

Proposition 1.29 ([11])**.**
Si A est un ensemble dénombrable, alors pour tout $n \in \mathbb{N}$, l'ensemble A^n est dénombrable.

Proposition 1.30 ([11])**.**
Une union dénombrable d'ensembles dénombrables est dénombrable.

3. Définition 1.16.
4. Surtout que je n'ai pas défini la notation $\{0, \dots, N\}$.
5. 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[11].

Les ensembles dénombrables sont les plus petits ensembles infinis possibles, comme en témoigne la proposition suivante.

Proposition 1.31.
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 $\varphi\colon E_0 \to E_1$ une bijection.

Soit $x_0 \in E_0 \backslash E_1$ (axiome du choix et tout ça). Nous définissons

$$\begin{aligned} \psi\colon \mathbb{N} &\to \{\varphi^k(x_0)\} \\ n &\mapsto \varphi^n(x_0) \end{aligned} \tag{1.8}$$

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

$$x_0 = \varphi^{k-l}(x_0) = \varphi\big(\varphi^{k-l-1}(x_0)\big) \tag{1.9}$$

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 $E_0 \backslash E_1$. Donc en réalité $\varphi^k(x_0) \neq \varphi^l(x_0)$ dès que $k \neq l$. □

Proposition 1.32.
Toute partie d'un ensemble fini est finie, et toute partie d'un ensemble dénombrable est finie ou dénombrable.

1.3 Groupes

1.3.1 Définition, unicité du neutre

Définition 1.33 (Groupe)**.**
Un ***groupe*** *est un ensemble G muni d'une opération interne $\cdot : G \times G \to G$ 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.

Lemme-définition 1.34 (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 $g \in G$: $e_1 g = g e_1 = g$. En particulier pour $g = e_2$ nous écrivons $e_1 e_2 = e_2 e_1 = e_2$. Mais en partant dans l'autre sens : $e_2 g = g e_2 = g$ avec $g = e_1$ nous avons $e_2 e_1 = e_1 e_2 = e_1$. En égalant ces deux valeurs de $e_2 e_1$ 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 $k_1 = k_2$.

□

Définition 1.35.
*Un groupe G est **abélien** ou **commutatif** si pour tous g et h dans G, $gh = hg$.*

Lemme 1.36.
Si G est un groupe et si $h \in G$, alors les applications

$$\begin{aligned} L_h : G &\to G \\ g &\mapsto hg \end{aligned} \tag{1.10}$$

et

$$\begin{aligned} R_h : G &\to G \\ g &\mapsto gh \end{aligned} \tag{1.11}$$

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. □

1.4 Anneaux

Définition 1.37 (Anneau[12])**.**
*Un **anneau**[6] est un triplet $(A, +, \cdot)$ avec les conditions*

(1) $(A, +)$ est un groupe 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.

Définition 1.38 (Morphisme d'anneaux[13])**.**
*Soient des anneaux unitaires A et B. Une application $f : A \to B$ est un **morphisme d'anneaux** si pour tout $a, b \in A$ nous avons :*

(1) $f(a + b) = f(a) + f(b)$,

(2) $f(ab) = f(a)f(b)$,

(3) $f(1_A) = 1_B$.

Lemme 1.39.
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,

$$a \cdot 0 = a \cdot (1 - 1) = a - a = 0. \tag{1.12}$$

Notons que la dernière égalité s'écrit en détail $a-a = a+(-a)$ qui donne le neutre de l'addition. □

Proposition 1.40.
Dans un anneau 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, $a = 0$. □

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

Soit X un ensemble et un anneau $(A, +, \times)$. Nous considérons $\mathrm{Fun}(X, A)$ l'ensemble des applications $X \to A$. Cet ensemble devient un anneau avec les définitions

$$(f + g)(x) = f(x) + g(x) \tag{1.13a}$$
$$(fg)(x) = f(x)g(x). \tag{1.13b}$$

Cela est la **structure canonique** d'anneau sur $\mathrm{Fun}(X, A)$.

Définition 1.41.
*Le **centralisateur** de $x \in A$ dans A est l'ensemble*

$$\{y \in A \text{ tel que } xy = yx\}, \tag{1.14}$$

*le **centre** de A est*

$$\{y \in A \text{ tel que } xy = yx, \forall x \in A\}. \tag{1.15}$$

Définition 1.42 (Morphisme d'anneaux)**.**
*Si $(A, +, \cdot)$ et $(B, +, \cdot)$ sont des anneaux, un **morphisme** est une application $f : A \to B$ 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.

Définition 1.43.
*Un **isomorphisme d'anneaux** est un morphisme bijectif.*

Définition 1.44 (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.*

Définition 1.45.
*Nous disons que A est un **anneau commutatif** si pour tout $a, b \in A$ nous avons $a + b = b + a$.*

Définition 1.46.
*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 1.47.
Au sens de la définition 1.46, 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 $\mathbb{Z}$.

1.5 Les entiers

Lemme 1.48.
Toute partie bornée de $\mathbb{Z}$ possède un plus grand élément.

Proposition 1.49.
Soit $a, b \in \mathbb{Z}$ tels que a divise b. Alors $a \leqslant b$.

1.5.1 Quelques autres résultats

Nous supposons ici connaitre, et avoir démontré les rudiments du calcul dans $\mathbb{N}$ et $\mathbb{Z}$. En particulier les produits remarquables, et les implications comme $a > b$ implique qu'il n'existe pas de x dans $\mathbb{N}$ tel que $a + x = b$.

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 Madore[7]. Son utilité est de pouvoir créer un langage de programmation pouvant traiter des paires d'entiers rien qu'en traitant des entiers.

Proposition 1.50 (Une bijection $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$)**.**
La fonction

$$\begin{aligned} f\colon \mathbb{N} \times \mathbb{N} &\to \mathbb{N} \\ (x, y) &\mapsto \begin{cases} y^2 + x & si\ x < y \\ x^2 + x + y & si\ y \leqslant x. \end{cases} \end{aligned} \tag{1.16}$$

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 $y \leqslant x$,
(3) si $k = y^2 + x$ avec $x < y$ alors il est impossible que $k = x'^2 + y'$ avec $y \leqslant x$.

Supposons $k = y^2 + x$ avec $x < y$. Alors aucun y' de la forme $y + s$ ne peut être solution parce que

$$y^2 + x = k = (y + s)^2 + x' = y^2 + 2sy + s^2 + x', \tag{1.17}$$

ce qui impliquerait $x' = x - 2sy - s^2 < 0$. Il ne peut donc pas y avoir deux solutions.

Supposons de la même manière que $k = x^2 + x + y$. Alors il n'existe pas de solutions avec $x' = x + s$ parce que cela donnerait

$$(x + s)^2 + (x + s) + y' = x^2 + x + y, \tag{1.18}$$

et donc

$$y' = y - 2sx - s^2 - s < 0. \tag{1.19}$$

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

$$f(1, a), f(2, a), \dots, f(a - 1, a) \tag{1.20}$$

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).

7. 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.

1.5.2 Anneau intègre

Définition 1.51 (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 3.8.

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 1.52 (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 $A^* = A\backslash\{0\}$.

Conformément à la définition 1.51 de diviseur, nous posons la définition suivante pour les diviseurs de zéro.

Définition 1.53 ([14])**.**
*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 b tel que $ab = 0$.*

*Nous disons que a est un **diviseur de zéro** si il est un diviseur de zéro à gauche ou à droite.*

Proposition-définition 1.54 ([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 soi b est nul.

(2) implique (3) Si $ab = ac$, alors $a(b - c) = 0$ et l'hypothèse dit que doit $a = 0$, 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.

□

1.5.3 Somme à valeurs dans un anneau

Définition 1.55.
Si $f\colon \{0, \dots, N\} \to A$ est une application vers un anneau A, alors nous définissons la notation $\sum_{i=0}^{N} f(i)$ par récurrence de la façon suivante :

(1) $\sum_{i=0}^{0} f(i) = f(0)$,

(2) $\sum_{i=0}^{k} f(i) = \sum_{i=0}^{k-1} f(i) + f(k)$.

Proposition-définition 1.56 ([1]).
Soient un ensemble fini S, un anneau commutatif A, et une fonction $f\colon S \to A$.

(1) Il existe un unique $N \in \mathbb{N}$ tel qu'il existe une bijection $\varphi\colon \{0,\dots,N\} \to S$.

(2) Si il existe deux bijections $\varphi_1\colon \{0,\cdots N\} \to S$ et $\varphi_2\colon \{0,\dots,N\} \to S$, alors

$$\sum_{i=0}^{N} f\big(\varphi_1(i)\big) = \sum_{i=0}^{N} f\big(\varphi_2(i)\big). \tag{1.21}$$

Ce nombre est noté

$$\sum_{s\in S} f(s). \tag{1.22}$$

La définition 1.56 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 12.99.

(3) L'existence d'une bijection entre I et $\{0,\dots,N\}$ ainsi que l'unicité du N pour lequel c'est possible sont donnés par la proposition 1.27.

Si nous avons une application $L\colon S \to S$, nous notons

$$\sum_{s\in S} f\big(L(s)\big) = \sum_{s\in S} (f\circ L)(s). \tag{1.23}$$

Cette façon d'écrire donne une interprétation pour la notation $\sum_{g\in G} f(hg)$ qui arrive dans la proposition 1.57. Il s'agit de considérer l'application L_h du lemme 1.36, de considérer [8]

$$\sum_{g\in G} f(hg) = \sum_{g\in G} (f\circ L_h)(g) \tag{1.24}$$

et de faire tourner la définition 1.56. La même chose tient pour définir $\sum_{g\in G}(gh)$ à l'aide de R_h.

Proposition 1.57 ([1]).
Soient un groupe fini G et une fonction $f\colon G \to A$ où A est un anneau commutatif. Alors

$$\sum_{g\in G} f(g) = \sum_{g\in G} f(gh) = \sum_{g\in G} f(hg) \tag{1.25}$$

pour tout $h \in G$.

Démonstration. Nous avons une bijection $\varphi\colon \{0,\dots,N\} \to G$ garantie par la proposition 1.27. La définition est que

$$\sum_{g\in G} f(g) = \sum_{i=0}^{N} f\big(\varphi(i)\big). \tag{1.26}$$

Par ailleurs, le lemme 1.36 donne une bijection $L_h\colon G \to G$ et permet de considérer la composée

$$\begin{aligned} \varphi'\colon \{0,\dots,N\} &\to G \\ \varphi' &= L_h \circ \varphi. \end{aligned} \tag{1.27}$$

La proposition 1.56 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 (1.24) donne

$$\begin{aligned} \sum_{g\in G} f(g) = \sum_{i=0}^{N} f\big(\varphi(i)\big) = \sum_{i=0}^{N} f\big(\varphi'(i)\big) = \sum_{i=0}^{N} (f\circ L_h\circ\varphi)(i) \\ = \sum_{i=0}^{N} (f\circ L_h)\big(\varphi(i)\big) = \sum_{g\in G} (f\circ L_h)(g) = \sum_{g\in G} f(hg). \end{aligned} \tag{1.28}$$

En ce qui concerne $\sum_{g\in G} f(gh)$, c'est la même chose, en utilisant R_h au lieu de L_h. □

8. Le fait que L_h soit une bijection n'a pas d'importance ici.

Dans le même ordre d'idée, pour le produit.

Proposition 1.58.
Si E est un ensemble fini et si G est un groupe abélien, alors pour toute fonction $f : E \to G$ et pour toute permutation σ de E,

$$\prod_{i\in E} f(i) = \prod_{i\in E} f\big(\sigma(i)\big) \tag{1.29}$$

1.5.4 Fonction puissance

Voici une première définition de la fonction puissance. Il y en aura d'autres, de plus en plus générales. Voir le thème 32.

Définition 1.59.
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 1.59 aurait pu être écrit $a^k \cdot a$ au lieu de $a \cdot a^k$.

Lemme 1.60 ([1])**.**
Si A est un anneau, si $a \in A$ et si $n \in \mathbb{N}$, alors

$$a^n = a \cdot a^{n-1} = a^{n-1} \cdot a. \tag{1.30}$$

1.6 Corps

1.6.1 Définitions, morphismes

Définition 1.61 ([15])**.**
*Un **corps** est un anneau*[9] *dans lequel tout élément non nul est inversible.*

Remarque 1.62.
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 1.61.

Proposition 1.63.
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 $A^* \subset U(A)$. i

Pour l'inclusion inverse, nous montrons qu'une élément inversible ne peut pas être nul. Cela n'est autre que le lemme 1.39 couplé à la proposition 1.40 : $a \cdot 0 = 0 \neq 1$ 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.

□

Lemme 1.64.
Un corps non nul est un anneau intègre[10].

9. Définition 1.37.
10. Définition 1.54.

Démonstration. En effet si a est un diviseur de zéro, alors $ax = 0$ pour un certain $x \neq 0$. Si a était inversible, nous aurions $x = a^{-1}ax = 0$, ce qui est impossible. □

Conséquence : dans un corps nous avons toujours la règle du produit nul, et l'élément nul n'est jamais inversible.

Définition 1.65 (Morphisme de corps)**.**
Un corps étant un anneau sans plus de structure, un ***morphisme de corps*** *n'est qu'un morphisme des anneaux.*

Le lemme suivant montre que définir un morphisme de corps comme étant simplement un morphisme des anneaux est une bonne idée.

Lemme 1.66.
Si $\phi\colon \mathbb{K} \to \mathbb{K}'$ est un morphisme de corps, alors

(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

$$1 = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1}). \tag{1.31}$$

Donc, par unicité de l'inverse[11], $\varphi(a^{-1}) = \varphi(a)^{-1}$.

Pour l'injectivité nous supposons $\varphi(a) = \varphi(b)$. Étant donné que $\mathbb{K}'$ est un corps, nous pouvons multiplier par $\varphi(b)^{-1}$:

$$\varphi(a)\varphi(b)^{-1} = 1. \tag{1.32}$$

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 $a = b$. □

1.6.2 Corps des fractions

Définition 1.67 ([16])**.**
Soit un anneau commutatif et intègre[12] *A et $E = A \times A\backslash\{0\}$. Nous y définissons les deux opérations suivantes :*

(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*

$$\mathrm{Frac}(A) = \big(A \times A\backslash\{0\}\big)/\sim . \tag{1.33}$$

Nous notons a/b la classe de (a, b).

Les éléments de $\mathrm{Frac}(A)$ *sont des* ***fractions rationnelles*** *de A.*

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 dit que $\mathrm{Frac}(A)$ est le plus petit corps contenant A.

Proposition 1.68 ([1])**.**
Si $\mathbb{L}$ est un corps contenant A en tant que sous-anneau[13]*, alors il existe un morphisme de corps injectif $\epsilon\colon \mathrm{Frac}(A) \to \mathbb{L}$.*

11. Lemme 1.34 (2).
12. Définition 1.54.
13. Bien entendu, nous pouvons trouver plein de corps contenant A en tant que sous-ensemble sans pour autant étendre A en tant qu'anneau ; il suffit d'y mettre une loi de composition farfelue.

Démonstration. Il suffit de vérifier que la formule

$$\epsilon(a/b) = ab^{-1} \tag{1.34}$$

vérifie toutes les conditions. Notons que dans le membre de droite de (1.34), l'inverse et le produit sont calculés dans $\mathbb{L}$.

Le fait que ϵ soit bien défini provient du fait que A soit commutatif :

$$\epsilon(ax/bx) = (ax)(bx)^{-1} = ab^{-1}xx^{-1} = ab^{-1} = \epsilon(a/b). \tag{1.35}$$

Le fait que ϵ soit un morphisme est une vérification de routine, par exemple ceci pour la somme :

$$\epsilon\big(a/b + c/d\big) = \epsilon\big((ad + cb)/bd)\big) = (ad + cb)(bd^{-1}) = ab^{-1} + cd^{-1}, \tag{1.36}$$

tandis que

$$\epsilon(a, b) + \epsilon(c, d) = ab^{-1} + cd^{-1}, \tag{1.37}$$

qui est égal (il faut aussi vérifier pour le produit).

Enfin ϵ est injective parce que si $\epsilon(a/b) = \epsilon(c/d)$, alors $ab^{-1} = cd^{-1}$, d'où il est facilement vu que $ad = cb$, c'est-à-dire $a/b = c/d$. □

Notons que si A est un anneau qui n'est pas un corps, le corps $\mathrm{Frac}(A)$ existe, mais si $R \in \mathrm{Frac}(A)$, il n'a pas de sens de vouloir calculer $R(\alpha)$ pour $\alpha \in A$.

Définition 1.69 (Évaluation d'une fraction rationnelle)**.**
Soit un corps $\mathbb{K}$ contenant l'anneau A. Si $R = P/Q \in \mathrm{Frac}(A)$ et si $\alpha \in \mathbb{K}$ nous définissons

$$R(\alpha) = (P/Q)(\alpha) = P(\alpha)Q^{-1}(\alpha). \tag{1.38}$$

Dans cette formule, les polynômes, l'inverse et le produit sont calculés dans $\mathbb{K}$ et non dans A.

Théorème-définition 1.70.
Soit $\mathbb{A}$ un anneau commutatif intègre.

(1) Il existe un corps commutatif $\mathbb{K}$ et un morphisme d'anneaux injectif $\epsilon\colon \mathbb{A} \to \mathbb{K}$ tels que pour tout $\lambda \in \mathbb{K}$, il existe $(a, b) \in \mathbb{A} \times \mathbb{A}^*$ tels que

$$\lambda = \epsilon(a)\big(\epsilon(b)\big)^{-1} \tag{1.39}$$

(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 $\mathbb{A}$ est le **corps des fractions** de $\mathbb{A}$, et sera noté $\mathrm{Frac}(\mathbb{A})$.*

Lemme 1.71 (Simplification de fraction)**.**
L'application $\mathbb{A} \times \mathbb{A}^* \to \mathbb{K}$ donnée par $(a, b) \mapsto \epsilon(a)\big(\epsilon(b)\big)^{-1}$ envoie (xa, xb) sur le même que (a, b).

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 1.72.
Soit un anneau A. Tout corps contenant un sous-anneau isomorphe à A contient un sous-corps isomorphe à $\mathrm{Frac}(A)$.

Démonstration. Soit un corps $\mathbb{K}$ contenant un sous-anneau A' isomorphe à A. Nous considérons la partie suivante de $\mathbb{K}$:

$$S = \{ab^{-1} \text{ tel que } a, b \in A\}. \tag{1.40}$$

Ensuite nous montrons que

$$\begin{aligned} \varphi\colon S &\to \mathrm{Frac}(A) \\ ab^{-1} &\mapsto a/b \end{aligned} \tag{1.41}$$

est un isomorphisme de corps.

Bien définie Si $ab^{-1} = xy^{-1}$ alors $ay = xb$ et donc $a/b = x/y$ par définition des classes de $\text{Frac}(A)$.

Surjectif Tout élément de $\text{Frac}(A)$ est de la forme a/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 $a/b = x/y$, et par définition des classes nous avons $ay = bx$ qui donne immédiatement $ab^{-1} = xy^{-1}$.

□

1.6.3 Suites de Cauchy dans un corps totalement ordonné

Définition 1.73.
Ordre et choses reliées dans un corps.

(1) *Un corps $\mathbb{K}$ est **totalement ordonné** s'il existe une relation d'ordre total*[14] *tel que*

(1a) *$x \leqslant y$ implique $x + z \leqslant y + z$ pour tout $x, y, z \in \mathbb{K}$*

(1b) *$x \geqslant 0$ et $y \geqslant 0$ implique $xy \geqslant 0$.*

(2) *Si $\mathbb{K}$ est un corps totalement ordonné, nous y définissons la valeur absolue par*

$$|x| = \begin{cases} x & si\ x \geqslant 0 \\ -x & si\ x \leqslant 0. \end{cases} \tag{1.42}$$

(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 $p, q \geqslant N$ alors $|x_p - x_q| \leqslant \epsilon$.*

(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 $k \geqslant N$ alors $|x_k - q| \leqslant \epsilon$.*

(5) *Un corps $\mathbb{K}$ est **archimédien** s'il est totalement ordonné et si pour tout $x, y \in \mathbb{K}$ avec $x > 0$, il existe $n \in \mathbb{N}$ tel que $nx \geqslant y$.*

(6) *Un corps totalement ordonné est **complet** si toute suite de Cauchy y est convergente.*

(7) *Si $x, \epsilon \in \mathbb{K}$ alors nous définissons la **boule ouverte** de centre a et de rayon ϵ par*

$$B(x, \epsilon) = \{y \in \mathbb{K} \text{ tel que } |x - y| < \epsilon\}, \tag{1.43}$$

*et la **boule fermée** par*

$$\overline{B(x, \epsilon)} = \{y \in \mathbb{K} \text{ tel que } |x - y| \leqslant \epsilon\}. \tag{1.44}$$

Remarque 1.74.
Nous étudierons plus tard la notion de caractéristique d'un anneau [15] ou d'un corps. Tout anneau totalement ordonné est nécessairement de caractéristique nulle, lemme 3.57.

Remarque 1.75.
En mettant côte à côte les points (4) et (7) nous pouvons dire que (x_k) converge vers q si et seulement si pour tout $\epsilon > 0$, nous avons $x_k \in B(q, \epsilon)$ à partir d'un certain indice N.

Ces boules prendront une nouvelle force avec le super-théorème 7.88.

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.

14. Définition 1.8.
15. définition 3.53

Lemme 1.76 (Propriétés de la valeur absolue)**.**
Soit $\mathbb{K}$ un corps totalement ordonné. Si $x, y \in \mathbb{K}$ alors

(1) Si $x \geqslant 0$ alors $-x \leqslant 0$.

(2) $|x| \geqslant 0$

(3) $|x| = 0$ si et seulement si $x = 0$

(4) $|x + y| \leqslant |x| + |y|$.

Démonstration. Point par point

(1) Nous partons de $x \geqslant 0$ et nous ajoutons $-x$ des deux côtés en profitant de la définition d'un corps totalement ordonné : $x - x \geqslant -x$ et donc $0 \geqslant -x$, c'est-à-dire $-x \leqslant 0$.

(2) Si $x \geqslant 0$ alors c'est vrai. Sinon, $x \leqslant 0$ et $|x| = -x \geqslant 0$ par le point (1).

(3) 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 $\pm x \neq 0$.

(4) Nous supposons que $x \leqslant y$ et nous distinguons divers cas suivant la positivité de x et y.

(4a) Si $x, y \geqslant 0$. Dans ce cas, $x + y \geqslant y \geqslant 0$, donc $|x + y| = x + y = |x| + |y|$.

(4b) Si $x, y \leqslant 0$. Dans ce cas, $x + y \leqslant 0$ et nous avons $|x + y| = -x - y = |x| + |y|$.

(4c) Si $x \leqslant 0$ et $y \geqslant 0$. Nous subdivisons encore en deux cas suivant que $x + y$ est positif ou négatif. Si $x + y \geqslant 0$, alors nous écrivons successivement

$$x \leqslant 0 \tag{1.45a}$$
$$x + y \leqslant y \leqslant y + |x| = |x| + |y| \tag{1.45b}$$

et donc $|x + y| = x + y \leqslant |x| + |y|$.

Nous supposons à présent que $x \leqslant 0$, $y \geqslant 0$ et $x + y \leqslant 0$. 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 1.77.
La partie (4) 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

$$|x - y| = |(x - z) + (z - y)| \leqslant |x - z| + |z - y|. \tag{1.46}$$

Lemme 1.78 (À propos de boules)**.**
Soient un corps totalement ordonné $\mathbb{K}$ et des éléments $x, y, \epsilon \in \mathbb{K}$.

(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,

$$|x - y| = \begin{cases} x - y & \text{si } x - y \geqslant 0 \\ y - x & \text{si } x - y \leqslant 0. \end{cases} \tag{1.47}$$

Nous pouvons maintenant démontrer nos choses.

(1) 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 $|x - y| < \epsilon$.

Dans l'autre sens, nous supposons que $|x - y| < \epsilon$.

Si $x - y \geqslant 0$ alors l'hypothèse signifie $x - y < \epsilon$, ce qui donne $y > x - \epsilon$. Mais l'inégalité $x - y \geqslant 0$ donne également $x \geqslant y$ et donc $x + \epsilon \geqslant y + \epsilon > y$. Notez le jeu de l'inégalité non stricte qui se change en inégalité stricte.

Si $x - y \leqslant 0$ nous pouvons faire le même raisonnement.

(2) C'est immédiat parce que

$$|x-y| \leqslant \epsilon < \epsilon'. \tag{1.48}$$

□

Proposition 1.79.
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 encore pas défini ni $\mathbb{R}$ ni $\mathbb{Q}$.

Vu que (x_n) converge vers x, il existe $N \in \mathbb{N}$ tel que pour tout $k > N$,

$$|x_k - x| < \epsilon. \tag{1.49}$$

Soient $p, q > N$. Alors en utilisant la majoration du lemme 1.76(4),

$$|x_p - x_q| = \big|(x_p - x) + (x - x_q)\big| \leqslant |x_p - x| + |x - x_q| \leqslant 2\epsilon. \tag{1.50}$$

Donc la suite (x_n) est de Cauchy. □

1.7 Les rationnels

Une construction très explicite est faite dans [9]. Ici nous allons prendre plus court :

Définition 1.80.
*Le corps des fractions de $\mathbb{Z}$ (définition 1.67) est noté $\mathbb{Q}$ et ses éléments sont les **rationnels**.*

Les résultats énoncés ici sont utilisés plus bas et servent de guide à un éventuel contributeur qui voudrait écrire une partie dédiée à $\mathbb{Q}$ et ses propriétés de base[16]. Nous espérons que des preuves se trouvent dans [9]. En tout cas, le lecteur est invité à ne rien prendre comme évident.

Lemme 1.81.
Tout rationnel est majoré par un naturel.

Proposition 1.82.
L'ensemble des rationnels est dénombrable.

Proposition 1.83.
Si $q < 1$, alors $qx < x$ pour tout $x \in \mathbb{Q}^+$.

Proposition 1.84.
Le corps $\mathbb{Q}$ est archimédien[17].

1.7.1 Suites de Cauchy dans les rationnels

Proposition 1.85 ([9])**.**
Principales propriétés des suites de Cauchy dans $\mathbb{Q}$.

(1) Toute suite convergente est de Cauchy[18].

(2) Toute suite de Cauchy est bornée.

(3) Si $x_n \to 0$ et si (y_n) est bornée, alors $x_n y_n \to 0$

(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.

16. Par exemple, définir une relation d'ordre sur $\mathbb{Q}$ et expliciter l'inclusion de $\mathbb{Z}$ dans $\mathbb{Q}$.
17. Définition 1.73(5).
18. Et non la réciproque, qui sera justement la grande innovation des nombres réels.

(5) *Si il existe $a, b \in \mathbb{Q}$ tels que $x_n \to a$ et $y_n \to b$ alors $x_n + y_n \to a + b$, $x_n - y_n \to a - b$ et $x_n y_n \to ab$.*

(6) *Soit (x_n) une suite de Cauchy qui ne converge pas vers zéro. Alors il existe n_0 tel que la suite $\left(\frac{1}{x_n}\right)_{n \geqslant n_0}$ soit de Cauchy.*

Démonstration. Point par point.

(1) C'est la proposition 1.79.

(2) Soit (x_n) une suite de Cauchy dans $\mathbb{Q}$. Avec $\epsilon = 1$ dans la définition, si $q > N_1$, nous avons

$$|x_q - x_{N_1}| \leqslant 1. \tag{1.51}$$

Et donc pour tout q plus grand que N_1, $x_N - 1 \leqslant x_q \leqslant x_N + 1$, ou encore, pour tout n :

$$|x_n| \leqslant \max\{|x_1|, |x_2|, \dots, |x_N|, |x_N + 1|\}. \tag{1.52}$$

La suite est donc bornée.

(3) Soit $\epsilon > 0$. Les hypothèses disent qu'il existe un N tel que $|x_n| \leqslant \epsilon$ dès que $n \geqslant N$. Et il existe aussi $M \geqslant 0$ tel que $|y_n| \leqslant M$ pour tout n. Du coup, lorsque $n \geqslant N$ nous avons $|x_n y_n| \leqslant M\epsilon$.

(4) En ce qui concerne la somme,

$$|x_p + y_p - x_q - y_q| \leqslant |x_p - x_q| + |y_p - y_q|. \tag{1.53}$$

Soit N_1 tel que si $p, q \geqslant N_1$ alors $|x_p - x_q| \leqslant \epsilon$ et N_2 de même pour la suite (y_n). En prenant $N = \max\{N_1, N_2\}$, la somme (1.53) est plus petite que 2ϵ dès que $p, q \geqslant N$.

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 $|x_n| \leqslant M$ et $|y_n| \leqslant M$. Nous avons :

$$|x_p y_p - x_q y_q| \leqslant |x_p y_p - x_q y_p| + |x_q y_p - x_q y_q| \leqslant |y_p||x_p - x_q| + |x_q||y_p - y_q|. \tag{1.54}$$

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

$$|x_p y_p - x_q y_q| \leqslant M\epsilon + M\epsilon = 2M\epsilon, \tag{1.55}$$

ce qui prouve que $(x_n y_n)$ est de Cauchy.

(5) En ce qui concerne la somme, nous pouvons tout de suite calculer

$$|x_n + y_n - (a + b)| \leqslant |x_n - a| + |y_n - b|. \tag{1.56}$$

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,

$$|x_n y_n - ab| \leqslant |x_n y_n - a y_n| + |a y_n - ab| \leqslant |y_n||x_n - a| + |a||y_n - b|. \tag{1.57}$$

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

$$y_n|x_n - a| + a|y_n - b| \to 0. \tag{1.58}$$

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 $n \geqslant N$ tel que $|x_n| > \alpha$. Mais notre suite est de Cauchy, donc il existe $n_0 \in \mathbb{N}$ tel que si $p, q \geqslant n_0$ alors

$$|x_p - x_q| \leqslant \frac{\alpha}{2}. \tag{1.59}$$

En fixant $N = n_0$, on obtient un naturel $n \geqslant n_0$ tel que $|x_n| \geqslant \alpha$. De plus, comme la suite est de Cauchy, si $p > n$ nous avons aussi $|x_n - x_p| \leqslant \frac{\alpha}{2}$. Cela implique $|x_p| \geqslant \frac{\alpha}{2}$ 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 $|x_k| \geqslant \alpha/2$ pour tout $k \geqslant n$. La suite $(1/x_k)_{k\geqslant n}$ 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 $p, q \geqslant K$, nous avons $|x_p| > \frac{\alpha}{2}$ et $|x_q| > \frac{\alpha}{2}$. Nous en déduisons que

$$\left|\frac{1}{x_p} - \frac{1}{x_q}\right| \leqslant \frac{|x_q - x_p|}{|x_p x_q|} \leqslant \frac{4}{\alpha^2}|x_q - x_p| \leqslant \frac{4}{\alpha^2}\epsilon. \tag{1.60}$$

Donc $\left(\frac{1}{x_n}\right)$ est de Cauchy.

□

1.7.2 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 $x_n^2 \to 2$.

Lemme 1.86.
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 3.36 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 1.130.

Proposition 1.87 (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 1.86 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 élément [19]. Il n'y a donc pas de fractions d'entiers dont le carré vaut 2. □

Lemme 1.88 (Série géométrique, voir aussi l'exemple 12.75)**.**
Si $q \in \mathbb{Q}$ et $p \in \mathbb{N}$ nous avons

$$\sum_{k=0}^{p} q^k = \frac{1-q^{p+1}}{1-q}. \tag{1.61}$$

Démonstration. En posant $S_p = 1 + q + q^2 + \cdots + q^p$, nous avons $S_p - qS_p = 1 - q^{p+1}$ et donc

$$S_p = \sum_{k=0}^{p} q^k = \frac{1-q^{p+1}}{1-q}. \tag{1.62}$$

□

Proposition 1.89.
La suite donnée par

$$x_n = 1 + \frac{1}{1!} + \cdots + \frac{1}{n!} \tag{1.63}$$

est de Cauchy et ne converge pas dans $\mathbb{Q}$.

Démonstration. Si $p > q > 0$ nous avons

$$x_p - x_q = \sum_{k=q+1}^{p} \frac{1}{k!} \tag{1.64a}$$

$$\leqslant \sum_{k=q+1}^{p} \frac{1}{(q+1)!} \frac{1}{(q+1)^{k-q-1}} \tag{1.64b}$$

$$\leqslant \frac{1}{(q+1)!} \lim_{p\to\infty} \sum_{k=0}^{p} \frac{1}{(q+1)^k} \tag{1.64c}$$

$$= \frac{1}{(q+1)!} \frac{1}{1-\frac{1}{q+1}} \tag{1.64d}$$

$$= \frac{1}{(q+1)!} \frac{q+1}{q} \tag{1.64e}$$

$$= \frac{1}{q!q}. \tag{1.64f}$$

Justifications :

— Pour (1.64b), 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 (1.64c), 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 (1.64d), le lemme 1.88 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

$$x_p - x_q \leqslant \frac{1}{b!b} < \frac{1}{b} < \frac{a}{b} = \epsilon. \tag{1.65}$$

Montrons par l'absurde que cette suite ne converge pas dans $\mathbb{Q}$. Pour cela, nous supposons que $\lim_{n\to\infty} x_n = \frac{a}{b} \in \mathbb{Q}$. Pour tout $p > q$ nous avons établi

$$0 < x_p - x_q < \frac{1}{qq!}. \tag{1.66}$$

19. Voir [9], et attention : ce n'est pas tout à fait évident.

Prenons la limite $p \to \infty$; par stricte croissance de la suite, les inégalités restent strictes :

$$0 < \frac{a}{b} - x_q < \frac{1}{qq!}. \tag{1.67}$$

Si $n > b$ alors nous pouvons écrire

$$\frac{a}{b} - x_n = \frac{\alpha}{n!} \tag{1.68}$$

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 (1.67) nous pouvons écrire

$$0 < \frac{\alpha}{q!} < \frac{1}{qq!}, \tag{1.69}$$

c'est-à-dire $0 < \alpha < \frac{1}{q}$, ce qui est impossible pour $\alpha \in \mathbb{Z}$. □

Lemme 1.90.
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 1.84), il existe $n \in \mathbb{N}$ tel que $1 < nA$. Pour ce n, nous avons

$$\left(\frac{1}{n}\right)^2 < \frac{1}{n} < A. \tag{1.70}$$

□

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 [3] que la suite est motivée par la méthode de Newton 35.53.

Proposition 1.91 ([3])**.**
Soient $A > 0$ dans $\mathbb{Q}$ et $x_0 \in \mathbb{Q}$. La suite (x_k) définie par

$$x_{k+1} = \frac{1}{2}\left(x_k + \frac{A}{x_k}\right) \tag{1.71}$$

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

$$y_{k+1} - A = \frac{(y_k - A)^2}{4y_k}. \tag{1.72}$$

Autrement dit, la suite $s_k = y_k - A$ vérifie

$$s_{k+1} = \frac{s_k^2}{4(A + s_k)}. \tag{1.73}$$

Quelle que soit la valeur de $s_0 = x_0^2 - A$, nous avons

$$s_1 = \frac{s_0^2}{4(A + s_1)} = \frac{(x_0^2 - A)^2}{4(A + x_0^2 - A)} = \frac{(x_0^2 - A)}{4x_0^2} > 0. \tag{1.74}$$

Donc à partir de s_1, tous les éléments sont positifs. Vu que $A > 0$ nous avons aussi

$$s_{k+1} < \frac{s_k^2}{4s_k} = \frac{s_k}{4} \tag{1.75}$$

et donc $s_k < s_0/4^k$. Donc $s_k \to 0$.

La suite (y_k) Nous venons de prouver que si $y_k = A + s_k$, alors $s_k \to 0$. Autrement dit, la suite y_k converge vers A dans $\mathbb{Q}$.

La suite (y_k) est donc de Cauchy par la proposition 1.85(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

$$|x_r^2 - x_s^2| < \epsilon \tag{1.76}$$

pour tout $r, s \geqslant n_0$.

Soit par ailleurs $q \in \mathbb{Q}$ tel que $q^2 < A$, assuré par le lemme 1.90. Quitte à prendre n_0 plus grand, nous supposons que $x_r, x_s > q$, et en particulier que $x_r + x_s \neq 0$. Cela permet d'écrire d'abord

$$x_r^2 - x_s^2 = (x_r + x_s)(x_r - x_s) \tag{1.77}$$

et ensuite de prendre la valeur absolue et de diviser par $|x_r + x_s|$:

$$|x_r - x_s| = \frac{|x_r^2 - x_s^2|}{|x_r + x_s|} < \frac{\epsilon}{2q}. \tag{1.78}$$

Donc (x_k) est une suite de Cauchy.

Pas de convergence pour $A = 2$ Supposons que $x_k \to a \in \mathbb{Q}$. Dans ce cas nous aurions $x_k^2 \to a^2 = A = 2$ (proposition 1.85(5)). Mais nous savons par la proposition 1.87 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 3.36 dira que $\sqrt{n}$ est soit entier soit irrationnel.

1.92.
Un petit programme en python explorer la suite de la proposition 1.91.

```python
#!/usr/bin/python3

def rec(A,x):
    return ((x**2+A)/x)/2

A = 3        # Compute square root of 3
x = 1000     # Initial guess: 1000

for i in range(1,100):
    print(i, x, x**2, x**2-A)
    x = rec(A, x)
```

tex/frido/codeSnip_4.py

1.8 Les réels

Une construction des réels via les coupures de Dedekind est donnée dans [17].

1.93.
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 9.19) alors que la topologie métrique (celle entre autres de $\mathbb{Q}$) ne sera définie que par le théorème 7.88. Nous avons donc dû définir en la définition 1.73 *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 topologiques [20]. Et par conséquent que $\mathbb{R}$ sera un espace métrique complet [21].

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[18].

1.8.1 L'ensemble

Soit $\mathcal{E}$ l'ensemble des suites de Cauchy [22] dans $\mathbb{Q}$. Soit aussi l'ensemble $\mathcal{E}_0$ constituée des suites qui convergent vers zéro [23].

En posant

$$x + y = (x_n + y_n) \tag{1.79}$$

et

$$xy = (x_n y_n), \tag{1.80}$$

l'ensemble $\mathcal{E}$ devient un anneau [24] 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 1.94.
La partie $\mathcal{E}_0$ est un idéal[25] *de l'anneau $\mathcal{E}$.*

Démonstration. Nous savons par la proposition 1.85(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 1.85 (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 $x \to 0$ nous avons alors $xy \to 0$ (par la proposition 1.85(3)). □

Théorème-définition 1.95 (L'anneau des réels[9])**.**
Sur l'ensemble quotient $\mathcal{E}/\mathcal{E}_0$, les opérations

(1) $\bar{u} + \bar{v} = \overline{u + v}$

(2) $\bar{u} \cdot \bar{v} = \overline{uv}$

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 Si $u, v \in \mathcal{E}$ et $h, k \in \mathcal{E}_0$ alors $h + k \in \mathcal{E}_0$ et nous avons

$$\overline{u + h} + \overline{v + k} = \overline{u + v + h + k} = \overline{u + v}. \tag{1.81}$$

20. Proposition 9.26.
21. Théorème 1.118 pour la complétude en tant que corps et théorème 1.79 pour la complétude en tant que espace métrique.
22. Définition 1.73(3)
23. Nous rappelons qu'à ce niveau nous n'avons pas encore prouvé que toutes les suites de Cauchy convergent.
24. Définition 1.37.
25. Définition 1.44.

ainsi que

$$\overline{u+h}\cdot\overline{v+k}=\overline{(u+h)(v+k)}=\overline{uv+uk+hv+hk}=\overline{uv} \tag{1.82}$$

parce que les suites des Cauchy u et v sont bornées, ce qui donne que uk, hv et hk sont des éléments de $\mathcal{E}_0$ par la proposition 1.85(3). Cela prouve que les définitions proposées sont bonnes.

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

$$\bar{x}=\{\text{suites qui convergent vers } q\}. \tag{1.83}$$

Si $y\in\bar{x}$ alors $y=x+h$ avec $h\in\mathcal{E}_0$, et comme $h_n\to 0$, on a $y_n\to q$. Réciproquement, si $y_n\to q$ alors pour chaque n nous avons

$$y_n=x_n+(y_n-x_n), \tag{1.84}$$

mais $y_n-x_n\to 0$. 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 zéro [26] alors il existe $y\in\mathcal{E}$ tel que $xy\in\bar{1}$.

Nous savons par la proposition 1.85(6) que x étant une suite de Cauchy dans $\mathbb{Q}$, il existe $n_0\in\mathbb{N}$ tel que $\left(\frac{1}{x_n}\right)_{n\geqslant n_0}$ est une suite de Cauchy. Nous posons alors

$$y_n=\begin{cases}0 & \text{si } n\leqslant n_0\\ \frac{1}{x_n} & \text{si } n>n_0.\end{cases} \tag{1.85}$$

Nous avons alors

$$(xy)_n=\begin{cases}0 & \text{si } n\leqslant n_0\\ 1 & \text{si } n>n_0\end{cases} \tag{1.86}$$

et donc $xy\in\bar{1}$.

□

1.96 (Quelque 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 notations 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 $x_k\to x$.

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

$$\begin{aligned}\varphi\colon\mathbb{Q}&\to\mathbb{R}\\ q&\mapsto\overline{[k\mapsto q]},\end{aligned} \tag{1.87}$$

c'est à dire que $\varphi(q)$ est la classe de la suite constante $x_k=q$.

Proposition 1.97.
Soit l'application

$$\begin{aligned}\varphi\colon\mathbb{Q}&\to\mathbb{R}\\ q&\mapsto\bar{q}.\end{aligned} \tag{1.88}$$

où par $\bar{q}$ nous entendons la classe de la suite constante égale à q (qui est de Cauchy).

26. $x\in\mathcal{E}$ peut soit ne pas converger du tout, soit converger vers autre chose que zéro.

(1) C'est un homomorphisme de corps injectif.

(2) Image(φ) *est un sous-corps de* $\mathbb{R}$

(3) $\varphi\colon \mathbb{Q} \to$ Image(φ) *est un isomorphisme de corps.*

Démonstration. Le fait que ce soit un homomorphisme est simplement

— $\varphi(q+q') = \overline{q+q'} = \bar{q} + \overline{q'}$

— $\varphi(qq') = \overline{qq'} = \bar{q}\overline{q'}$.

En ce qui concerne l'injectivité, si q est tel que $\varphi(q) = \bar{0} = \mathcal{E}_0$, c'est que

$$\varphi(q) = \{\text{suites de Cauchy qui convergent vers zéro}\} \tag{1.89}$$

Mais nous savons aussi que[27]

$$\varphi(q) = \bar{q} = \{\text{suites de Cauchy qui convergent vers } q\} \tag{1.90}$$

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.

1.8.2 Relation d'ordre

Nous définissons les parties $\mathcal{E}^+$ et $\mathcal{E}^-$ de $\mathcal{E}$ par

(1) $x \in \mathcal{E}^+$ si et seulement si pour tout $\epsilon > 0$, 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 $\mathcal{E}^{++} = \mathcal{E}^+ \backslash \mathcal{E}_0$.

Lemme 1.98.
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 $n \geqslant N$. Par conséquent, $|x_n| \leqslant \epsilon$ pour tout $n \geqslant N$ et la suite x converge vers zéro, c'est-à-dire $x \in \mathcal{E}_0$.

Pour prouver le second point, soit $x \in \mathcal{E}\backslash\mathcal{E}^-$, 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 $n, p \geqslant n_0$ alors $|x_n - x_p| \leqslant \frac{\alpha}{2}$. En particulier, si $n \geqslant n_0$, et si $p > n$ est tel que $x_p > \alpha$, on obtient

$$x_n > \frac{\alpha}{2} > 0 \tag{1.91}$$

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. □

Lemme 1.99 ([9])**.**
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.

27. Voir dans la démonstration du théorème 1.95.

(1) Définition de $\mathcal{E}^+$ et $\mathcal{E}^-$.

(2) Pour $n \geqslant N_{\epsilon/2}$ 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 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 $n \geqslant n_1$. Mais $x - y \in \mathcal{E}_0$, donc il existe n_2 tel que $|x_n - y_n| < \frac{\epsilon}{2}$ dès que $n \geqslant n_2$. En prenant n plus grand que n_1 et n_2, nous avons en même temps

$$\begin{cases} x_n > -\frac{\epsilon}{2} & \text{(1.92a)} \\ |x_n - y_n| < \frac{\epsilon}{2}. & \text{(1.92b)} \end{cases}$$

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 $y \in \mathcal{E}^-$.

□

Définition 1.100 (Positivité dans $\mathbb{R}$)**.**
Vocabulaire et notations.

(1) Nous notons $\mathbb{R} = \mathcal{E}/\mathcal{E}_0$.

(2) Nous notons $\mathbb{R}^+ = \mathcal{E}^+$.

(3) Nous notons $\mathbb{R}^- = \mathcal{E}^-$.

*(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 $\mathcal{E}_0$.

1.101.
Avec les conventions de la définition 1.100, 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 $\mathbb{R}^+\backslash\{0\}$.

(4) Le mot « positif » signifie « positif ou nul » ; le mot « négatif » signifie « négatif ou nul ».

Cela vient des conventions de la remarque 1.101 qui sont également celles de Wikipédia[19].

Définition 1.102 (Ordre dans $\mathbb{R}$)**.**
Si $a, b \in \mathbb{R}$ nous notons $a \leqslant b$ si et seulement si $b - a$ est positif. Nous notons aussi $a > b$ si et seulement si $b - a \in \mathbb{R}^+\backslash\{0\}$, etc.

Lemme 1.103.
Les premières propriétés de l'ordre.

(1) L'ensemble $(\mathbb{R}, \leqslant)$ est un corps totalement ordonné (définitions 1.8 et 1.73).

(2) L'application

$$\begin{aligned} \varphi\colon \mathbb{Q} &\to \mathbb{R} \\ q &\mapsto \bar{q} \end{aligned} \tag{1.93}$$

dont nous avons déjà parlé dans la proposition 1.97 est strictement croissante.

Démonstration. Nous prouvons la stricte croissance de φ. Si $q < l$ alors $\varphi(q) - \varphi(l) = \overline{q - l}$ est la classe de la suite constante $q - l$ qui est un élément strictement positif de $\mathbb{Q}$. Nous avons donc $\overline{q - l} \in \mathbb{R}^+$, et donc $\varphi(q) < \varphi(l)$. □

Remarque 1.104.
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 1.105.
Si $x, y, z \in \mathbb{R}$ avec $x > 0$ sont tels que $z > y/x$ alors $zx > y$.

Démonstration. Nous savons que

$$z - \frac{y}{x} \in \mathcal{E}^+ \backslash \{0\} = \mathcal{E}^{++}. \tag{1.94}$$

Vu que $x \in \mathcal{E}^{++}$, multiplier par x fait rester dans $\mathcal{E}^{++}$:

$$zx - x\frac{y}{x} \in \mathcal{E}^{++}. \tag{1.95}$$

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 1.106.
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 $|a_n| \leqslant m/q$ pour tout n (proposition 1.85(2)). Soit M un naturel strictement plus grand que m/q[28].

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 positif[29]. Par définition de la relation d'ordre, $M \geqslant a$.

Seconde façon La suite (a_n) est majorée par $\frac{m}{q}$, donc on a dans $\mathbb{Q}$ et pour tout n :

$$a_n \leqslant \frac{m}{q} = M \leqslant qM. \tag{1.96}$$

L'application $\varphi\colon \mathbb{Q} \to \mathbb{R}$ est croissante, donc

$$\varphi\big((a_n)\big) \leqslant \varphi(qM). \tag{1.97}$$

□

En corollaire, nous avons

Lemme 1.107.
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 1.108 ([9]).
Le corps $\mathbb{R}$ est archimédien[30].

Démonstration. Le lemme 1.103 dit que $\mathbb{R}$ est totalement ordonné. Soient $x, y \in \mathbb{R}$ avec $x > 0$; posons $a = \frac{y}{x}$. Le lemme 1.106 nous donne un $p \in \mathbb{N}$ tel que $p > a$.Nous concluons alors avec le lemme 1.105 :

$$px > ax = \frac{y}{x}x = y. \tag{1.98}$$

□

28. Lemme 1.81.
29. Et nous allons d'ailleurs arrêter de toujours préciser « la classe de » lorsque ce n'est pas nécessaire.
30. Définition 1.73(5).

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 1.109.
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 1.108) nous donne $q \in \mathbb{N}$ tel que $q(y - x) > 1$. Soit

$$E = \{n \in \mathbb{Z} \text{ tel que } \frac{n}{q} \leqslant x\}. \tag{1.99}$$

Cet ensemble n'est pas vide à cause du lemme 1.107 ; de plus, comme $|x|q \leqslant n_0$ pour un certain n_0 (à cause du lemme 1.106), l'ensemble E est majoré par n_0. Donc E possède un plus grand élément [31] p qui vérifie

$$\frac{p}{q} \leqslant x < \frac{p+1}{q}. \tag{1.100}$$

De plus $(p+1)/q < y$. En effet nous avons

$$\frac{p+1}{q} = \frac{p}{q} + \frac{1}{q} \leqslant x + \frac{1}{q} < x + y - x = y \tag{1.101}$$

où nous avons utilisé l'inégalité stricte $y - x > \frac{1}{q}$.

Nous avons donc

$$x < \frac{p+1}{q} < y, \tag{1.102}$$

et le nombre $(p+1)/q$ convient comme s. □

Remarque 1.110.
Le lemme 1.109 a également pour conséquence que des ensembles comme $[-1, 1]$ ne sont pas bien ordonnés (définition 1.8). 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...

1.111.
Soit $q_0 \in \mathbb{Q}$ tel que $0 \leqslant q_0 < 1$. On définit alors $d_1 \in \{0, 1\}$ comme valant 1 si $2q_0 \geqslant 1$ et 0 sinon. Puis on pose $q_1 = 2q_0 - d_1$.

Poursuivant de la sorte, on crée une suite $(d_n)_{n\geqslant 1}$: c'est le **développement dyadique** de q_0.

Lemme 1.112 ([1])**.**
Soit q, q' deux rationnels tels que $0 \leqslant q < q' < 1$. 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 $(d_n)_{n\geqslant 1}$ et $(d'_n)_{n\geqslant 1}$. Notons

$$E = \{n \in \mathbb{N} \text{ tel que } d_n \neq d'_n\}. \tag{1.103}$$

Comme $q \neq q'$, les développements dyadiques sont différents [32], 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 $a = \sum_{i=1}^{N} d_i 2^i$. □

Corollaire 1.113.
Pour tous réels x, y tels que $0 \leqslant x < y \leqslant 1$, il existe un nombre de la forme $d = a/2^n$, avec $n \in \mathbb{N}$ et $a \in \mathbb{N}$, $a \leqslant 2^n$, tel que $x < d < y$.

31. Lemme 1.48.
32. À vérifier tout de même...

Lemme 1.114 ([1]).
Soient des réels a, b, x, y tels que

$$a \leqslant x \leqslant b \tag{1.104}$$

et

$$a \leqslant y \leqslant b, \tag{1.105}$$

alors $|x - y| \leqslant |b - a|$.

1.8.3 Complétude

Lemme 1.115 ([9]).
Toute suite de Cauchy dans $\mathbb{Q}$ converge dans $\mathbb{R}$ vers le réel qu'elle représente.

Plus précisément, en suivant les notations de 1.96, si (x_k) est une suite de Cauchy dans $\mathbb{Q}$, alors la suite $\varphi(x_k)$ dans $\mathbb{R}$

(1) est de Cauchy dans $\mathbb{R}$,

(2) converge dans $\mathbb{R}$ vers $\bar{x}$.

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 $\lim_{n\to\infty} x_n = \bar{x}$. Dans cette dernière limite, chacun des x_n est vu dans $\mathbb{R}$.

Si $\epsilon \in \mathbb{Q}$ est donné, il existe N_ϵ tel que si $p, q \geqslant N_\epsilon$ alors $|x_p - x_q| < \epsilon$, c'est-à-dire

$$x_p - \epsilon < x_q < x_p + \epsilon. \tag{1.106}$$

Soit $p \geqslant N_\epsilon$ fixé. Pour tout $q \geqslant N_\epsilon$ nous avons $x_p - \epsilon < x_q < x_p + \epsilon$. Par conséquent, la suite $n \mapsto (x_p - \epsilon) - q_n$ est un élément de $\mathcal{E}^-$ et au niveau des classes nous pouvons écrire

$$\overline{n \mapsto (x_p - \epsilon) - x_n} \leqslant 0. \tag{1.107}$$

Vu que $x_p - \epsilon$ représente la suite constante nous avons l'inégalité suivante dans $\mathbb{R}$:

$$x_p - \epsilon - \bar{x} \leqslant 0 \tag{1.108}$$

ou encore : $\bar{x} \geqslant x_p - \epsilon$. En faisant de même avec l'autre partie de l'inégalité, $x_p - \epsilon \leqslant \bar{x} \leqslant x_p + \epsilon$, ce qui implique que

$$x_p \in B(\bar{x}, \epsilon) \tag{1.109}$$

dès que $p \geqslant N_\epsilon$. Cela signifie que $x_p \to \bar{x}$ dans $\mathbb{R}$. □

Proposition 1.116.
Soit une suite convergente $x_k \xrightarrow{\mathbb{Q}} q$. Alors

$$\varphi(x_k) \xrightarrow{\mathbb{R}} \varphi(q) \tag{1.110}$$

où φ est la fonction qui à un rationnel fait correspondre la classe de la suite constante correspondante[33].

Démonstration. Le fait d'avoir une convergence $x_k \to q$ dans $\mathbb{Q}$ implique que la suite (x_k) est de Cauchy, par la proposition 1.85(1).

Le lemme 1.115 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. □

33. Voir les notations en 1.96.

Proposition 1.117 ([1]).
Deux choses à propos de suites de rationnels convergent 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 1.109 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 choisit 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 $0 < q_0 < x$. □

Théorème 1.118 (Complétude de $\mathbb{R}$, critère de Cauchy[9]).
Nous avons :

(1) Le corps $\mathbb{R}$ est un corps complet (définition 1.73(6))

(2) Une suite dans $\mathbb{R}$ est convergente (définition 1.73(4)) si et seulement si elle est de Cauchy (définition 1.73(3)).

Notez la grande similitude entre ce théorème et le théorème 9.39. 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 1.109 un $y_n \in \mathbb{Q}$ tel que

$$x_n - \frac{1}{n} < y_n < x_n + \frac{1}{n}. \tag{1.111}$$

(y_n) est une suite de Cauchy dans $\mathbb{Q}$ Nous prouvons que (y_n) est une suite de Cauchy dans $\mathbb{Q}$ (définition 1.73(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 $p, q \geqslant n_\epsilon$, alors $|x_p - x_q| < \epsilon$.

Nous avons :

$$|y_p - y_q| \leqslant |y_p - x_p| + |x_p - x_q| + |x_q - y_q| < \frac{1}{p} + \epsilon + \frac{1}{q}. \tag{1.112}$$

En choisissant $N_\epsilon > \max\{n_\epsilon, \frac{1}{\epsilon}\}$ (ce qui est possible par le lemme 1.106), et en prenant $p, q > N_\epsilon$, nous avons

$$|y_p - y_q| \leqslant 3\epsilon, \tag{1.113}$$

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 1.115). 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

$$|\bar{y} - x_p| \leqslant |\bar{y} - y_p| + |y_p - x_p| \leqslant \epsilon + \frac{1}{p}. \tag{1.114}$$

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 1.79. □

Nous avons terminé avec la construction des réels. Les propriétés topologiques arrivent en la section 8.1. En particulier le théorème 9.39 pour la complétude de $\mathbb{R}$ en tant qu'espace métrique.

1.8.4 Intervalles

Nous avons déjà défini la notion d'intervalle pour un espace totalement ordonné en 1.13. Nous posons quelque notations dans $\mathbb{R}$.

Définition 1.119.
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) $[a,b[= \{x \in \mathbb{R} \text{ tel que } a \leqslant x < b\}$
(3) $]a,b] = \{x \in \mathbb{R} \text{ tel que } a < x \leqslant b\}$
(4) $[a,b] = \{x \in \mathbb{R} \text{ tel que } a \leqslant x \leqslant b\}$
(5) $]-\infty,a] = \{x \in \mathbb{R} \text{ tel que } x \leqslant a\}$
(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) $[a,\infty[= \{x \in \mathbb{R} \text{ tel que } x \geqslant a\}$.
(9) $]-\infty,\infty[= \mathbb{R}$.

La proposition 1.123 nous dira que tous les intervalles de $\mathbb{R}$ sont d'une de ces formes.

1.8.5 Maximum, supremum et compagnie

Ce n'est un secret pour personne que $\mathbb{R}$ est un ensemble totalement ordonné[34] : 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 1.120.
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 $x \in A$, $M \geqslant x$.*
*(2) Un nombre m est un **minorant** de A si m est plus petit que tous les éléments de A : pour tout $x \in A$, $m \leqslant x$.*

Nous parons 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 1.121
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.

△

34. Lemme 1.103(1), définition 1.102.

Proposition-définition 1.122 (Least-upper-bound property[20]).
Soit A une partie majorée de $\mathbb{R}$. Il existe un unique élément $M \in \mathbb{R}$ tel que

(1) $M \geqslant x$ 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 $\infty \notin \mathbb{R}$.

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 1.109). 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) :

$$\begin{aligned} &x_0 \text{ est un élément de } A,\\ &x_1 \text{ est un minorant de } A,\\ &a_0 = x_0\\ &b_0 = x_1\\ &b_1 = x_1. \end{aligned} \tag{1.115}$$

Ensuite, nous faisons la récurrence suivante :

$$\begin{aligned} x_{n+1} &= \frac{a_n + b_n}{2},\\ a_{n+1} &= \begin{cases} a_n & \text{si } x_{n+1} \text{ minore } A\\ x_{n+1} & \text{sinon,} \end{cases}\\ b_{n+1} &= \begin{cases} x_{n+1} & \text{si } x_{n+1} \text{ minore } A\\ b_n & \text{sinon.} \end{cases} \end{aligned} \tag{1.116}$$

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

$$\begin{aligned} |a_n - b_n| &= |a_{n-1} - x_n|\\ &= \left|a_{n-1} - \frac{a_{n-1} + b_{n-1}}{2}\right|\\ &= \frac{1}{2}|a_{n-1} - b_{n-1}|, \end{aligned} \tag{1.117}$$

ce qui prouve que $|a_n - b_n| \to 0$. Nous montrons maintenant que la suite (a_n) est de Cauchy. En effet nous avons

$$|a_n - a_{n-1}| = \begin{cases} 0\\ \left|\frac{a_n - b_n}{2}\right| \end{cases} \leqslant \frac{1}{2n}. \tag{1.118}$$

Il en est de même pour la suite (b_n). Ce sont deux suites de Cauchy (donc convergentes par la proposition 1.79) 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. □

1.8.5.1 Intervalles

Proposition 1.123.
Tous les intervalles de $\mathbb{R}$ sont d'une des formes listées dans la définition 1.119.

1.8.5.2 Quelques exemples

En matières 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 1.124
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 :

$$10 = \max[0, 10] = \sup[0, 10] \quad 10 = \sup[0, 10[\tag{1.119}$$

Exemple 1.125
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 1.126
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. △

Exemple 1.127
Pour les intervalles, ces notions sont simples : les bornes de l'intervalle sont les supremum et infimum, et ce sont des minima et maxima si l'intervalle est fermé.

(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 1.128
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, $\frac{1}{2}$, $\frac{1}{3}$, ... Le plus grand d'entre eux est 1 parce que tous les nombres de la forme $\frac{1}{n}$ avec $n \geqslant 1$ 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. △

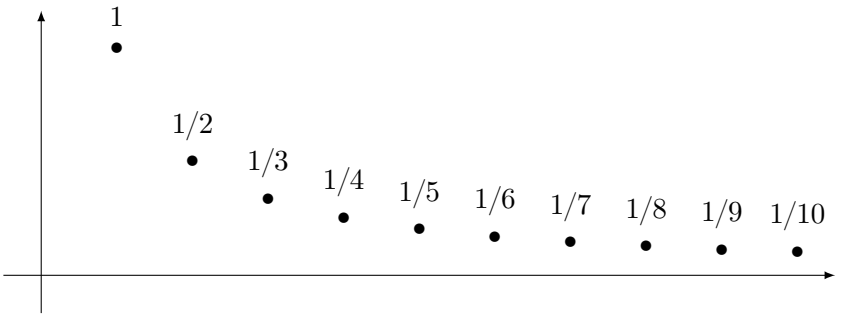


FIGURE 1.1 – Les premiers points du type $x_n = 1/n$.

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 8.11).

Exemple 1.129
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 minium (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. △

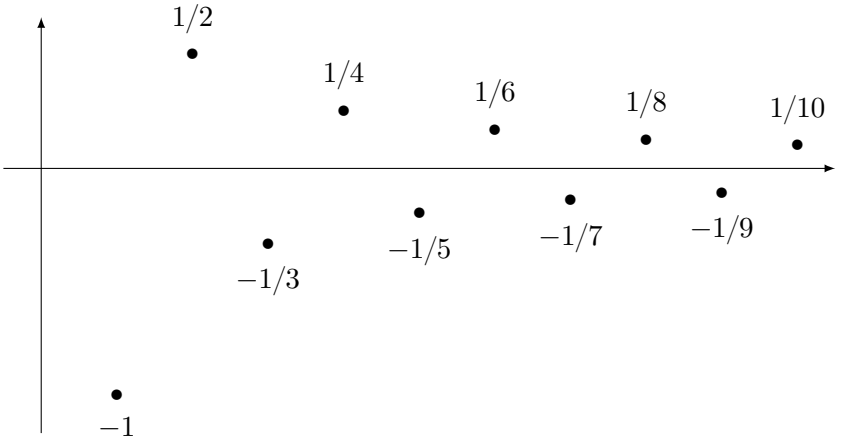


FIGURE 1.2 – Les quelques premiers points du type $(-1)^n/n$.

1.8.6 Racines

Dans cette section, nous définissons $\sqrt{x}$ pour $x \in \mathbb{R}^+$. Vous notez que c'est fait de façon assez algébrique[35], ou en tout cas, en restant proche des définitions. Des définition plus technologiques utilisant la continuité de $x \mapsto x^n$ et qui prouvent que c'est bijectif sur un domaine choisit avec prudence existent, et c'est fait dans la définition 13.311. Il est même expliqué dans [3] que la méthode décrite ici permet de définir $\sqrt[n]{x}$ pour tout n entier, et pas seulement pour $n = 2$.

Proposition 1.130.
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 1.96, 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 1.91 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

$$r = \bar{x}. \tag{1.120}$$

En ce qui concerne r^2, nous avons, par définition du produit dans $\mathbb{R}$,

$$r^2 = \bar{x}^2 = \overline{(x_k^2)}, \tag{1.121}$$

c'est la classe de la suite de Cauchy donnée par les x_k^2. Posons $y_k = x_k$; la relation (1.121) s'écrit

$$r^2 = \bar{y}. \tag{1.122}$$

La proposition 1.91 nous dit également que y est une suite de Cauchy et que

$$y_k \xrightarrow{\mathbb{Q}} q \tag{1.123}$$

La proposition 1.116 donne alors $\bar{y} = \bar{q}$, et finalement

$$r^2 = \bar{q} = \varphi(q). \tag{1.124}$$

Ici tout n'est pas encore terminé avec l'existence parce qu'il faut nous assurer que $r \geqslant 0$. 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 $r_1^2 = r_2^2$. Le lemme 1.103 dit que $\mathbb{R}$ est totalement ordonné ; disons pour fixer les idées que $r1 \leqslant r_2$. Cela signifie, par définition de l'ordre sur $\mathbb{R}$, que $r_2 - r_1 \geqslant 0$. 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 :

$$r_2^2 = (r_1 + s)^2 = r_1^2 + 2r_1 s + s^2. \tag{1.125}$$

Vu que $r_1^2 = q = r_2^2$, nous avons $2r_1 s + s^2 = 0$ ou encore

$$s(2r_1 + s) = 0. \tag{1.126}$$

Vu que $\mathbb{R}$ est un corps, il est un anneau intègre[36] et la règle du produit nul s'applique : soit $s = 0$, soit $2r_2 + s = 0$. Vu que $r_2 > 0$ et que $s \geqslant 0$, nous avons $2r_2 + s > 0$ et donc $s = 0$. Nous en déduisons que $r_1 = r_2$.

□

35. Discutable parce que des limites sont utilisées.
36. Lemme 1.64.

1.9 Les complexes

Problèmes et choses à faire

Encore une fois, cette section n'est pas du tout faite. Le but de cette section serait de

- Construire $\mathbb{C}$ en tant qu'ensemble
- Construire les opérations courantes.
- Démontrer les propriétés de base.

Attention : il est sans espoir de parler de forme trigonométrique ici parce que les exponentielles et fonctions trigonométriques ne sont définies qu'avec les séries.

Nous donnons ici en vrac quelques propriétés et définitions que se doivent d'être présentes dans la version finale de cette section, si elle existe un jour.

Comme partout dans ce chapitre sur la construction des ensembles de nombres, certains propriétés qui ont l'air toute simples peuvent, en fonction des définitions prises, s'avérer pas du tout évidentes.

1.9.1 Définitions

Un nombre complexe s'écrit sous la forme $z = a + bi$, où a et b sont des nombres réels appelés (et notés) respectivement partie réelle ($a = \Re(z)$) et partie imaginaire ($b = \Im(z)$) de z. L'ensemble des nombres de cette forme s'appelle l'ensemble des nombres complexes ; cet ensemble porte une structure de corps et est noté $\mathbb{C}$. Le nombre complexe $i = 0 + 1i$ est un nombre imaginaire qui a la particularité que $i^2 = -1$.

Deux nombres complexes $a+bi$ et $c+di$ sont égaux si et seulement si $a = c$ et $b = d$, c'est-à-dire leurs parties réelles sont égales, et leurs parties imaginaires sont égales.

Pour $z = a + bi$ un nombre complexe, on note $\bar{z} = a - bi$ le *complexe conjugué* de z. Dans le plan de Gauss, il s'agit du symétrique de z par rapport à la droite réelle (généralement dessinée horizontalement).

On définit le module du complexe z par $|z| = \sqrt{z\bar{z}} = \sqrt{a^2 + b^2}$. Dans le plan de Gauss, il s'agit de la distance entre 0 et z.

Proposition 1.131.
Si z_1 et z_2 sont des nombres complexes, alors

$$|z_1 z_2| = |z_1||z_2|. \tag{1.127}$$

Nous avons aussi, pour tout $n \in \mathbb{N}$,

$$|z^n| = |z|^n. \tag{1.128}$$

Démonstration. D'abord $(a + bi)(c + di) = ac - db + (ad + bc)i$, de telle sorte que

$$|(a + bi)(c + di)|^2 = (ac - bd)^2 + (ad + bc)^2. \tag{1.129}$$

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 $|z^n| = |z|^n$. □

Voila. 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.

Proposition 1.132.
Pour tous $z = a + bi$ et z' nombres complexes, on a

(1) $z\bar{z} = a^2 + b^2$;
(2) $\bar{\bar{z}} = z$;
(3) $|z| = |\bar{z}|$;
(4) $|zz'| = |z|\,|z'|$;
(5) $|z + z'| \leqslant |z| + |z'|$.

Lemme 1.133.
Pour tout $z \in \mathbb{C}$ nous avons $z\bar{z} = \bar{z}z = |z|^2$.

Chapitre 2

Théorie des groupes

Pour rapplel, la notion de groupe est définie en 1.33.

2.1 Groupes

Définition 2.1 ([21])**.**
Soit G un groupe. Le ***centralisateur*** *de $H \subset G$ est*

$$\mathcal{Z}_G(H) = \{g \in G \text{ tel que } hg = gh \, \forall h \in H\}; \tag{2.1}$$

il contient donc tous les éléments de G qui commutent avec ceux de H.

Si H est un sous-groupe, son ***normalisateur*** *est*

$$N_G(H) = \{g \in G \text{ tel que } gH = Hg\}. \tag{2.2}$$

Définition 2.2.
Le ***centre*** *d'un groupe G est l'ensemble des éléments de G qui commutent avec tous les autres :*

$$Z_G = \{z \in G \text{ tel que } gz = zg \, \forall g \in G\}. \tag{2.3}$$

Si $g \in G$ nous notons $Z_G(g)$ le ***centralisateur*** *de g dans G :*

$$Z_G(g) = \{h \in G \text{ tel que } hg = gh\}. \tag{2.4}$$

C'est l'ensemble des éléments de G qui commutent avec g.

Définition 2.3.
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 $N \lhd G$.

Définition 2.4.
Un sous-groupe H de G est un sous-groupe ***caractéristique*** *si $\alpha(H) = H$ pour tout $\alpha \in \mathrm{Aut}(G)$.*

Définition 2.5 (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 2.6 (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 $\mathrm{gr}(A)$.*

Lorsque A est fini (disons $A = \{a_1, \ldots, a_n\}$), on note aussi le sous-groupe engendré $\langle a_1, \ldots, a_n \rangle$.

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 2.7.
Tout sous-groupe de G contenant A est inclus dans $\mathrm{gr}(A)$.

Lemme 2.8 ([22])**.**
Si A est une partie du groupe G, alors le sous-groupe $\mathrm{gr}(A)$ *engendré*[1] *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 $\mathrm{gr}(A)$ *peut être écrit sous la forme*

$$\prod_{i=1}^{n} g_i^{a_i} \tag{2.5}$$

où $a_i \in \mathbb{Z}$ et $g\colon \mathbb{N} \to G$ n'est pas spécialement injective : il peut arriver que $g_i = g_j$.

Démonstration. Nous nommons $\mathrm{gr}(A)$ le groupe engendré par A et par H l'ensemble

$$H = \{g_1 \dots g_n \text{ tel que } g_i \in A \cup A^{-1}\}. \tag{2.6}$$

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.

— Le produit de $g_1 \dots g_n$ par $h_1 \dots h_n$ est également dans H[2].

Vu que H est un groupe contenant A, nous avons $\mathrm{gr}(A) \subset H$ parce que $\mathrm{gr}(A)$ est une intersection dont un des éléments est H.

Par ailleurs tout groupe contenant A doit contenir les inverses et les produits finis, donc $H \subset \mathrm{gr}(A)$.

Au final, $H = \mathrm{gr}(A)$, ce qu'il fallait. □

Lemme 2.9.
Soit un groupe G et un sous-groupe $H = \mathrm{gr}(h_1, \dots, h_n)$. Si $\alpha \in G$, alors

$$\alpha H \alpha^{-1} = \mathrm{gr}(\alpha h_1 \alpha^{-1}, \dots, \alpha h_n \alpha^{-1}). \tag{2.7}$$

Démonstration. Il s'agit d'une conséquence du lemme 2.8. Un élément de $\mathrm{gr}(\alpha h_1 \alpha^{-1}, \dots, \alpha h_n \alpha^{-1})$ 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

$$\alpha h_i \alpha^{-1} \alpha h_j \alpha^{-1} = \alpha h_i h_j \alpha^{-1} \in \alpha H \alpha^{-1}. \tag{2.8}$$

Donc

$$\mathrm{gr}(\alpha h_1 \alpha^{-1}, \dots, \alpha h_n \alpha^{-1}) \subset \alpha H \alpha^{-1}. \tag{2.9}$$

L'inclusion dans l'autre sens est du même tonneau. □

Définition 2.10 (Partie génératrice, groupe monogène)**.**
Soit G, un groupe et A une partie de G. Si $\mathrm{gr}(A) = G$, *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 2.11 (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****.*

1. Définition 2.6.
2. Et c'est ici qu'on se rend compte que la décomposition n'est probablement que rarement unique.

Définition 2.12.
Soit le groupe $\big(\mathbb{Z}/10\mathbb{Z},+\big)$. *L'élément* $[2]_{10}$ *n'est pas générateur parce que ses puissances*[3] *sont*

$$\mathrm{gr}([2]_{10}) = \{[2]_{10},[4]_{10},[6]_{10},[8]_{10},[0]_{10}\}. \tag{2.10}$$

Par contré l'élément $[3]_{10}$ *est générateur : ses puissances sont dans l'ordre*

$$[3]_{10},[6]_{10},[9]_{10},[2]_{10},[5]_{10},[8]_{10},[1]_{10},[4]_{10},[7]_{10},[0]_{10}. \tag{2.11}$$

Un exemple presque identique, mais un peu masqué sera l'exemple 19.155.

2.2 Sous-groupe normal

Proposition 2.13.
Soit N *un sous-groupe de* G. *Les propriétés suivantes sont équivalentes :*

(1) $gNg^{-1} \subseteq N$ *pour tout* $g \in G$,
(2) $gNg^{-1} = N$ *pour tout* $g \in G$,
(3) $gN = Ng$ *pour tout* $g \in G$,
(4) N *est une union de classes de conjugaison de* G,
(5) N *est normal*[4].

Définition 2.14.
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 2.15 (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*

$$\min\{n \in \mathbb{N} \text{ tel que } g^n = e\}, \tag{2.12}$$

s'il existe ; dans le cas contraire, nous disons que l'ordre de g *est infini.*

Nous verrons que le corollaire 2.32 au théorème de Lagrange dira que l'ordre d'un élément divise l'ordre du groupe.

Lemme 2.16 ([23])**.**
Si H *et* K *sont normaux dans le groupe* G *et si* $H \cap K = \{e\}$ *alors* $HK \simeq H \times K$.

Définition 2.17.
*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.*

Si l'ordre de tous les éléments acceptent un majorant commun, alors l'exposant du groupe est le plus petit commun multiple des ordres des éléments. En particulier pour un groupe fini, l'exposant est le ppcm des ordres des éléments du groupe.

Le théorème de Burnside 11.262 nous donnera un bon paquet d'exemples de groupes d'exposant fini dans $\mathrm{GL}(n,\mathbb{C})$.

3. 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.
4. Définition 2.3.

Proposition 2.18.
Soit H un sous-groupe normal de G et $\psi: G \to K$ un homomorphisme.

(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

$$\begin{aligned}
[\psi(g_1)][\psi(g_2)] &= \big[\psi(g_1)\psi(g_2)\big] && (2.13a)\\
&= \big[\psi(g_1g_2)\big] && (2.13b)\\
&= \{\psi(g_1g_2)\psi(h) \text{ tel que } h \in H\} && (2.13c)\\
&= \{\psi(g_1g_2h) \text{ tel que } h \in H\} && (2.13d)\\
&= \psi\Big(\{g_1g_2h \text{ tel que } h \in H\}\Big) && (2.13e)\\
&= \psi\big(\overline{g_1g_2}\big) && (2.13f)\\
&= \psi(\overline{g_2g_1}) && (2.13g)\\
&= \text{refaire à l'envers} && (2.13h)\\
&= [\psi(g_2)][\psi(g_1)]. && (2.13i)
\end{aligned}$$

Par conséquent $\psi(G)/\psi(H)$ est abélien. □

2.2.1 Classes de conjugaison

Définition 2.19.
*Soit un groupe G et un élément $g \in G$. La **classe de conjugaison** de g est la partie*

$$C_g = \{kgk^{-1} \text{ tel que } k \in G\}. \tag{2.14}$$

Lemme 2.20.
Un groupe est abélien si et seulement si ses classes de conjugaison sont des singletons.

Démonstration. Supposons que G soit abélien. Alors

$$C_g = \{kgk^{-1} \text{ tel que } k \in G\} = \{g\}. \tag{2.15}$$

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. □

2.3 Groupe dérivé

Définition 2.21.
*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. Le **groupe dérivé** de G est le sous-groupe noté $D(G)$ ou $[G, G]$ engendré par les commutateurs.*

Autrement dit, $D(G)$ est l'intersection de tous les sous-groupes de G contenant tous les commutateurs. Intersection non vide parce que G lui-même en fait partie.

En vertu du lemme 2.8, 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

$$D(G) = \bigcup_{m=1}^{\infty} S_m. \tag{2.16}$$

Lemme 2.22.
Le groupe dérivé est un sous-groupe caractéristique[5]*, et un sous-groupe normal*[6]*.*

Démonstration. Il est évident que si $\alpha \in \mathrm{Aut}(G)$ alors

$$\alpha\big([g,h]\big) = \big[\alpha(g),\alpha(h)\big], \tag{2.17}$$

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,

$$x(ghg^{-1}h^{-1})x^{-1} = (xgx^{-1})(xhx^{-1})(xg^{-1}x^{-1})(xh^{-1}x^{-1}) \tag{2.18a}$$
$$= (xgx^{-1})(xhx^{-1})(xgx^{-1})^{-1}(xhx^{-1})^{-1}. \tag{2.18b}$$

□

Proposition 2.23.
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

$$[g][h] = [gh] = [ghh^{-1}g^{-1}hg] = [hg] = [h][g]. \tag{2.19}$$

□

Le groupe quotient $G/D(G)$ est appelé l'**abélianisé** de G et est parfois noté G^{ab}.

Si $f\colon G \to A$ est un homomorphisme entre le groupe G et un groupe abélien A, alors $f\big(D(G)\big) = \{0\}$. Du coup f passe au quotient de G par $D(G)$, et il existe une unique application $\bar{f}\colon G/D(G) \to A$ telle que $f = \bar{f} \circ \pi$ où $\pi\colon G \to G/D(G)$ est la projection canonique.

2.4 Théorèmes d'isomorphismes

Définition 2.24.
*Soient un groupe G, un ensemble X et une application $f\colon X \to G$. Le **noyau** de f est la partie*

$$\ker(f) = \{x \in X \text{ tel que } f(x) = e\} \tag{2.20}$$

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 $\pi\colon G \to G/N$ est un homomorphisme surjectif de noyau N.

Théorème 2.25 (Premier théorème d'isomorphisme)**.**
Soit $\theta\colon G \to H$ un homomorphisme de groupe. Alors

(1) $\mathrm{Ker}\,\theta$ *est normal dans G,*

(2) $\mathrm{Image}\,\theta$ *est un sous-groupe de H*

(3) nous avons un isomorphisme naturel

$$G/\mathrm{Ker}\,\theta \simeq \mathrm{Image}\,\theta \tag{2.21}$$

Démonstration. Point par point.

(1) Le fait que $\mathrm{Ker}\,\theta$ soit un sous-groupe de G est clair ; montrons qu'il est normal. Si $g \in G$ et $u \in \mathrm{Ker}\,\theta$, alors $\theta(g^{-1}ug) = \theta(g^{-1})\theta(u)\theta(g) = \big(\theta(g)\big)^{-1}\theta(g) = 1_H$, et donc $g^{-1}ug \in \mathrm{Ker}\,\theta$.

5. Définition 2.4.
6. Définition 2.3.

(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 $G/\operatorname{Ker}\theta$, l'isomorphisme est donné par $\varphi[g] = \theta(g)$.

□

Théorème 2.26 (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

$$\frac{HN}{N} \simeq \frac{H}{H \cap N}. \tag{2.22}$$

(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,

$$nhn'h' = n\underbrace{hn'h^{-1}}_{\in N}hh' \in NH. \tag{2.23}$$

Cela prouve que NH est un groupe.
De la même façon, nous prouvons que HN est un groupe par

$$hnh'n' = hh'\underbrace{h'^{-1}nh'}_{\in N}n' \in HN \tag{2.24}$$

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

$$\begin{aligned} j\colon H &\to HN \\ h &\mapsto h \end{aligned} \tag{2.25}$$

et la surjection canonique

$$\sigma\colon HN \to HN/N \tag{2.26}$$

Nous considérons ensuite l'application composée

$$\begin{aligned} f\colon H &\to HN/N \\ h &\mapsto hN. \end{aligned} \tag{2.27}$$

f est surjective L'application f est surjective parce que l'élément $hnN \in HN/N$ est l'image de h, étant donné que $hnN = hN$.

$\operatorname{Ker}(f) = H \cap N$ Si $a \in H \cap N$, nous avons $f(a) = aN = N$, et donc $H \cap N \subset \operatorname{Ker} f$. D'autre part, si $h \in H$ vérifie $h \in \operatorname{Ker} f$, alors $f(h) = hN = N$, ce qui est uniquement possible si $h \in N$.

Le premier théorème d'isomorphisme implique alors que $H/\operatorname{Ker} f \simeq \operatorname{Image} f$, c'est-à-dire

$$H/N \cap H \simeq HN/N. \tag{2.28}$$

□

Théorème 2.27 (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

$$(G/M)/(N/M) \simeq G/N. \tag{2.29}$$

Démonstration. Afin de montrer que N/M est normal dans G/M, nous considérons $g \in G$, $nM \in N/M$ et nous calculons

$$gnMg^{-1} = gng^{-1}\underbrace{gMg^{-1}}_{=M} = \underbrace{gng^{-1}}_{\in N}M \in N/M. \tag{2.30}$$

Pour prouver l'isomorphisme nous considérons le morphisme

$$\begin{aligned} \varphi\colon G/M &\to G/N \\ gM &\mapsto gN. \end{aligned} \tag{2.31}$$

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

$$(G/M)/\operatorname{Ker}\varphi \simeq \operatorname{Image}\varphi, \tag{2.32}$$

c'est-à-dire

$$(G/M)/(N/M) \simeq G/N. \tag{2.33}$$

□

2.5 Indice d'un sous-groupe et ordre des éléments

Lemme 2.28.
Lorsque H est normal dans G, alors la définition

$$[a] \cdot [b] = [ab] \tag{2.34}$$

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 (2.34) est une bonne définition : $[ah] \cdot [bh'] = [ab]$ pour tout $h, h' \in H$. Nous avons :

$$[ah] \cdot [ah'] = [ahah'] = [ahb]. \tag{2.35}$$

Pour montrer que cela est $[ab]$, l'astuce est d'introduire bb^{-1} à côté du a :

$$[ahb] = [abb^{-1}hb] = [ab] \tag{2.36}$$

parce que $b^{-1}hb \in H$ du fait que H soit normal dans G. □

Exemple 2.29([24])
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

$$\begin{aligned} f\colon G &\to G/H \\ g &\mapsto [g] \end{aligned} \tag{2.37}$$

est un morphisme de groupes. △

Définition 2.30.
*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 6.55).

Théorème 2.31 (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

$$|G/H| = \frac{|G|}{|H|}. \tag{2.38}$$

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

$$\begin{aligned} \varphi\colon H &\to gH \\ h &\mapsto gh. \end{aligned} \tag{2.39}$$

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 :

$$|G| = |H| \cdot \text{ nombre de classes.} \tag{2.40}$$

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. □

Corollaire 2.32.
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 $g^n = e$.

Démonstration. Soit G un groupe fini et considérons, à $g \in G$ fixé, le sous-groupe

$$H = \{g^k \text{ tel que } k \in \mathbb{N}\}. \tag{2.41}$$

Par le théorème de Lagrange 2.31, 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. □

D'autres résultats à propos d'ordres et d'indices de groupes finis dans la proposition 3.31 et le lemme 3.33. En particulier le théorème de Cauchy 3.27 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 2.33.
*Une **suite de composition** pour un groupe G est une suite finie de sous-groupes $(G_i)_{i=0,\dots,n}$ telle que*

$$\{e\} = G_n \subseteq G_{n-1} \subseteq \dots \subseteq G_1 \subseteq G_0 = G \tag{2.42}$$

et telle que G_{i+1} est normal[7] *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 2.38).

Lemme 2.34 (du papillon[25])**.**
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

$$\frac{A'(A\cap B)}{A'(A\cap B')} \simeq \frac{(A\cap B)B'}{(A'\cap B)B'} \simeq \frac{B'(A\cap B)}{B'(A'\cap B)}. \tag{2.43}$$

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 $x,y\in A\cap B'$,

$$axby = xx^{-1}axbx^{-1}xy \tag{2.44}$$

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

$$x^{-1}a^{-1} = \underbrace{x^{-1}a^{-1}x}_{\in A'}x^{-1}. \tag{2.45}$$

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

$$\begin{aligned}
(bf)^{-1}(ax)(bf) &= (bf)^{-1}(a\underbrace{xbx^{-1}}_{=c\in A'}xf) && \text{(2.46a)}\\
&= f^{-1}b^{-1}acxf && \text{(2.46b)}\\
&= f^{-1}b^{-1}acf\ \underbrace{f^{-1}xf}_{=y\in A\cap B'} && \text{(2.46c)}\\
&= \underbrace{f^{-1}b^{-1}acf}_{\in A'}y && \text{(2.46d)}\\
&\in A'(A\cap B'). && \text{(2.46e)}
\end{aligned}$$

Pour prouver l'isomorphisme

$$\frac{A'(A\cap B)}{A'(A\cap B')} = \frac{(A\cap B)B'}{(A'\cap B)B'}, \tag{2.47}$$

nous allons utiliser le deuxième théorème d'isomorphisme (2.27(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

$$\frac{A'(A\cap B')(A\cap B)}{A'(A\cap B')} \simeq \frac{A\cap B}{A\cap B\cap A'(A\cap B')}. \tag{2.48}$$

7. Nous rappelons au cas où que « normal » signifie « distingué ».

Pour simplifier un peu cette expression nous prouvons d'abord que

$$(A\cap B)\cap A'(A\cap B')=(A'\cap B)(A\cap B'). \tag{2.49}$$

L'inclusion $\supset$ est facile. Pour l'autre sens, étant donné que $A'(A\cap B')\subset A$ nous avons

$$A\cap B\cap A'(A\cap B)=B\cap A'(A\cap B). \tag{2.50}$$

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

$$(A\cap B)\cap A'(A\cap B')=B\cap A'(A\cap B)\subset(A'\cap B)(A\cap B'), \tag{2.51}$$

et donc l'égalité (2.49). Toujours dans l'idée de simplifier (2.48) 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

$$\frac{A'(A\cap B)}{A'(A\cap B')}=\frac{A\cap B}{(A'\cap B)(A\cap B')}. \tag{2.52}$$

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

$$\frac{B'(A\cap B)}{B'(A'\cap B)}=\frac{A'(A\cap B)}{A'(A\cap B')}. \tag{2.53}$$

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

$$bx=x\underbrace{x^{-1}bx}_{\in B'}\in(A\cap B)B'. \tag{2.54}$$

□

Proposition 2.35.
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 (2.31) s'applique et nous avons à chaque pas de la suite de composition nous avons

$$\left|\frac{G_i}{G_{i+1}}\right|=\frac{|G_i|}{|G_{i+1}|} \tag{2.55}$$

et il suffit d'écrire $|G|$ de façon télescopique :

$$|G|=\prod_{0\leqslant i\leqslant n-1}\frac{|G_i|}{|G_{i+1}|} \tag{2.56}$$

□

Nous disons que les deux suites de composition $(G_i)_{0\leqslant i\leqslant r}$ et $(G_j)_{0\leqslant j\leqslant s}$ sont **équivalentes** si $r=s$ et s'il existe une permutation $\sigma\in S_{r-1}$ telle que

$$\frac{G_i}{G_{i+1}}\simeq\frac{H_{\sigma(i)}}{H_{\sigma(i)+1}}. \tag{2.57}$$

Proposition 2.36 (Schreider)**.**
Deux suites de composition d'un même groupe admettent des raffinements équivalents.

Démonstration. Soient les suites de composition

$$\{e\} = G_m \subseteq \ldots \subseteq G_1 \subseteq G_0 = G \tag{2.58a}$$
$$\{e\} = H_m \subseteq \ldots \subseteq H_1 \subseteq H_0 = G \tag{2.58b}$$

Nous raffinons la suite (G_i) en remplaçant $G_{i+1} \subseteq G_i$ par

$$G_{i+1} = G_{i+1}(G_i \cap H_n) \subset G_{i+1}(G_i \cap H_{n-1}) \subseteq \ldots \subseteq G_{i+1}(G_i \cap H_0) = G_i, \tag{2.59}$$

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 2.34 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

$$\frac{G_{i+1}(G_i \cap H_k)}{G_{i+1}(G_i \cap H_{k+1})} \simeq \frac{H_{k+1}(H_k \cap G_i)}{H_{k+1}(H_k \cap G_{i+1})} \tag{2.60}$$

en vertu du lemme du papillon (2.34). Le membre de droite de (2.60) est un des quotients du raffinement de (H_j). □

Lemme 2.37 (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 2.38 (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 2.37. 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. □

2.7 Groupes résolubles

Définition 2.39.
*Le groupe G est **résoluble** s'il existe une suite finie de sous-groupes G_i*

$$\{e\} = G_n \subset G_{n-1} \subset \ldots \subset G_1 \subset G_0 = G \tag{2.61}$$

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 [8] dont les quotients sont abéliens.

8. Voir définition 2.33.

Lemme 2.40 ([26]).
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 proposition suivantes sont équivalentes :

— Le groupe G/H est abélien

— pour tout $x, y \in G$, $\bar{x}\bar{y} = \bar{y}\bar{x}$

— $\bar{x}\bar{y}\bar{x}^{-1}\bar{y}^{-1} = \bar{e}$

— $\overline{xyx^{-1}y^{-1}} = \bar{e}$

— $[x, y] \in H$

— $D(G) \subset H$.

□

Proposition 2.41 ([26]).
Un groupe est résoluble si et seulement si sa suite dérivée termine sur $\{e\}$.

Démonstration. Grâce au lemme 2.22 et à la proposition 2.23, si la suite dérivée termine sur $\{e\}$ alors la suite dérivé est une suite qui répond aux conditions de la définition 2.39 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

$$\{e\} = G_n \subset G_{n-1} \subset \ldots \subset G_1 \subset G_0 = G \tag{2.62}$$

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 :

$$D^i(G) \subset G_i \tag{2.63}$$

Par le lemme 2.40 nous avons aussi

$$D(G_i) \subset G_{i+1}. \tag{2.64}$$

En dérivant (2.63) et en tenant compte de (2.64), $D^{i+1}(G) \subset D(G_i) \subset G_{i+1}$. 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. □

Proposition 2.42.
Soient des groupes G et H. Nous supposons que G est résoluble et nous considérons un homomorphisme $\psi\colon G \to H$. Alors $\psi(G)$ est résoluble.

Démonstration. Vu que G est résoluble, il existe une suite de sous-groupes G_i tels que

$$\{e\} = G_n \subset G_{n-1} \subset \ldots \subset G_1 \subset G_0 = G \tag{2.65}$$

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 $\psi(G)_n = \psi\big(\{e\}\big) = \{e\}$ ainsi que $\psi(G)_0 = \psi(G)$; donc

$$\{e\} = \psi(G)_n \subset \psi(G)_{n-1} \subset \ldots \subset \psi(G)_1 \subset \psi(G)_0 = \psi(G). \tag{2.66}$$

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 2.18.

□

2.8 Action de groupes

Définition 2.43 (Thème 60)**.**
Une ***action de groupe*** *G sur un ensemble E est la donnée, pour chaque élément $g \in G$, d'une fonction $\phi_g : E \to E$, 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.*

Lemme 2.44.
Pour tout $g \in G$,

(1) L'application $\phi_g \colon E \to E$ 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

$$(\phi_{g^{-1}}\phi_g)(x) = (\phi_{g^{-1}}\phi_g)(y), \tag{2.67}$$

ce qui donne $x = y$ parce que $\phi_{g^{-1}}\phi_g = \phi_{g^{-1}g} = \phi_e = \mathrm{Id}$.
Les dernières trois égalités écrites disent que $\phi_{g^{-1}}$ est l'inverse[9] 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 2.45 (Quelques notions autour de l'action)**.**
Si G agit sur un ensemble E, nous notons $G \cdot x$ l'$\boldsymbol{orbite}$ *de $x \in E$ sous l'action de G :*

$$G \cdot x = \{gx \text{ tel que } g \in G\}.$$

Nous notons G_x ou $\mathrm{Fix}(x)$ le ***stabilisateur*** *de x :*

$$\mathrm{Fix}(x) = G_x = \{g \in G \text{ tel que } g \cdot x = x\}. \tag{2.68}$$

Pour $g \in G$, nous notons enfin $\mathrm{Fix}(g)$ le ***fixateur*** *de g :*

$$\mathrm{Fix}(g) = \{x \in E \text{ tel que } g \cdot x = x\}. \tag{2.69}$$

Définition 2.46.
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 24.93.

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 $g \cdot h = hg^{-1}$.

Définition 2.47.
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 $\mathbf{Ad}(g) \colon G \to G$ 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.

9. Si vous décidez de dire ça a un jury dans un concours, soyez prêts à préciser les domaines.

Nous avons une relation d'équivalence à gauche et une à droite. D'abord

$$x \sim_g y \Leftrightarrow xh = y \tag{2.70}$$

pour un certain $h \in H$. Ensuite

$$x \sim_d y \Leftrightarrow hx = y \tag{2.71}$$

pour un certain $h \in H$.

Le lemme suivant est une généralisation du théorème de Lagrange 2.31.

Lemme 2.48.
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

$$\begin{aligned} f\colon (G/H)_g &\to (G/H)_d \\ [x]_g &\mapsto [x^{-1}]_d \end{aligned} \tag{2.72}$$

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

$$f([x]_g) = f([y]_g). \tag{2.73}$$

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

$$\begin{aligned} f\colon [x]_g &\to [y]_g \\ xh &\mapsto yh. \end{aligned} \tag{2.74}$$

(3) Le nombre d'éléments dans une classe est égal à $|H|$ par la bijection

$$\begin{aligned} g\colon [x]_g &\to H \\ xh &\mapsto h. \end{aligned} \tag{2.75}$$

Par conséquent

$$|G| = |H| \cdot \text{nombre de classes} = |H| \cdot \text{cardinal de } (G/H)_g, \tag{2.76}$$

et nous avons bien

$$\text{cardinal de } (G/H)_g = \frac{|G|}{|H|} = |G : H|. \tag{2.77}$$

□

Proposition 2.49 (Orbite-stabilisateur[27])**.**
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 $\mathrm{Fix}(x)$ est finie si et seulement si $\mathrm{Fix}(x)$ est d'indice fini dans G. Dans ce cas nous avons

$$\mathrm{Card}(G \cdot x) = |G : \mathrm{Fix}(x)|. \tag{2.78}$$

Une autre façon d'écrire la même formule :

$$|G| = |\mathrm{Fix}(x)||\mathcal{O}_x|. \tag{2.79}$$

C'est la formule (2.78) qui est nommée formule des classes sur wikipédia.

Démonstration. (1) Soit l'application

$$\begin{aligned} \psi\colon G\cdot x &\to G/G_x \\ a\cdot x &\mapsto [a]. \end{aligned} \tag{2.80}$$

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 $\mathrm{Fix}(x)$, par conséquent $|A_y|=|\mathrm{Fix}(x)|$ pour tout $y\in\mathcal{O}_x$. Les A_y pour différents y sont disjoints et nous avons de plus

$$\bigcup_{y\in\mathcal{O}_x} A_y = G. \tag{2.81}$$

Les ensemble A_y divisent donc G en $|\mathcal{O}_x|$ paquets de $|\mathrm{Fix}(x)|$ éléments. D'où la formule (2.79).

□

Corollaire 2.50.
Soit C_g la classe de conjugaison d'un élément g du groupe fini G. Alors

$$\mathrm{Card}(C_g) = |G : Z_G(g)| \tag{2.82}$$

où $Z_G(g)$ est le centralisateur de g dans G[10] *de G.*

Démonstration. Cela est une application de la proposition 2.49 (formule (2.78)) 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 :

$$\begin{aligned} \mathrm{Fix}(g) &= \{h\in G \text{ tel que } h\cdot g = g\} && \text{(2.83a)}\\ &= \{h\in G \text{ tel que } hgh^{-1}=g\} && \text{(2.83b)}\\ &= \{h\in G \text{ tel que } gh=hg\} && \text{(2.83c)}\\ &= Z_G(g). && \text{(2.83d)} \end{aligned}$$

Donc la formule $\mathrm{Card}(G\cdot g)=|G:G_g|$ devient, dans le cas de l'action adjointe de G sur lui-même : $\mathrm{Card}(C_g)=|G:Z_G(g)|$. □

Lemme 2.51.
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.

Corollaire 2.52 (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

(1) $E=\bigcup_i \mathcal{O}_i$, l'union est disjointe,

(2) $\mathrm{Card}(E)=\sum_i \mathrm{Card}(\mathcal{O}_i)$.

Définition 2.53.
*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.*

10. Définition 2.2.

Autrement dit, les images des éléments d'un domaine fondamental forment une partition de l'ensemble :

$$E = \bigsqcup_{g\in G} g(F) \tag{2.84}$$

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 $g(F) \cap g'(F) = \varnothing$.

Proposition 2.54 (Équation des classes[28])**.**
Soit G, un groupe fini opérant sur un ensemble E. Si E'' est un ensemble contenant exactement un élément de chaque orbite dans $E\backslash \operatorname{Fix}_G(E)$, alors

$$|G| = |\operatorname{Fix}_G(E)| + \sum_{x\in E''} \frac{|G|}{|\operatorname{Fix}_G(x)|}. \tag{2.85}$$

Si de plus G est un p-groupe, alors

$$|E| = |\operatorname{Fix}_G(E)| \mod p. \tag{2.86}$$

Démonstration. Par le corollaire 2.52, 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,

$$|G| = \operatorname{Card}(\operatorname{Fix}_G(E)) + \sum_{x\in E''} \frac{|G|}{|\operatorname{Fix}_G(x)|} \tag{2.87}$$

où nous avons utilisé le fait que $|G| = |\operatorname{Fix}_G(x)||\mathcal{O}_x|$.

Si G est un p-groupe alors si $x \in E''$, $\operatorname{Fix}_G(x)$ est un sous-groupe propre de G et donc $|\operatorname{Fix}_G(x)|$ est un diviseur propre de $|G|$. Du coup la fraction $|G|/|\operatorname{Fix}_G(x)|$ est une puissance non nulle de p et l'équation (2.85) devient immédiatement (2.86). □

Corollaire 2.55 (Équation des classes)**.**
Soit G, un groupe et $C_1, \dots, C_l$ la liste de ses classes de conjugaison contenant plus de un éléments. Alors

$$\operatorname{Card}(G) = \operatorname{Card}\big(Z(G)\big) + \sum_i |G : Z_{g_i}| = \operatorname{Card}\big(Z(G)\big) + \sum_i \frac{\operatorname{Card}(G)}{\operatorname{Card}\big(\operatorname{Fix}(g_i)\big)} \tag{2.88}$$

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, $\operatorname{Card}(C_{g_i}) = |G : Z_{g_i}|$ par le théorème orbite-stabilisateur (proposition 2.49). □

Théorème 2.56 (Formule de Burnside)**.**
Si G est un groupe fini agissant sur l'ensemble fini E et si Ω est l'ensemble des orbites, alors

$$\operatorname{Card}(\Omega) = \frac{1}{|G|} \sum_{g\in G} \operatorname{Card}\big(\operatorname{Fix}(g)\big). \tag{2.89}$$

Démonstration. Nous considérons l'ensemble

$$A = \{(g, x) \in G \times E \text{ tel que } gx = x\}, \tag{2.90}$$

et nous en calculons le cardinal de deux façons. D'abord

$$\begin{aligned}\mathrm{Card}(A) &= \sum_{x\in E} \mathrm{Card}\{g \in g \text{ tel que } gx = x\} && (2.91a)\\ &= \sum_{x\in E} \mathrm{Card}(\mathrm{Fix}(x)) && (2.91b)\\ &= \sum_{\omega\in\Omega}\sum_{x\in\omega} \mathrm{Card}(\mathrm{Fix}(x)) && (2.91c)\\ &= \sum_{\omega\in\Omega} \frac{|G|}{\mathrm{Card}(\omega)} && (2.91d)\\ &= |G|. && (2.91e)\end{aligned}$$

Pour obtenir (2.91d) nous avons utilisé l'équation des classes (2.79). L'autre façon de calculer $\mathrm{Card}(A)$ est de regrouper ainsi :

$$\mathrm{Card}(A) = \sum_{g\in G} \mathrm{Card}\{x \in E \text{ tel que } gx = x\} = \sum_{g\in G} \mathrm{Card}(\mathrm{Fix}(g)). \tag{2.92}$$

En égalisant les deux expressions de $\mathrm{Card}(A)$ nous trouvons

$$|G|\,\mathrm{Card}(\Omega) = \sum_{g\in G} \mathrm{Card}(\mathrm{Fix}(g)). \tag{2.93}$$

□

Proposition 2.57.
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 2.58.
Soit G un groupe cyclique[11] *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 :

$$H_d = \{x \in G \text{ tel que } x^d = e\} = \{x \in G \text{ tel que } \exists y \in G \text{ tel que } y^{n/d} = x\} = \langle a^{n/d}\rangle. \tag{2.94}$$

Définition 2.59.
*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 Permutations, groupe symétrique

Nous donnons ici quelque éléments à propos du groupe symétrique. Beaucoup de choses supplémentaires sont reportées à la section 5.6. Voir aussi le thème 59.

Définition 2.60.
*Soit un ensemble E. Une **permutation** de l'ensemble E est une bijection $E \to E$. 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 $\{1, \dots, n\} \to \{1, \dots, n\}$.*

11. Définition 2.11.

Définition 2.61.
*Une **transposition** est une permutation qui inverse deux éléments. Plus précisément, une bijection $\sigma: E \to E$ est une transposition si il existe $a, b \in E$ tels que*

$$\sigma(x) = \begin{cases} a & si\ x = b \\ b & si\ x = a \\ x & sinon. \end{cases} \tag{2.95}$$

Lemme 2.62 ([29]).
Le groupe symétrique S_n est un ensemble fini contenant $n!$ éléments.

Lemme 2.63 ([30]).
Deux résultats.

(1) Tout groupe est isomorphe à une 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

$$\begin{aligned} \tau_g: G &\to G \\ x &\mapsto gx. \end{aligned} \tag{2.96}$$

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

$$\begin{aligned} \varphi: G &\to S_G \\ g &\mapsto \tau_g \end{aligned} \tag{2.97}$$

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 $\varphi: G \to \text{Image}(\varphi)$ 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. □

2.9.1 Décomposition en cycles

Définition 2.64.
*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 2.65.
*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*

$$\epsilon(\sigma) = (-1)^{N_\sigma} \tag{2.98}$$

*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

$$(1, \sigma(1), \sigma^2(1), \dots, \sigma^k(1)) \tag{2.99}$$

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 2.66 ([27]).
Soit $\sigma = (i_1, \dots, i_k) \in S_n$, un cycle de longueur k et $\theta \in S_n$. Alors

$$\theta\sigma\theta^{-1} = \big(\theta(i_1), \dots, \theta(i_k)\big). \tag{2.100}$$

Tous les cycles de longueur k sont conjugués entre eux.

Proposition 2.67 (Classes de conjugaison et structure en cycles[31]).
Une classe de conjugaison 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

$$\sigma' = \tau\sigma\tau^{-1} = (\tau c_1 \tau^{-1}) \dots (\tau c_m \tau^{-1}), \tag{2.101}$$

mais $\tau c_i \tau^{-1}$ est un cycle de même longueur que c, puisque le lemme 2.66 nous dit que si $\sigma = (a_1, \dots, a_k)$, alors $\tau c \tau^{-1} = \big(\tau(a_1), \dots, \tau(a_k)\big)$. 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 2.66. Comme les supports des c_i et des c'_i sont disjoints, la permutation $\tau_1 \dots \tau_m$ conjugue σ et σ'. □

Exemple 2.68
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.

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

$$C_1 = \{\mathrm{Id}\} \tag{2.102a}$$
$$C_2 = \{(1,2), (1,3), (2,3)\} \tag{2.102b}$$
$$C_3 = \{(1,2,3), (2,1,3)\}. \tag{2.102c}$$

△

Exemple 2.69
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 2.67). Le groupe symétrique S_4 possède dont 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 2.70.
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 2.71.
Si une permutation peut être écrire sous forme d'un produit d'une nombre pair de permutations, alors toute décomposition en permutations sera en quantité paire.

Une telle permutation est une ***permutation paire****.*

Lemme 2.72 ([23])**.**
Un k-cycle est une permutation impaire si k est pair et paire si k est impair.

Proposition 2.73 ([27])**.**
Soit S_n le groupe symétrique.

(1) L'application $\epsilon\colon S_n \to \{1,-1\}$ 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 $i \leqslant j$ en 4 groupes suivant que $\theta(i) \gtrless \theta(j)$ et $\sigma\big(\theta(i)\big) \gtrless \sigma\big(\theta(j)\big)$. Nous notons N_1, N_2, N_3 et N_4 le nombre de couples dans chacun des quatre groupes :

(i,j)	$\sigma\big(\theta(i)\big) < \sigma\big(\theta(j)\big)$	$\sigma\big(\theta(i)\big) > \sigma\big(\theta(j)\big)$
$\theta(i) < \theta(j)$	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 $\sigma\big(\theta(i)\big)$ et $\sigma\big(\theta(j)\big)$ (parce que θ est une bijection). Donc $N_\sigma = N_2 + N_3$. Par conséquent nous avons

$$\epsilon(\sigma)\epsilon(\theta) = (-1)^{N_2+N_3}(-1)^{N_3+N_4} = (-1)^{N_2+N_4} = (-1)^{N_{\sigma\theta}} = \epsilon(\sigma\theta). \tag{2.103}$$

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 2.66 dit que

$$\tau_{ij} = \theta\tau_{j-1,j}\theta^{-1}. \tag{2.104}$$

La signature étant un homomorphisme,

$$\epsilon(\tau_{ij}) = \epsilon(\theta)\epsilon(\tau_{j-1,j})\epsilon(\theta)^{-1} = \epsilon(\tau_{j-1,j}) = -1. \tag{2.105}$$

Nous passons maintenant à la partie unicité de la proposition. Soit un homomorphisme surjectif $\varphi\colon S_n \to \{-1,1\}$ et τ, une transposition telle que $\varphi(\tau) = -1$ (qui existe parce que sinon φ ne serait

pas surjectif[12]). Si τ' est une autre transposition, il existe $\sigma \in S_n$ tel que $\tau' = \sigma\tau\sigma^{-1}$ (lemme 2.66). Dans ce cas, $\varphi(\tau') = \varphi(\tau) = -1$, et si $\sigma = \tau_1 \dots \tau_k$),

$$\varphi(\sigma) = (-1)^k = \epsilon(\sigma). \tag{2.106}$$

□

Corollaire 2.74.
Si $\sigma \in S_n$, alors

$$\epsilon(\sigma) = \epsilon(\sigma^{-1}). \tag{2.107}$$

Démonstration. Comme dit par la proposition 2.73, ϵ est un homomorphisme, donc

$$\epsilon(\sigma)\epsilon(\sigma^{-1}) = \epsilon(\sigma\sigma^{-1}) = \epsilon(\mathrm{Id}) = 1. \tag{2.108}$$

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. □

2.10 Produit semi-direct de groupes

Définition 2.75.
*Une **suite exacte** est une suite d'applications comme suit :*

$$\dots \xrightarrow{f_i} A_i \xrightarrow{f_{i+1}} A_{i+1} \xrightarrow{f_{i+2}} \dots \tag{2.109}$$

où pour chaque i, les applications f_i et f_{i+1} vérifient $\ker(f_{i+1}) = \mathrm{Image}(f_i)$. Lorsque les ensembles A_i sont des groupes, alors nous demandons de plus que les f_i soient de homomorphismes.

Très souvent nous sommes confrontés à des suites exactes de la forme

$$1 \longrightarrow A \xrightarrow{f} G \xrightarrow{g} B \longrightarrow 1 \tag{2.110}$$

où G, A et B sont des groupes, 1 est l'identité. La première flèche est l'application $\{1\} \to A$ qui à 1 fait correspondre 1. La dernière est l'application $B \to 1$ 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 2.76.
*Soient N et H deux groupes et un morphisme de groupes $\phi\colon H \to \mathrm{Aut}(N)$. 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)*

$$(n, h) \cdot (n', h') = (n\phi_h(n'), hh'). \tag{2.111}$$

Attention à l'ordre quelque peu contre intuitif. Lorsque nous notons $N \times_\phi H$, c'est bien $\phi\colon H \to \mathrm{Aut}(N)$, 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 2.47.

Le théorème suivant permet de reconnaitre un produit semi-direct lorsqu'on en voit un.

Théorème 2.77 ([6])**.**
Soit une suite exacte de groupes

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{s} H \longrightarrow 1 \tag{2.112}$$

S'il existe un sous-groupe $\tilde{H}$ de G à partir duquel s est un isomorphisme, alors

$$G \simeq i(N) \times_\sigma \tilde{H} \tag{2.113}$$

où σ est l'action adjointe[13] de $\tilde{H}$ sur $i(N)$.

12. Nous utilisons ici le fait que tous les éléments de S_n sont des produits de transpositions, proposition 2.70.
13. Le fait que H agisse sur $i(N)$ fait partie du théorème.

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
$$\begin{aligned} \phi\colon G &\to \tilde{N} \times \tilde{H} \\ nh &\mapsto (n, h) \end{aligned} \tag{2.114}$$
est une bijection. C'est une conséquence des points (3) et (4).

(6) Si sur $\tilde{N} \times \tilde{H}$ nous mettons le produit
$$(n, h) \cdot (n', h') = (n\sigma_h n', hh') \tag{2.115}$$
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
$$\begin{aligned} \phi(nhn'h') &= \phi(n \underbrace{hn'h^{-1}}_{\in\tilde{N}} hh') && \text{(2.116a)} \\ &= \phi\big((nhn'h^{-1})(hh')\big) && \text{(2.116b)} \\ &= (nhn'h^{-1}, hh') && \text{(2.116c)} \\ &= (n, h) \cdot (n', h') && \text{(2.116d)} \\ &= \phi(nh)\phi(n'h'). && \text{(2.116e)} \end{aligned}$$

□

Corollaire 2.78.
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 $n \in N$ [14]),

(2) $H \cap N = \{e\}$,

(3) $HN = G$.

Alors l'application
$$\begin{aligned} \psi\colon N \times_\sigma H &\to G \\ (n, h) &\mapsto nh \end{aligned} \tag{2.117}$$
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.

14. Ou encore que H agit sur N par automorphismes internes.

2.11 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 2.79
Le groupe additif $\mathbb{Q}/\mathbb{Z}$ est un groupe de torsion parce que si $[x] = [p/q]$, alors $q[x] = [p] = [0]$.
△

2.12 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 $I = \mathbb{N}$.

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 3.99 où nous parlons d'idéal maximum propre. Comparez par exemple avec [32]. Soyez attentifs.

En cas de doutes, nous suivons les conventions de Wikipédia.

3.1 Inversible et niplolens

Le concept d'anneau est la définition 1.37.

Lemme 3.1.
Si a et b commutent, nous avons, pour tout $r \in \mathbb{N}$ et $r > 0$, la formule

$$a^{r+1} - b^{r+1} = (a-b)\left(\sum_{k=0}^{r} a^{r-k}b^k\right). \tag{3.1}$$

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

$$1 = 1 - a^n = (1-a)(1 + a + \cdots + a^{n-1}) = (1 + a + \cdots + a^{n-1})(1-a). \tag{3.2}$$

La somme $1 + a + \cdots + a^{n-1}$ est donc un inverse de $(1-a)$. □

3.2 PGCD, PPCM et éléments inversibles

La définition de pgcd et ppcm dans un anneau commutatif est la définition 1.46. 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 intègre[1] *A, on a l'équivalence suivante concernant deux éléments $a, b \in A$:*

$$a \mid b \Leftrightarrow (b) \subset (a). \tag{3.3}$$

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 1.42 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 ([33])**.**
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. □

Lemme 3.5 ([33])**.**
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. □

3.3 Le groupe et anneau des entiers

Certes $\mathbb{Z}$ est un groupe pour l'addition, mais c'est également un anneau[2] parce que nous avons les deux opérations d'addition et de multiplication. Nous n'allons pas nous priver de cette belle structure juste parce que le titre du chapitre est « groupes ».

3.3.1 Division euclidienne

Théorème 3.6 (Division euclidienne[34])**.**
Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$, avec $0 \leqslant r < b$, tel que

$$a = bq + r. \tag{3.4}$$

Démonstration. Remarquons que $r = a - bq$, et donc, une fois l'existence et l'unicité de q établie, celle de r suivra.

1. Définition 1.54.
2. Définition 1.37.

Unicité Nous supposons avoir $(q,r) \in \mathbb{Z} \times \mathbb{N}$ tel que $0 \leqslant r < b$ et $a = bq + r$. Alors forcément $r = a - qb$ et $0 \leqslant a - qb < b$, ou encore

$$qb \leqslant a < (1+q)b. \tag{3.5}$$

Ces deux inéquations fixent $q \in \mathbb{Z}$. En effet nous démontrons maintenant que seul $k = 0$ permet à $q + k$ de vérifier ces deux inéquations (parmi les $k \in \mathbb{Z}$). Si $q \geqslant 1$ alors

$$(q+k)b = (q+1)b + (k-1)b > a. \tag{3.6}$$

Et si $k \leqslant -1$ alors

$$(q+k+1)b \leqslant qb \leqslant a. \tag{3.7}$$

D'où l'unicité de q et par conséquent celle de r.

Existence Nous considérons l'ensemble

$$E = \{q \in \mathbb{Z} | bq \leqslant a\}.$$

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 1.48. Ce maximum vérifie

$$bq \leqslant a < b(q+1). \tag{3.8}$$

Cela donne $0 \leqslant a - bq < b$ et le résultat en posant $r = a - qb$.

□

Définition 3.7.
*L'opération $(a,b) \mapsto (q,r)$ donnée par le théorème 3.6 est la **division euclidienne**. Le nombre q est le **quotient** et r est le **reste** de la division de a par b.*

3.3.2 Sous-groupes de $(\mathbb{Z}, +)$

Proposition 3.8.
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 3.6, il existe $q \in \mathbb{Z}$ et $r \in \mathbb{N}$, uniques, tels que $x = nq + r$ et $0 \leqslant r < n$. 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 avions 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 $n = m$.

3.3.3 PGCD, PPCM et Bézout

Vu que $\mathbb{Z}$ est un anneau intègre, nous avons la définition 1.46 de pgcd et de ppcm.

Proposition 3.9 (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 $d \leqslant \delta$ (proposition 1.49). □

Lemme 3.10.
Soient $p, q \in \mathbb{Z}^*$. Les entiers $\operatorname{ppcm}(p,q)$ *et* $\operatorname{pgcd}(p,q)$ *fournissent les isomorphismes de groupes suivants :*

$$p\mathbb{Z} \cap q\mathbb{Z} = \operatorname{ppcm}(p,q)\mathbb{Z} \tag{3.9a}$$
$$p\mathbb{Z} + q\mathbb{Z} = \operatorname{pgcd}(p,q)\mathbb{Z}. \tag{3.9b}$$

Définition 3.11.
Si $\operatorname{pgcd}(p,q) = 1$*, 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.

Définition 3.12.
Un ***nombre premier*** *est un naturel acceptant exactement deux diviseurs distincts.*

Avec cette définition, 0 n'est pas premier, 1 n'est pas premier et 2 est premier.

Théorème 3.13 (Théorème de Bézout [3][35], thème 48)**.**
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

$$au + bv = 1 \tag{3.10}$$

Démonstration. Soit $d = \operatorname{pgcd}(a,b)$ 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 $\operatorname{pgcd}(a,b) = 1$ et nous considérons l'ensemble

$$E = \{au + bv \text{ tel que } u, v \in \mathbb{Z}\} \cap \mathbb{N}^*. \tag{3.11}$$

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

$$m = au_1 + bv_1. \tag{3.12}$$

Par le théorème de division euclidienne [4] (avec a et m), il existe des entiers uniques q et r tels que

$$a = mq + r \tag{3.13}$$

avec $0 \leqslant r < m$. En remplaçant m par sa valeur (3.12), $a = (au_1 + bv_1)q + r$ et

$$r = a(1 - u_1 q) - bv_1 q, \tag{3.14}$$

c'est-à-dire que $r \in \mathbb{Z}a + \mathbb{Z}b$ en même temps que $0 \leqslant r < m$. 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 $m = 1$. □

Corollaire 3.14.
Soient p et q deux entiers premiers entre eux. Alors

$$p\mathbb{Z} + q\mathbb{Z} = \mathbb{Z}; \tag{3.15}$$

en particulier, pour tout $x \in \mathbb{Z}$, il existe u_x, v_x entiers tels que $u_x p + v_x q = x$.

3. Il y a une super application ici : https://perso.univ-rennes1.fr/matthieu.romagny/agreg/dvt/mauvais_prix.pdf.
4. Théorème 3.6.

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.

Démonstration. Soit $x \in \mathbb{Z}$. Le théorème de Bézout nous donne k et l tels que $kp + lq = 1$. Du coup, $(xk)p + (xl)q = x$. □

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 39.42 et ce qui suit.

Proposition 3.15.
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 3.6 de division euclidienne à x et $a + b$: il existe des entiers p_x, r_x, uniques, tels que

$$\begin{cases} x = (p_x - 1)(a + b) + r_x & \text{(3.16a)} \\ 0 \leqslant r_x < a + b. & \text{(3.16b)} \end{cases}$$

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

$$ua + vb = p_x(a + b) - x \tag{3.17}$$

par le corollaire 3.14. Ainsi, x peut s'écrire

$$x = (p_x - u)a + (p_x - v)b. \tag{3.18}$$

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 corollaire 3.14, nous considérons les nombres u_i et v_i définis par

$$u_i a + v_i b = i \tag{3.19}$$

pour $i = 1, \ldots, a + b$. 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

$$x = (p_x - u_k)a + (p_x - v_k)b \tag{3.20}$$

pour un certain k. Cela demande $u_k a + v_k b = ua + vb = p_x(a + b) - x$ par l'équation (3.17). 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

$$x = (p_x - 1)(a + b) + r_x > p^*(a + b), \tag{3.21}$$

ce qui donne

$$(p_x - 1)(a + b) > p^*(a + b) - r_x > (p - 1)(a + b). \tag{3.22}$$

ou encore $p_x > p^*$. Nous avons finalement

$$p_x \geqslant p^* \geqslant u^* \geqslant u_k \tag{3.23}$$

et

$$p_x \geqslant p^* \geqslant v^* \geqslant v_k. \tag{3.24}$$

De ce fait, la décomposition (3.20) est celle que nous voulions.

□

Remarque 3.16.
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 3.17
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

$$1004 = 72 \cdot 7 + 100 \cdot 5. \tag{3.25}$$

Ensuite $4 = 25 - 21 = -3 \cdot 7 + 5 \cdot 5$. Au final,

$$1000 = 75 \cdot 7 + 95 \cdot 5. \tag{3.26}$$

△

3.3.4 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 (20.2).

Cela se base sur le lemme suivant.

Lemme 3.18.
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

$$\frac{a}{s} = \frac{qb}{s} + \frac{r}{s}$$

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. □

Remarque 3.19.
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 :

$$a = q_2 b + r_2 \qquad r_2 < b \tag{3.27a}$$
$$b = q_3 r_2 + r_3 \qquad r_3 < r_2 \tag{3.27b}$$
$$\vdots \tag{3.27c}$$

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 $\text{pgcd}(a, b) = \text{pgcd}(r_{n-1}, r_n) = r_n$.

3.3.4.1 Algorithme d'Euclide pour le PGCD

Écrivons l'algorithme[36] en détail (parce que Bézout, ça va être la même chose en cinq fois plus compliqué). On pose

$$r_0 = a \tag{3.28a}$$
$$r_1 = b \tag{3.28b}$$

(ce qui explique que nous n'ayons pas utilisé r_0 et r_1 précédemment). Ensuite on écrit la division euclidienne $a = q_2 b + r_2$, c'est-à-dire $r_0 = q_2 r_1 + r_2$. Cela donne r_2 et q_2 en termes de r_0 et r_1 :

$$r_2 = r_0 - q_2 r_1. \tag{3.29}$$

Ensuite, sachant r_2 nous pouvons continuer :

$$r_1 = q_3 r_2 + r_3 \tag{3.30}$$

donne q_3 et $r_3 = r_1 - q_3 r_2$. On continue avec $r_2 = q_4 r_3 + r_4$. Tout cela pour poser la suite

$$\begin{aligned} r_0 &= a \\ r_1 &= b \\ r_k &= q_{k+2} r_{k+1} + r_{k+2} \end{aligned} \tag{3.31}$$

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 3.18 et le principe de l'algorithme d'Euclide nous donnent

$$\begin{cases} \operatorname{pgcd}(r_k, r_{k+1}) = \operatorname{pgcd}(r_{k+1}, r_{k+2}) = \operatorname{pgcd}(a, b) & \text{(3.32a)} \\ 0 \leqslant r_{k+1} < r_k. & \text{(3.32b)} \end{cases}$$

La suite étant strictement décroissante, nous prenons r_n, le dernier non nul : $r_{n+1} = 0$. Dans ce cas la dernière équation sera

$$r_{n-1} = q_n r_n \tag{3.33}$$

avec $\operatorname{pgcd}(a, b) = \operatorname{pgcd}(r_n, r_{n-1}) = r_n$.

Exemple 3.20
Calculons le PGCD de 18 et 231. Pour cela nous écrivons les divisions euclidiennes en chaîne :

$$231 = 18 \cdot 12 + 15 \tag{3.34a}$$
$$18 = 1 \cdot 15 + 3 \tag{3.34b}$$
$$15 = 5 \cdot 5 + 0. \tag{3.34c}$$

Donc le PGCD est 3 (le dernier reste non nul). △

3.3.4.2 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 connaitre la liste complète des r_k jusqu'à $r_n = \operatorname{pgcd}(a, b)$, ainsi que la liste complète des divisions euclidiennes

$$r_k = q_{k+2} r_{k+1} + r_{k+2}. \tag{3.35}$$

Nous voulons trouver les couples (u_k, v_k) de telle façon à avoir à chaque étape

$$r_n = u_k r_k + v_k r_{k-1}. \tag{3.36}$$

Notons que c'est à chaque fois r_n que nous construisons. La première équation de type Bézout à résoudre est

$$r_n = u_n r_n + v_n r_{n-1}, \tag{3.37}$$

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 :

$$r_n = u_k r_k + v_k r_{k-1} = u_{k-1} r_{k-1} + v_{k-1} r_{k-2}; \tag{3.38}$$

dans laquelle nous substituons $r_{k-2} = q_k - r_{k-1} + r_k$:

$$\begin{aligned} u_k r_k + v_k r_{k-1} &= u_{k-1} r_{k-1} + v_{k-1}(q_k r_{k-1} + r_k) && (3.39)\\ &= (u_{k-1} + q_k v_{k-1}) r_{k-1} + v_{k-1} r_k && (3.40) \end{aligned}$$

et nous égalons les coefficients de r_k et r_{k-1} pour obtenir

$$\begin{cases} v_{k-1} = u_k & (3.41a)\\ u_{k-1} = v_k - v_{k-1} q_k. & (3.41b) \end{cases}$$

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

$$r_n = u_1 r_1 + v_1 r_0, \tag{3.42}$$

c'est-à-dire

$$\operatorname{pgcd}(a, b) = u_1 b + v_1 a. \tag{3.43}$$

Nous avons ainsi trouvé des coefficients de Bézout pour a et b.

3.3.5 Décomposition en facteurs premiers

Lemme 3.21 (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 $\operatorname{pgcd}(a, c) = 1$ et le théorème de Bézout 3.13 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. □

Lemme 3.22 (Lemme d'Euclide[37])**.**
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 $\operatorname{pgcd}(a, p) = 1$. Dans ce cas le lemme de Gauss 3.21 implique que p divise b. □

Le théorème fondamental de l'arithmétique permet de décomposer des nombres en facteurs premiers.

Théorème 3.23 ([38])**.**
Tout entier strictement positif peut être écrit comme un produit de nombres premiers d'une unique façon, à l'ordre près des facteurs.

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 3.22, 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. □

En d'autres termes, pour tout entier $n > 1$, il existe une 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) $n = \prod_{i=1}^{r} p_i^{k_i}$.

Proposition 3.24.
Soient $a, b \in \mathbb{Z}^*$. Si

$$a = \epsilon \prod_{p \text{ premiers}} p^{\mu(p)} \quad \text{et} \quad b = \epsilon' \prod_{p \text{ premier}} p^{\nu(p)}, \tag{3.44}$$

alors

$$\operatorname{pgcd}(a,b) = \prod p^{\min\{\mu(p),\nu(p)\}} \tag{3.45a}$$
$$\operatorname{ppcm}(a,b) = \prod p^{\max\{\mu(p),\nu(p)\}} \tag{3.45b}$$

Corollaire 3.25 ([1])**.**
Un élément $m \in \mathbb{Z}^*$ vérifie $m \leqslant p^n$ et $\operatorname{pgcd}(m, p^n) \neq 1$ si et seulement si $m = qp$ pour un certain $q \leqslant p^{n-1}$.

Problèmes et choses à faire

Il faut vérifier si le corollaire 3.25 est correct. Et puis rédiger des démonstrations de tout ce petit monde.

Lemme 3.26.
Un entier $n \geqslant 1$ 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 $n \geqslant 2$.

En ce qui concerne l'existence, nous décomposons n en facteurs premiers [5] et nous séparons les puissances paires des puissances impaires :

$$n = \prod_{i=1}^{r} p_p^{2\alpha_i} \prod_{j=1}^{s} q_j^{2\beta_j+1} \tag{3.46a}$$
$$= \underbrace{\left(\prod_{i=1}^{r} p_i^{2\alpha_i} \prod_{j=1}^{s} q^{2\beta_j} \right)}_{m^2} \underbrace{\prod_{j=1}^{s} q_j}_{q}. \tag{3.46b}$$

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 $d = \operatorname{pgcd}(m_1, m_2)$ et k_1, k_2 définis par $m_1 =$

5. Théorème 3.23.

dk_1, $m_2 = dk_2$. Par construction, $\text{pgcd}(k_1, k_2) = 1$. Étant donné que

$$n = q_1 d^2 k_1^2 = q_2 d^2 k_2^2, \tag{3.47}$$

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 (3.47) se réduit à $n = q_1 m_1^2 = q_2 l^2 m_1^2$ et donc

$$q_1 = q_2 l^2, \tag{3.48}$$

ce qui signifie $l = 1$ et donc $m_1 = m_2$. □

Dans $\mathbb{N}$, il y a assez bien de nombres premiers. Nous allons voir maintenant que la somme des inverses des nombres premiers diverge. Pour comparaison, la somme des inverses des carrés converge. Il y a donc plus de nombres premiers que de carrés.

3.3.6 Ordre d'un élément dans un groupe fini

Théorème 3.27 (Théorème de Cauchy[39])**.**
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.

Le lemme suivant indique que sous hypothèse de commutativité, l'ordre d'un élément est une notion multiplicative.

Lemme 3.28 ([40])**.**
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 $r_1 s_1$ avec $r_1 \mid r$ et $s_1 \mid s$. Nous avons

$$a^{r_1 s_1} b^{r_1 s_1} = (ab)^{r_1 s_1} = 1, \tag{3.49}$$

que nous élevons à la puissance r_2 où r_2 est définit en posant $r = r_1 r_2$:

$$a^{r s_1} b^{r s_1} = 1. \tag{3.50}$$

Et comme $a^{r s_1} = 1$, nous concluons que $b^{r s_1} = 1$. Donc $s \mid r s_1$. Par le lemme de Gauss 3.21, 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 $r_1 s_1 = rs$. □

Lemme 3.29 ([27])**.**
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 2.31) 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 2.13. □

Lemme 3.30 ([41])**.**
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 $a^m \in H$. □

Proposition 3.31 ([41])**.**
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 3.30. Étant donné que m et n sont premiers entre eux, par le théorème de Bézout 3.13, il existe $a, b \in \mathbb{Z}$ tels que

$$am + bn = 1. \tag{3.51}$$

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 $|H'| = |H| = |G|/m$. □

3.32.
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 3.33.
L'ensemble des ordres[6] *d'un groupe commutatif est stable par PPCM*[7].

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 $\text{ppcm}(r, s)$.

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 :

$$r = \prod_{i=1}^{k} p_i^{\alpha_i} \tag{3.52a}$$

$$s = \prod_{i=1}^{k} p_i^{\beta_i} \tag{3.52b}$$

où $\{p_i\}_{i=1\ldots k}$ est l'ensemble des nombres premiers arrivant dans les décompositions de r et de s. Si nous posons

$$r' = \prod_{\substack{i=1 \\ \alpha_1 > \beta_i}}^{k} p_i^{\alpha_i} \tag{3.53a}$$

$$s' = \prod_{\substack{i=1 \\ \alpha_i \leqslant \beta_i}}^{k} p_i^{\beta_i}, \tag{3.53b}$$

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 3.28 pour conclure que l'ordre de $x^{r/r'}y^{s/s'}$ est $r's' = m$. □

3.3.7 Écriture des fractions

Théorème 3.34.
Tout élément de $\mathbb{Q}^+$ s'écrit de façon unique comme quotient de deux entiers premiers entre eux.

Démonstration. En deux parties[8]

Unicité Supposons avoir $\frac{a}{b} = \frac{c}{d}$ avec $\text{pgcd}(a, b) = \text{pgcd}(c, d) = 1$. Nous avons

$$ad = bc \tag{3.54}$$

donc

(1) a divise bc mais est premier avec b donc a divise c par le lemme de Gauss 3.21.

6. Définition 2.15.
7. Définition 1.46.
8. Définitions des pgcd et ppcm en 1.46.

(2) c divise ad mais est premier avec d donc c divise a par le lemme de Gauss 3.21.

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

$$\frac{a}{b} = \frac{a/\operatorname{pgcd}(a,b)}{b/\operatorname{pgcd}(a,b)}, \tag{3.55}$$

qui est encore un quotient d'entiers parce que $\operatorname{pgcd}(a,b)$ divise aussi bien a que b. Il faut montrer que les nombres $a/\operatorname{pgcd}(a,b)$ et $b/\operatorname{pgcd}(a,b)$ sont premiers entre eux. Pour cela nous supposons que k est un diviseur commun. En particulier, les nombres $a/k\operatorname{pgcd}(a,b)$ et $b/k\operatorname{pgcd}(a,b)$ sont des entiers, ce qui fait que $k\operatorname{pgcd}(a,b)$ est un diviseur commun de a et b. Étant donné que $\operatorname{pgcd}(a,b)$ est le plus grand tel diviseur, nous devons avoir $k\operatorname{pgcd}(a,b) = \operatorname{pgcd}(a,b)$ c'est-à-dire que $k = 1$. Donc les nombres $a/\operatorname{pgcd}(a,b)$ et $b/\operatorname{pgcd}(a,b)$ sont premiers entre eux.

□

Proposition 3.35.
Les entiers p et q sont premiers entre eux si et seulement si p^2 et q^2 sont premiers entre eux.

Démonstration. Si p^2 et q^2 sont premiers entre eux, par le théorème de Bézout 3.13 il existe $a, b \in \mathbb{Z}$ tels que

$$ap^2 + bq^2 = 1 \tag{3.56}$$

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 $\operatorname{pgcd}(p,q) = k \neq 1$. 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. □

Une des conséquences de ces résultats sera le fait que $\sqrt{n}$ est irrationnelle dès que n n'est pas un carré parfait, théorème 3.36.

Nous avons déjà vu dans la proposition 1.87 que $\sqrt{2}$ était irrationnel. En fait le théorème suivant va nous montrer que le nombre $\sqrt{n}$ est soit entier, soit irrationnel.

Théorème 3.36.
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 3.34 nous donne $p, q \in \mathbb{N}$ premiers entre eux tels que $\sqrt{n} = p/q$. La proposition 3.35 nous enseigne de plus que p^2 et q^2 sont premiers entre eux. Nous avons

$$p^2 = nq^2. \tag{3.57}$$

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. □

3.3.8 Équation diophantienne linéaire à deux inconnues

Soient a, b et c des entiers naturels donnés. Nous considérons l'équation

$$ax + by = c \tag{3.58}$$

à résoudre[42] 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 $d = \operatorname{pgcd}(a,b)$ et notons $a = da'$, $b = db'$. Nous avons déjà l'équation

$$d(a'x + b'y) = c, \tag{3.59}$$

et donc si c n'est pas un multiple de d, il n'y a pas de solutions[9]. Si par contre c est un multiple de d alors nous écrivons $c = c'd$ et l'équation devient

$$a'x + b'y = c' \tag{3.60}$$

C'est maintenant que nous utilisons le théorème de Bézout 3.13 : vu que a' et b' sont premiers entre eux, nous avons la relation $a'u + b'v = 1$ pour certains[10] 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 :

$$a'(x - c'u) = b'(c'v - y). \tag{3.61}$$

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 forcément[11] diviser $c'v - y$. Disons $c'v - y = ka'$. Alors $a'(x - c'u) = b'ka'$ et donc

$$x = b'k + c'u. \tag{3.62}$$

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

$$\begin{cases} x = b'k + c'u & \text{(3.63a)} \\ y = vc' - a'k & \text{(3.63b)} \end{cases}$$

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 (3.63) sont solutions.

Exemple 3.37
Résoudre l'équation $2x + 6y = 52$.

Nous pouvons factoriser 2 dans le membre de gauche et simplifier alors toute l'équation par 2 :

$$x + 3y = 26. \tag{3.64}$$

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

$$x + 3y = 26 \times (-5 + 3 \times 2), \tag{3.65}$$

et donc $x + 5 \times 26 = 3(y - 26 \times 6)$, et en posant $k = y - 26 \times 6$ nous avons

$$x = 3k - 130. \tag{3.66}$$

En injectant nous trouvons l'équation $3k - 130 + 3y = 26$ et donc

$$y = 52 - k. \tag{3.67}$$

△

3.3.9 Quotients

Nous écrivons $a = b \mod p$ essentiellement s'il existe $k \in \mathbb{Z}$ tel que $b + kp = a$. Plus généralement nous notons $[a]_p = \{a + kp | k \in \mathbb{Z}\}$ et l'écriture « $a = n \mod p$ » peut tout autant signifier $a = [b]_p$ que $a \in [b]_p$. La différence entre les deux est subtile mais peut de temps en temps valoir son pesant d'or.

9. Exemple : $8x+2y = 9$. Le membre de gauche est certainement un nombre pair et il n'y a donc pas de solutions.
10. Nous avons décrit un algorithme pour les trouver en démontrant l'équation 3.43.
11. C'est Gauss 3.21 qui le dit, et vous savez que lorsque Gauss dit, c'est *forcément* vrai.

Proposition 3.38.
Soit $n \in \mathbb{N}$. Le groupe $\mathbb{Z}/n\mathbb{Z}$ est monogène. Si $n \neq 0$, le groupe $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre n.

Démonstration. Nous considérons la surjection canonique $\mu\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Si $a \in \mathbb{Z}$, alors $\mu(a) = a\mu(1)$. Par conséquent $\mathbb{Z}/n\mathbb{Z} = \text{gr}\big(\mu(1)\big)$ 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 3.6 donne l'existence de q et r avec $0 \leqslant r < n$ et $q \geqslant 0$ tels que

$$x_0 = nq + r. \tag{3.68}$$

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

$$\mathbb{Z}/n\mathbb{Z} = \mu(\mathbb{Z}) = \mu(\mathbb{N}_{n-1}). \tag{3.69}$$

La restriction $\mu\colon \mathbb{N}_{n-1} \to \mathbb{Z}/n\mathbb{Z}$ 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 3.39 ([43]).
Soit $q \in \mathbb{N}$ avec $q \geqslant 2$. 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 3.6, il existe $a, b \in \mathbb{Z}$ tels que $n = ad + b$ avec $0 \leqslant b < d$. En remarquant que $q^d \in [1]_{q^d-1}$ nous avons

$$q^n = (q^d)^a q^b \in [1]_{q^d-1} q^b = [q^b]_{q^d-1}. \tag{3.70}$$

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

$$q^n \in [1]_{q^d-1}. \tag{3.71}$$

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

$$[1]_{q^d-1} = [q^b]_{q^d-1}, \tag{3.72}$$

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 $q \geqslant 2$, 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. □

3.4 Binôme de Newton et morphisme de Frobenius

Proposition 3.40 ([44]).
Pour tout $x, y \in \mathbb{R}$ et $n \in \mathbb{N}$, nous avons

$$(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k \tag{3.73}$$

où

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \tag{3.74}$$

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 (3.73) soit vraie pour $n \geqslant 1$, et prouvons la pour $n + 1$. Nous avons

$$\begin{aligned}(x+y)^{n+1} &= (x+y)\cdot\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k \\ &= \sum_{k=0}^{n}\binom{n}{k}x^{n-k+1}y^k + \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^{k+1} \\ &= x^{n+1} + \sum_{k=1}^{n}\binom{n}{k}x^{n-k+1}y^k + \sum_{k=0}^{n-1}\binom{n}{k}x^{n-k}y^{k+1} + y^{n+1}.\end{aligned} \tag{3.75}$$

La seconde grande somme peut être transformée en posant $i = k + 1$:

$$\sum_{k=0}^{n-1}\binom{n}{k}x^{n-k}y^{k+1} = \sum_{i=1}^{n}\binom{n}{i-1}x^{n-(i-1)}y^{i-1+1}, \tag{3.76}$$

dans lequel nous pouvons immédiatement renommer i par k. En remplaçant dans la dernière expression de (3.75), nous trouvons

$$(x+y)^{n+1} = x^{n+1} + y^{n+1} + \sum_{k=1}^{n}\left[\binom{n}{k} + \binom{n}{k-1}\right]x^{n-k+1}y^k. \tag{3.77}$$

La thèse découle maintenant de la formule

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k} \tag{3.78}$$

qui est vraie parce que

$$\frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)(n-k+1)!} = \frac{n!(n-k+1)+n!k}{k!(n-k+1)!} = \frac{n!(n+1)}{k!(n-k+1)!}, \tag{3.79}$$

par simple mise au même dénominateur. □

3.5 Idéal dans un anneau

La définition d'un idéal dans un anneau est la définition 1.44.

Définition 3.41 (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 3.42.
*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 3.43.
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 3.44
L'ensemble $2\mathbb{Z}$ est un idéal de $\mathbb{Z}$. On peut aussi le noter (2). △

Proposition-définition 3.45.
Soit A, un anneau, I un idéal bilatère[12] *de A. Nous considérons la relation d'équivalence $x \sim y$ si et seulement si $x - y \in I$. Sur le quotient*

$$A/\sim = A/I, \tag{3.80}$$

nous mettons les opérations

(1) $\bar{x} + \bar{y} = \overline{x + y}$;

(2) $\bar{x}\bar{y} = \overline{xy}$.

Nous avons alors les résultats suivants :

(1) Les opérations sont bien définies,

(2) l'ensemble A/I est un anneau

(3) la surjection canonique $A \to A/I$ est un morphisme.

Cet anneau est appelé ***anneau quotient****.*

Démonstration. Nous montrons que le produit est bien défini[13]. Nous savons que, par définition,

$$\bar{x} = \{x + i \text{ tel que } i \in I\}. \tag{3.81}$$

Calculons le produit de représentants génériques de $\bar{x}$ et de $\bar{y}$:

$$(x + i_1)(y + i_2) = xy + xi_2 + yi_1 + i_1i_2. \tag{3.82}$$

Vu que I est un idéal nous avons $xi_2 + yi_1 + i_1i_2 \in I$ et donc bien

$$(x + i_1)(y + i_2) \in \overline{xy}. \tag{3.83}$$

□

Proposition 3.46 (Premier théorème d'isomorphisme pour les anneaux)**.**
Soient A et B des anneaux et un homomorphisme $f\colon A \to B$. Nous considérons l'injection canonique $j\colon f(A) \to B$ et la surjection canonique $\phi\colon A \to A/\ker f$. Alors il existe un unique isomorphisme

$$\tilde{f}\colon A/\ker f \to f(A) \tag{3.84}$$

tel que $f = j \circ \tilde{f} \circ \phi$.

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle j} \\ A/\ker f & \xrightarrow[\tilde{f}]{} & f(A) \subset B \end{array} \tag{3.85}$$

Proposition 3.47.
Soient I un idéal de A et la projection canonique

$$\phi\colon A \to A/I. \tag{3.86}$$

Elle est une bijection entre les idéaux de A contenant I et les idéaux de A/I.

Dit de façon imagée :

$$\{\text{idéaux de } A \text{ contenant } I\} \simeq \{\text{idéaux de } A/I\}. \tag{3.87}$$

12. Définition 1.44.
13. Si vous le voulez, n'hésitez pas à m'envoyer un patch pour le reste de la démonstration.

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

$$\phi(i)\phi(j) = \phi(ij) \in \phi(J). \tag{3.88}$$

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 $I \subset \phi^{-1}(K)$. □

Proposition 3.48 ([1])**.**
Si A est un anneau, nous avons les équivalences

(1) A est un corps[14]*.*

(2) A est non nul et ses seuls[15] *seuls 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 $I = A$.

(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 44)**.**
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. □

3.5.1 Résultats supplémentaires sur l'anneau des entiers

Corollaire 3.51.
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 3.8, 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 3.52.
Soient $n \geqslant 2$ un entier et $\phi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ la surjection canonique. Nous noterons $\tilde{a} = \phi(a)$. Alors l'ensemble des inversibles de $\mathbb{Z}/n\mathbb{Z}$ est donné par

$$U(\mathbb{Z}/n\mathbb{Z}) = \phi(P_n) = \{\tilde{x} \text{ tel que } 0 \leqslant x \leqslant n \text{ tel que } \operatorname{pgcd}(x,n) = 1\}. \tag{3.89}$$

où P_n est l'ensemble $P_n = \{x \in \{0,\dots,n-1\} \text{ tel que } \operatorname{pgcd}(x,n) = 1\}$.

14. Définition 1.61.
15. Je vous laisse vous poser de grandes questions sur le fait que le vide est un idéal ou non.

De plus,

$$\text{Card}\left(U(\mathbb{Z}/n\mathbb{Z})\right) = \varphi(n). \tag{3.90}$$

Démonstration. Soit $0 \leqslant x \leqslant n$ tel que $\text{pgcd}(x,n) = 1$. Il existe donc [16] $u, v \in \mathbb{Z}$ tels que $ux + vn = 1$. En passant aux classes,

$$\tilde{u}\tilde{x} = \tilde{1}, \tag{3.91}$$

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 prouve [17] que $\text{pgcd}(x,n) = 1$. □

3.6 Caractéristique

Lemme-définition 3.53.
Soit l'application

$$\begin{aligned} \mu\colon \mathbb{Z} &\to A \\ n &\mapsto n \cdot 1_A. \end{aligned} \tag{3.92}$$

(1) C'est un morphisme d'anneaux.

(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 11.171.

Lemme 3.54.
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. □

Lemme 3.55.
Si p est la caractéristique de l'anneau A, alors nous avons l'isomorphisme d'anneaux

$$\mathbb{Z}1_A \simeq \mathbb{Z}/p\mathbb{Z}. \tag{3.93}$$

Démonstration. L'isomorphisme est donné par l'application $n1_A \mapsto \phi(n)$ si ϕ est la projection canonique $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$. □

Proposition 3.56.
La caractéristique d'un anneau fini divise son cardinal.

Démonstration. Si A est un anneau, le groupe $\mathbb{Z}$ agit sur A par

$$n \cdot a = a + n1_A. \tag{3.94}$$

Chaque orbite de cette action est de la forme

$$\mathcal{O}_a = \{a + n1_A \text{ tel que } n = 0, \ldots, p-1\} \tag{3.95}$$

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. □

Lemme 3.57 ([45])**.**
Un anneau totalement ordonné est de caractéristique nulle.

16. Théorème de Bézout 3.13
17. À nouveau avec le Théorème de Bézout.

Démonstration. Le morphisme $\mu\colon \mathbb{Z} \to A$, $n \mapsto n1_A$ est strictement croissant, en particulier $\mu(x) \neq \mu(y)$ dès que $x \neq y$. Donc $\ker(\mu) = \{0\}$. □

L'ensemble typique de caractéristique p est $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Proposition 3.58.
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

$$(a+b)^p = a^p + b^p \tag{3.96}$$

pour tout $a, b \in A$.

Démonstration. Nous utilisons la formule du binôme de la proposition 3.40 et le fait que les coefficients binomiaux non extrêmes sont divisibles par p et donc nuls. □

Proposition 3.59.
Soit A un anneau commutatif unitaire de caractéristique p. L'application

$$\begin{aligned} \mathrm{Frob}_A\colon A &\to A \\ x &\mapsto x^p \end{aligned} \tag{3.97}$$

est un automorphisme d'anneau unitaire.

Nous le nommons le **morphisme de Frobenius**. Nous utiliserons aussi les itérés du morphisme de Frobenius : $\mathrm{Frob}^k\colon x \mapsto x^{p^k}$.

Exemple 3.60
Soit à factoriser $X^p - 1$ dans $\mathbb{F}_p$. Grâce au morphisme de Frobenius, nous avons immédiatement

$$X^p - 1 = (X-1)^p. \tag{3.98}$$

△

3.7 Module sur un anneau

Définition 3.61 (module sur un anneau[46])**.**
*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 $+\colon M \times M \to M$,

(2) $\cdot$ est une loi de composition externe, c'est-à-dire $\cdot : A \times M \to M$

telles que

(1) $(M, +)$ est un groupe[18]*.*

(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 3.62.
Si M est un module sur un anneau, alors $(M, +)$ est un groupe commutatif.

18. Nous verrons dans la proposition 3.62 qu'il est forcément commutatif.

Démonstration. Il suffit de calculer $(1+1)\cdot(x+y)$ de deux façons différentes :

$$(1+1)\cdot(x+y) = 1\cdot(x+y) + 1\cdot(x+y) = x+y+x+y \tag{3.99}$$

d'une part et

$$(1+1)\cdot(x+y) = (1+1)\cdot x + (1+1)\cdot y = x+x+y+y, \tag{3.100}$$

d'autre part. En égalant les deux expressions, il vient

$$x+y+x+y = x+x+y+y, \tag{3.101}$$

qui se simplifie (nous sommes dans un groupe) en $y+x = x+y$. □

Définition 3.63.
*Un **espace vectoriel** est un module sur un corps commutatif*[19].

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

$$\begin{aligned} \mu_x\colon A^{(I)} &\to M \\ (a_i)_{i\in I} &\mapsto \sum_{i\in I} a_i x_i. \end{aligned} \tag{3.102}$$

Ici $A^{(I)}$ désigne l'ensemble de toutes les applications $I \to A$ de support fini.

Définition 3.64.
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 3.65.
*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 3.66
Un anneau A est lui-même un A-module et ses sous-modules sont les idéaux. △

Définition 3.67.
*Soit M un module sur un anneau commutatif A. Un **projecteur** est une application linéaire $p\colon M \to M$ 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 $\sum_{i\in I} p_i = \mathbb{1}$.*

Théorème 3.68.
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

$$p_i(x_1 + \dots + x_n) = x_i \tag{3.103}$$

forment une famille orthogonale de projecteurs et $p_1 + \dots + p_n = \mathrm{Id}$.

Inversement, si $(p_1, \dots, p_n)$ est une famille orthogonale de projecteurs dans un module $\mathcal{E}$ tel que $\sum_{i=1}^n p_i = \mathrm{Id}$, alors

$$M = \bigoplus_{i=1}^{n} p_i(M). \tag{3.104}$$

19. La condition de commutativité n'est pas indispensable, mais comme nous ne parlerons que de corps commutatifs …

Définition 3.69.
Un module est ***simple*** *ou* ***irréductible*** *s'il n'a pas d'autre 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 3.70
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 $\mathcal{E}$. △

Définition 3.71 (Algèbre[47])**.**
Si $\mathbb{K}$ *est un corps commutatif*[20]*, une* $\mathbb{K}$***-algèbre*** A *est un espace vectoriel*[21] *muni d'une opération bilinéaire* $\times : A \times A \to A$*, 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* $f : A \to B$ *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 3.72 ([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, et donc dans X. □

Définition 3.73.
*L'****algèbre engendrée*** *par* X *est l'intersection de toutes les sous-algèbres de* A *contenant* X *(qui est une algèbre par le lemme 3.72).*

3.8 Anneau intègre

La définition d'un anneau intègre est la définition 1.54.

Exemple 3.74
Un corps[22] est toujours un anneau intègre. 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. △

Exemple 3.75
L'ensemble $\mathbb{Z}$ avec les opérations usuelles est un anneau intègre. △

20. Définition 1.61
21. Définition 3.63.
22. Définition 1.61.

Exemple 3.76
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. △

Nous verrons au théorème 3.157 que l'anneau A est intègre si et seulement si $A[X]$ est intègre.

Corollaire 3.77.
L'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier.

Démonstration. Supposons que n soit premier. La proposition 3.52 donne les inversibles de $\mathbb{Z}/n\mathbb{Z}$ par

$$U(\mathbb{Z}/n\mathbb{Z}) = \{\tilde{x} \text{ tel que } 0 \leqslant x \leqslant n \text{ tel que } \operatorname{pgcd}(x,n) = 1\}. \tag{3.105}$$

Mais comme n est premier, $\operatorname{pgcd}(x,n) = 1$ 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 $1 < p \leqslant q < n$. Alors

$$[p]_n[q]_n = [pq]_n = [0]_n. \tag{3.106}$$

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. □

3.8.1 Caractéristique d'un anneau intègre

Lemme 3.78.
La caractéristique[23] *d'un anneau intègre est zéro ou un nombre premier.*

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 3.77 dit que $\mathbb{Z}/p\mathbb{Z}$ est intègre si et seulement si p est premier, ce qui conclut la preuve. □

Exemple 3.79
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 :

$$\begin{pmatrix} 1 & \\ & 1 \end{pmatrix} + \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} + \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} = 0. \tag{3.107}$$

△

Exemple 3.80
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 11.44. △

3.8.2 Divisibilité et classes d'association

Lemme 3.81.
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 $a = ub$.

23. Définition 3.53.

Démonstration. Les hypothèses à propos de la divisibilité nous indiquent que $a = xb$ et $b = ya$ pour certains $x, y \in A$. Du coup,

$$b(1 - yx) = 0. \tag{3.108}$$

Étant donné que $\mathbb{A}$ 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. □

Définition 3.82.
*On dit de deux éléments $a, b \in A$ qu'ils sont **associés** si ils vérifient les hypothèses du lemme 3.81 ; 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 3.83
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 :

$$(2 + i)(4 + i) = 7 + 6i. \tag{3.109}$$

△

Problèmes et choses à faire
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 $1/2^n$?

3.8.3 PGCD et PPCM

«««< Updated upstream Pour le théorème de Bézout et autres opérations avec des modulo, voir le thème 48. Le pgcd et le ppcm sont définis en 1.46.

Lemme 3.84.
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 $u \in \mathbb{A}$ 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 3.81), il existe un inversible u tel que $\delta = u\delta'$.

Le même type de raisonnement tient pour le PPCM. □

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 3.85.
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.

3.8.4 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 3.86.
Un anneau fini intègre est un corps.

Démonstration. Soit A un tel anneau. Soit $a \neq 0$. Les applications

$$l_a : x \to ax \tag{3.110a}$$
$$r_a : x \to xa \tag{3.110b}$$

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 [24]

$$b = b(ac) = (ba)c = c. \tag{3.111}$$

Par conséquent b est un inverse de a. □

Proposition 3.87.
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 corollaire 3.77. Le fait que $\mathbb{Z}/n\mathbb{Z}$ soit un corps lorsque $\mathbb{Z}/n\mathbb{Z}$ est intègre est la proposition 3.86. 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 1.64). □

3.8.5 Élément irréductible

Définition 3.88 (Élément irréductible[48])**.**
*Un élément d'un anneau commutatif est **irréductible** si il n'est ni inversible, ni le produit de deux éléments non inversibles.*

3.89.
Nous allons voir dans la section 3.11 que le concept d'élément irréductible n'est vraiment utile que dans le cas des anneaux intègres.

Exemple 3.90
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 : $0 = 0 \cdot 0$. △

Exemple 3.91
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 $b = \pm 1$. △

24. 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.

3.9 Anneau factoriel

Définition 3.92 (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 permutation[25] $\sigma \in S_k$ telle que p_i et $q_{\sigma(i)}$ soient associés[26].

Un anneau factoriel permet de caractériser le pgcd et le ppcm de nombres.

Proposition 3.93.
Soit une famille $\{a_n\}$ d'éléments de A qui se décomposent en irréductibles comme

$$a_i = \prod_k p_k^{\alpha_{k,i}}. \tag{3.112}$$

Alors

$$\text{pgcd}\{a_n\} = \prod_k p_k^{\min_i\{\alpha_{k,i}\}}. \tag{3.113}$$

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 inversible[27].

De la même manière,

$$\text{ppcm}\{a_n\} = \prod_k p_k^{\max_i\{\alpha_{k,i}\}}. \tag{3.114}$$

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'inclusion[28] : $a < b$ si et seulement si $(b) \subset (a)$.

Exemple 3.94
L'anneau $\mathbb{Z}[i\sqrt{3}]$ n'est pas factoriel parce que 4 a au moins deux décompositions distinctes en irréductibles :

$$4 = 2 \cdot 2, \tag{3.115}$$

et

$$4 = (1 + i\sqrt{3})(1 - i\sqrt{3}). \tag{3.116}$$

△

Nous allons voir dans l'exemple 3.134 que $\mathbb{Z}[i\sqrt{2}]$ est factoriel parce qu'il sera euclidien.

3.10 Anneau principal et idéal premier

Définition 3.95.
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 3.96.
Un anneau est ***principal*** *si*

25. Définition 2.60.
26. Définition 3.82.
27. 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.
28. Voir proposition 3.3.

(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 3.129) et nous utilisons la proposition 3.131 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 3.122.

Définition 3.97.
*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 3.98.
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 3.99 ([32])**.**
Soit un anneau commutatif[29] *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 3.98. 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 $x \in A \backslash I$.
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 $J = A$.
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 $x \in A \backslash I$, il faut prouver que tout idéal contenant I et x est A.

29. Tous les anneaux du Frido sont commutatifs

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 $[ax] = [A]$. C'est-à-dire que $ax - 1 \in I$. Nous avons alors

$$1 = ax + \underbrace{(1 - ax)}_{\in I}. \tag{3.117}$$

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 1.64 dit que A/I est un anneau intègre. Le point (1) dit alors que I est un idéal premier. □

Remarque 3.100.
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 3.97.

Proposition 3.101 ([49])**.**
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 $\bar{a}\bar{b} = \overline{ab} = 0$ 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. □

Proposition 3.102 (Thème 44, [1])**.**
Soit A un anneau principal qui n'est pas un corps. Pour un idéal propre I de A, les conditions suivantes sont équivalentes :

(1) I est un idéal maximal[30] *;*

(2) I est un idéal premier non nul[31] *;*

(3) il existe p irréductible[32] *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 $\overline{ab} = 0$, et par définition du produit dans le quotient, $\bar{a}\bar{b} = 0$. Par intégrité de l'anneau A/I (un corps est un anneau intègre, exemple 3.74) 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.

(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[33].

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

30. Définition 3.49.
31. Définition 3.97.
32. Définition 3.88.
33. ça me semble un peu trop facile. Lisez attentivement, et écrivez-moi pour dire si vous êtes d'accord ou pas.

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 sont 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 $I = J$.

□

3.103.
Dans la proposition 3.102, 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 3.104.
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 3.105
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 3.106(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 $\phi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. La proposition 3.47 dit que $S = \phi(J)$ où J est un idéal de $\mathbb{Z}$ contenant $n\mathbb{Z}$. Mais le corollaire 3.51 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

$$[km]_n = k[m]_n \in ([m]_n). \tag{3.118}$$

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

$$k[m]_n = [km]_n = \phi(km) \in \phi(m\mathbb{Z}). \tag{3.119}$$

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 (corollaire 3.77).

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 3.107
Nous verrons dans la proposition 27.24 que l'anneau des fonctions holomorphes sur un compact de $\mathbb{C}$ est principal. △

Définition 3.108.
Nous disons que deux éléments d'un anneau principal sont ***premiers entre eux*** *si leur PGCD est* 1.

Théorème 3.109.
Si A est un anneau principal et si p et q sont premiers entre eux dans A, alors on a l'isomorphisme d'anneaux

$$A/pqA \simeq A/pA \times A/qA. \tag{3.120}$$

3.10.1 Bézout

Théorème 3.110 ([50])**.**
Toute partie S d'un anneau principal admet un PGCD et un PPCM. De plus

$$\delta = \text{pgcd}(S) \Leftrightarrow (\delta) = \sum_{s\in S}(s)\mu = \text{ppcm}(S) \Leftrightarrow (\mu) = \bigcap_{s\in S}(s) \tag{3.121}$$

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

$$(\delta) = \sum_{s\in S}(s) \tag{3.122a}$$

$$(\mu) = \bigcap_{s\in S}(s) \tag{3.122b}$$

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

$$\sum_{x\in S}(x) \subset (d), \tag{3.123}$$

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 $\mu \mid m$.

□

Corollaire 3.111 (Théorème de Bézout[50])**.**
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

$$ua + vb = 1. \tag{3.124}$$

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

$$1 \in \text{pgcd}(a,b) = \sum_{x=a,b} (x) = (a) + (b). \tag{3.125}$$

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 $1 \in \text{pgcd}(a,b)$. □

Le lemme de Gauss est une application immédiate de Bézout. Il y aura aussi un lemme de Gauss à propos de polynômes (lemme 6.44), et une généralisation directe au théorème de Gauss, théorème 6.43.

Lemme 3.112 (lemme de Gauss)**.**
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 (3.13) nous donne donc $s, t \in \mathbb{A}$ tels que $sa + tc = 1$. En multipliant par b,

$$sab + tbc = b. \tag{3.126}$$

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. □

Un cas usuel d'utilisation est le cas de $A = \mathbb{N}^*$.

3.10.2 Élément premier

Définition 3.113 ([51])**.**
*Soit un anneau commutatif A. Un élément $p \in A$ est **premier** si il est*

(1) non nul,

(2) non inversible,

(3) si p divise un produit ab, alors il divise soit a soit b (ou le deux).

Proposition 3.114 ([52])**.**
Dans un anneau intègre[34] tout élément premier est irréductible[35].

Démonstration. Soit p, un élément premier dans un anneau intègre A.

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 3.113, 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 :

$$p = pxb. \tag{3.127}$$

Mais l'anneau est intègre et permet donc des simplifications par tout élément non nul. La relation 3.127 donne donc

$$1 = xb, \tag{3.128}$$

ce qui signifie que b est inversible.

Un travail similaire montre que a est inversible si p divise b.

□

34. Si pas intègre, voir l'exemple 3.116.
35. Toutes les définitions dans le thème 50.

Exemple 3.115
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 3.114 devient fausse.

Exemple 3.116
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, ok. 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 $(a,b)(c,d) = (ac,b)$. 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.

△

Exemple 3.117
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. △

Proposition 3.118 ([53, 1], thème 50)**.**
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 propre[36]*.*

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 3.96. Dans un anneau intègre, tout élément premier est irréductible, c'est la proposition 3.114.

(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 3.99(3).

□

Un exemple d'élément premier non irréductible est $[4]_6$ dans l'anneau non principal $\mathbb{Z}/6\mathbb{Z}$. Voir 3.127 et le lemme 3.128.

36. 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

3.10.3 Anneau noethérien

Définition 3.119.
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 3.120.
Tout anneau principal[37] *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 emboités. 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 $n \geqslant N$ nous avons

$$J \subset J_N \subset J_n \subset J. \tag{3.129}$$

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 $n \geqslant N$ nous avons $J_N = J_n = J$. La suite est par conséquent stationnaire. □

Exemple 3.121
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 3.128. △

Théorème 3.122 ([54])**.**
Tout anneau principal est factoriel.

Exemple 3.123($\mathbb{Z}[i\sqrt{5}]$ 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 $\mathbb{Z}[i\sqrt{5}]$ par[38]

$$\begin{aligned} N\colon \mathbb{Z}[i\sqrt{5}] &\to \mathbb{N} \\ z &\mapsto z\bar{z}. \end{aligned} \tag{3.130}$$

Le fait que ce soit à valeurs dans $\mathbb{N}$ est un simple calcul :

$$N(x + iy\sqrt{5}) = (x + iy\sqrt{5})(x - iy\sqrt{5}) = x^2 + 5y^2. \tag{3.131}$$

De plus N est multiplicative : $N(z_1z_2) = N(z_1)N(z_2)$.

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,

$$N(\alpha)N(\beta) = 1, \tag{3.132}$$

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 3.92) parce que

$$2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}). \tag{3.133}$$

Cela donne deux décompositions du nombre 6 en produit d'éléments non associés[39] (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 3.122. △

37. Définition 3.96.
38. C'est le carré de la norme usuelle, mais c'est l'usage dans le milieu.
39. Définition 3.82.

3.11 Anneau $\mathbb{Z}/6\mathbb{Z}$

Nous allons donner quelque 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

$$1 \times [4]_6 = [4_6] \tag{3.134}$$

et ensuite

$$2 \times [4]_6 = [8]_6 = [2]_6, \tag{3.135}$$

puis

$$3 \times [4]_6 = [2 + 4]_6 = [6]_6 = [0]_6, \tag{3.136}$$

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

(3.137)

Pour ne pas alourdir, nous n'avons pas écrit $[x]_6$ partout au lieu de x.

3.124 (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

$$U(\mathbb{Z}/6\mathbb{Z}) = \{[1]_6, [5]_6\}. \tag{3.138}$$

3.125 (Diviseurs de zéro)**.**
Les diviseurs de zéro sont ceux qui ont un $[0]_6$ dans leur table de multiplication, c'est-à-dire

$$\{[2]_6, [3]_6, [4]_6\}. \tag{3.139}$$

3.126 (Irréductibles)**.**
Les irréductibles sont ceux qui ne sont ni inversibles ni produit de deux éléments non inversibles. Les non inversibles sont :

$$\{[0]_6, [2]_6, [3]_6, [4]_6\}. \tag{3.140}$$

Ils sont candidats à être irréductibles. Les produits de ces éléments (on oublie les crochets) sont :

$$2 \times 2 = 4 \tag{3.141a}$$
$$2 \times 3 = 0 \tag{3.141b}$$
$$2 \times 4 = 2 \tag{3.141c}$$
$$3 \times 3 = 3 \tag{3.141d}$$
$$3 \times 4 = 0 \tag{3.141e}$$
$$4 \times 4 = 4. \tag{3.141f}$$

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.

3.127 (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

$$\big\{[2]_6,[3]_6,[4]_6\big\}. \tag{3.142}$$

Vous noterez que $\mathbb{Z}/6\mathbb{Z}$ a des éléments premiers non irréductibles. Cela est un contre-exemple à la proposition 3.118 dans le cas d'un anneau non-intègre.

Lemme 3.128 ([1]).
L'anneau $\mathbb{Z}/6\mathbb{Z}$ est noetherien, mais ni intègre ni principal[40].

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. □

3.12 Anneau euclidien

Définition 3.129 (Wikipédia).
*Soit A un anneau intègre. Un **stathme euclidien** sur A est une application $\alpha\colon A\backslash\{0\}\to\mathbb{N}$ tel que*

(1) $\forall a,b\in A\backslash\{0\}$, il existe $q,r\in A$ tel que

$$a=qb+r \tag{3.143}$$

et $\alpha(r)<\alpha(b)$.

(2) Pour tout $a,b\in A\backslash\{0\}$, $\alpha(b)\leqslant\alpha(ab)$.

*Un anneau est **euclidien** s'il accepte un stathme euclidien.*

40. Toutes les définitions dans le thème 50.

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.

Exemple 3.130
Le stathme de $\mathbb{N}$ pour la division euclidienne usuelle est $\alpha(n) = n$. Si $a, b \in \mathbb{N}$ nous écrivons

$$a = qb + r \tag{3.144}$$

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

$$r - b = a - b(q + 1) < a - b\frac{a}{b} = 0, \tag{3.145}$$

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 3.131 ([55]).
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 $a \in I\backslash\{0\}$ qui minimise $\alpha(a)$ va générer [41]. 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 3.132.
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 3.131.

D'abord $\mathbb{Z}$ est intègre, c'est l'exemple 3.75.

La condition $\alpha(b) \leqslant \alpha(ab)$ est immédiate : $|a| \leqslant |ab|$ 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

$$|a| = q_0|b| + r_0 \tag{3.146}$$

avec $r_0 < |b|$. Cela existe parce que $\alpha(x) = x$ est un stathme sur $\mathbb{N}$ par l'exemple 3.130.

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 3.129(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 3.129(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 3.129(1) parce que

$$\alpha(-r_0) = r_0 < |b| = \alpha(b). \tag{3.147}$$

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 3.129(1).

□

Nous venons de voir que $\mathbb{Z}$ est principal ; le lemme suivant nous dit que $\mathbb{Z}[X]$ n'est pas principal, lui.

41. Un tel élément existe...

Lemme 3.133 ([56]).
Si A est un anneau intègre qui n'est pas un corps, alors $A[X]$ n'est pas principal.

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 $Q = k'X = k'kQ$, ce qui implique que $kk' = 1$. L'idéal engendré par k contient donc en particulier $kk' = 1$ et donc contient $A[X]$ en entier :

$$1 = k'k \in k'(P) = (P). \tag{3.148}$$

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

$$1 = UX + Va. \tag{3.149}$$

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. □

Nous verrons dans le lemme 3.163 que si $\mathbb{K}$ est un corps, alors $\mathbb{K}[X]$ est principal.

Exemple 3.134
Prouvons que $\mathbb{Z}[i\sqrt{2}]$ est un anneau euclidien. Pour cela nous démontrons que

$$\begin{aligned} N\colon \mathbb{Z}[i\sqrt{2}] &\to \mathbb{N} \\ a + bi\sqrt{2} &\mapsto a^2 + 2b^2 \end{aligned} \tag{3.150}$$

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

$$\frac{z}{t} = \alpha + \beta i\sqrt{2}. \tag{3.151}$$

Nous désignons par $\alpha + \epsilon_1$ et $\beta + \epsilon_2$ les entiers les plus proches de α et b. Nous avons $|\epsilon_1|, |\epsilon_2| \leqslant \frac{1}{2}$. Nous posons alors naturellement

$$q = (\alpha + \epsilon_1) + (\beta + \epsilon_2)i\sqrt{2} \tag{3.152}$$

et nous calculons $r = z - qt$:

$$2b'\epsilon_2 - a'\epsilon_1 + i\sqrt{2}\big(\epsilon_1 b' - a'\epsilon_2\big). \tag{3.153}$$

Nous trouvons

$$N(r) = a'^2\epsilon_1^2 + 4b'^2\epsilon_2^2 + 2a'^2\epsilon_1^2 + 2b'^2\epsilon_2^2 \leqslant \frac{3}{4}a'^2 + \frac{3}{2}b'^2. \tag{3.154}$$

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

$$N(zt) = (a^2 + 2b^2)(a'^2 + 2b'^2), \tag{3.155}$$

et tant que $t \neq 0$ nous avons bien $N(zt) > N(z)$. △

Notons en particulier que $\mathbb{Z}[i\sqrt{2}]$ est factoriel et principal.

Exemple 3.135
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 3.82) si et seulement si $a = \pm b$.

De plus si p est irréductible [42], alors $-p$ est irréductible. Les éléments irréductibles de $\mathbb{Z}[i\sqrt{2}]$ arrivent donc par pairs 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 décomposition en facteurs irréductibles d'éléments. △

Le lemme suivant fait en pratique partie de l'exemple 3.138, mais nous l'isolons pour plus de clarté [43].

Lemme 3.136.
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 3.135 nous pouvons écrire

$$y = \pm p_1^{\sigma_1} \dots p_n^{\sigma_n} \tag{3.156a}$$
$$a = \pm p_1^{\alpha_1} \dots p_n^{\alpha_n} \tag{3.156b}$$
$$b = \pm p_1^{\beta_1} \dots p_n^{\beta_n} \tag{3.156c}$$

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 $\beta = 3\sigma_i$ (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. □

3.12.1 Équations diophantiennes

Exemple 3.137
L'équation diophantienne

$$x^2 = 3y^2 + 8 \tag{3.157}$$

n'a pas de solutions. En effet si nous prenons l'équation modulo 3 nous obtenons

$$[x^2]_3 = [3y^2 + 8]_3 = [8]_3 = [2]_3. \tag{3.158}$$

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 $2^2 = 4 = 1 \neq 2$. △

Exemple 3.138
Résolvons l'équation diophantienne

$$x^2 + 2 = y^3. \tag{3.159}$$

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 (3.150).

42. Définition 3.88
43. Merci à Marvoir pour m'avoir souligné le manque.

L'élément $i\sqrt{2}$ est irréductible parce que $N(i\sqrt{2}) = 2$, et si nous avions $i\sqrt{2} = pq$, alors nous aurions $N(p)N(q) = 2$, ce qui n'est possible que si $N(p)$ ou $N(q)$ vaut 1.

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

$$x = (i\sqrt{2})^\beta q \tag{3.160}$$

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 3.136). 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

$$\begin{cases} x = a^3 - 6ab^2 & \text{(3.161a)} \\ 1 = 3a^2b - 2b^3 & \text{(3.161b)} \end{cases}$$

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

$$(x, z) = (-5, 1 + i\sqrt{2}) \tag{3.162a}$$
$$(x, z) = (5, -1 + i\sqrt{2}) \tag{3.162b}$$
$$\tag{3.162c}$$

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 $(-5, 3)$. △

3.12.2 Triplets pythagoriciens et équation de Fermat pour $n = 4$

Définition 3.139.
*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 3.140.
On dit qu'un triplet pythagoricien est ***primitif*** *si les trois nombres sont premiers dans leur ensemble*[44].

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 nombre[45], donc les nombres x, y et z sont premiers deux à deux.

Lemme 3.141.
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'ou 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. □

Proposition 3.142 (Triplets pythagoriciens[57, 58])**.**
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

$$\begin{cases} x = d(u^2 - v^2) & \text{(3.163a)} \\ y = 2duv & \text{(3.163b)} \\ z = d(u^2 + v^2) & \text{(3.163c)} \end{cases}$$

ou

$$\begin{cases} x = 2duv & \text{(3.164a)} \\ y = d(u^2 - v^2) & \text{(3.164b)} \\ z = d(u^2 + v^2) & \text{(3.164c)} \end{cases}$$

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 (3.163) :

$$x^2 + y^2 = d^2(u^2 - v^2) + 4d^2u^2v^2 = d^2(u^2 + v^2)^2, \tag{3.165}$$

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 $\left(\frac{x}{k}, \frac{y}{k}, \frac{z}{k}\right)$ 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 généralité[46], grâce au lemme 3.141, nous pouvons supposer x est pair tandis que y et z sont impairs. Comme $x^2 = (z+y)(z-y)$, nous avons

$$\left(\frac{x}{2}\right)^2 = \left(\frac{z+y}{2}\right)^2 \left(\frac{z-y}{2}\right)^2. \tag{3.166}$$

44. Définition 3.11.
45. Parce que k et k^2 ont les mêmes facteurs premiers.
46. En échangeant les rôles de x et y ici, nous obtenons à la fin la seconde forme des solutions.

Vu que z et y sont premiers entre eux, les nombres $z-y$ et $z+y$ sont également premiers entre eux [47]. Donc les facteurs premiers (qui arrivent au moins au carré) de $(x/2)^2$ sont chacun soit dans $(z+y)/2$ soit dans $(z-y)/2$. Nous en déduisons que ces derniers sont des carrés d'entiers. Nous posons

$$\frac{z-y}{2}=u^2 \quad \frac{z+y}{2}=v^2. \tag{3.167}$$

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 $(x/2)^2=u^2v^2$ et donc $x=2uv$ puis par somme et différence :

$$\begin{cases} x=2uv & \text{(3.168a)}\\ y=v^2-u^2 & \text{(3.168b)}\\ z=u^2+v^2, & \text{(3.168c)} \end{cases}$$

ce qu'il fallait. □

Remarque 3.143.
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 3.144 ([57])**.**
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 minimum [48]). 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 3.142, il existe $u,v\in\mathbb{N}^*$ premiers entre eux tels que, sans perte de généralité [49], on ait

$$\begin{cases} \bar{x}=2uv & \text{(3.169a)}\\ \bar{y}=u^2-v^2 & \text{(3.169b)}\\ z=u^2+v^2. & \text{(3.169c)} \end{cases}$$

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 3.141 implique alors que v soit pair.

De l'équation 3.169b, 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 3.142, en se souvenant que v est pair : il existe donc deux nombres r et s premiers entre eux tels que

$$\begin{cases} v=2rs & \text{(3.170a)}\\ y=r^2-s^2 & \text{(3.170b)}\\ u=r^2+s^2. & \text{(3.170c)} \end{cases}$$

47. Si $z-y=kn$ et $z+y=km$, faisant la somme et la différence on voit que y et z sont divisibles par k.
48. Voir quelque chose comme le lemme 1.32.
49. 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 :

$$\begin{cases} r = \alpha^2 & (3.171a)\\ s = \beta^2 & (3.171b)\\ r^2 + s^2 = \gamma^2. & (3.171c) \end{cases}$$

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 :

$$\begin{aligned} z &= u^2 + v^2 && \text{par 3.169c}\\ &= r^2 + s^2 + 4r^2s^2 && \text{par 3.170}\\ &= \gamma^2 + 4r^2s^2\\ &> \gamma^2, \end{aligned}$$

et a fortiori $\gamma < z$. □

3.13 Polynômes à coefficients dans un anneau commutatif

Nous définissons ici $A[X]$ où A est un anneau commutatif. Pour la définition de $\mathbb{K}(X)$ où $\mathbb{K}$ est un corps, voir 6.72.

3.13.1 Définitions

Soit A un anneau commutatif. Nous considérons $\mathcal{P}$ l'ensemble des suites presque nulles d'éléments de A, ce sont les suites $(a_n)_{n\in\mathbb{N}}$ qui ne possèdent qu'un nombre fini d'éléments non nuls.

Cela est un A-module libre de base [50]

$$(e_n)_k = \delta_{nk}. \tag{3.172}$$

Si $a, b \in \mathcal{P}$, nous définissons le produit ab par

$$(ab)_n = \sum_{k=0}^{n} a_k b_{n-k}, \tag{3.173}$$

et la somme par

$$(a + b)_n = a_n + b_n. \tag{3.174}$$

Cela est bien un élément de $\mathcal{P}$ parce qu'il existe $N \in \mathbb{N}$ tel que $a_n = b_n = 0$ pour tout $n \geqslant N$. Avec la somme et le produit par un scalaire (élément de A), le module $\mathcal{P}$ devient une A-algèbre commutative unitaire. L'unité est

$$e_0 = (1, 0, \ldots). \tag{3.175}$$

Définition 3.145.
*En tant que A-algèbre, l'ensemble $\mathcal{P}$ est l'**algèbre des polynômes en une indéterminée** à coefficients dans A. Elle est notée $A[X]$ pour des raisons que nous expliquons dans 3.13.2.*

Définition 3.146.
L'ensemble $A[X]$ devient un $\mathbb{K}$-espace vectoriel avec la définition

$$(\lambda P)_k = \lambda P_k. \tag{3.176}$$

50. Définition 3.64.

Définition 3.147.
Si $P \in A[X]$ est la suite $(a_k)_{k\in\mathbb{N}}$ et si $\alpha \in A$, alors nous définissons

$$P(\alpha) = \sum_{k\in\mathbb{N}} a_k \alpha^k. \tag{3.177}$$

La somme est toujours finie.

Lemme 3.148.
Si A est un anneau et si $\alpha \in A$, alors l'application

$$\begin{aligned} g\colon A[X] &\to A \\ P &\mapsto P(\alpha) \end{aligned} \tag{3.178}$$

est un morphisme d'anneaux[51].

Démonstration. Nous notons P_k les éléments de la suite définissant P et Q_k ceux de Q. Alors nous avons

$$(P+Q)(\alpha) = \sum_k (P_k + Q_k)\alpha^k = \sum_k P_k\alpha^k + \sum_k Q_k\alpha^k = P(\alpha) + Q(\alpha) \tag{3.179}$$

et

$$P(\alpha)Q(\alpha) = \big(\sum_n P_n\alpha^n\big)\big(\sum_k Q_k\alpha^k\big) = \sum_k Q_k\big(\sum_n P_n\alpha^n\big)\alpha^k = \sum_k\sum_n Q_k P_n^{n+k} \tag{3.180a}$$

$$= \sum_m \big(\sum_{l=0}^{m} P_l Q_{m-l}\big)\alpha^m = \sum_m (PQ)_m\alpha^m = (PQ)(\alpha). \tag{3.180b}$$

□

Définition 3.149.
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* $\deg(P)$.

3.13.2 Notations

Le polynôme donné par la suite $(a_n)_{n\in\mathbb{N}}$ est souvent notée

$$\sum_k a_k X^k. \tag{3.181}$$

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.

3.13.2.1 Première façon

La première est de dire qu'il n'a pas de significations, et que X^2 est un simple abus de notations pour écrire $(0, 0, 1, 0, \cdots)$. 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.

51. Définition 1.38.

3.13.2.2 Seconde façon

La seconde façon de voir le « X » est de nous rappeler que $A[X]$ a une base en tant de que 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 $\mathcal{P}$ exprimé avec X. i

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.

Lemme 3.150.
Nous avons

$$P(X) = P \tag{3.182}$$

pour tout $P \in A[X]$.

Démonstration. Un polynôme $P \in A[X]$ peut s'évaluer sur n'importe quel élément d'un anneau qui étend A : si $P = (a_k)_{k\in\mathbb{N}}$ alors par définition $P(\alpha) = \sum_k a_k\alpha^k$. Or $A[X]$ est lui-même un anneau qui étend A ; donc si Q est un polynôme, ça a un sens d'écrire $P(Q)$ et le résultat sera un élément de $A[X]$. Avec en particulier $Q = X$, c'est-à-dire $Q = (0, 1, 0, \ldots)$, l'élément $P(X)$ de $A[X]$ vaut

$$\sum_k a_k X^k, \tag{3.183}$$

qui est exactement P lui-même. □

Mais il faut bien comprendre que si P est le polynôme $(-3, 2, 1, 0, \ldots)$, 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 $P = X^2 + 2X - 3$.

3.151.
Dans la suite, nous considérons cette seconde façon de comprendre la notation X.

Lemme 3.152.
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

$$Q(\bar{X}) = \overline{Q(X)} = \bar{Q}. \tag{3.184}$$

Démonstration. Si $Q = \sum_k a_k X^k$, alors par la linéarité de la prise de classes,

$$\bar{Q} = \sum_k a_k \overline{X^k}. \tag{3.185}$$

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 3.45). Toujours par définition du produit appliqué à l'élément $\bar{X}$ nous avons $(\bar{X})^2 = \overline{X^2}$; par récurrence $\overline{X^k} = \bar{X}^k$, et

$$\bar{Q} = \sum_k a_k \bar{X}^k = Q(\bar{X}). \tag{3.186}$$

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 3.150. □

3.13.3 Monômes

3.153.
Les éléments de la forme λX^k avec $\lambda \in A$ et $k \in \mathbb{N}$ sont des **monômes**.

Nous allons aussi considérer

$$A_n[X] = \{P \in A[X] \text{ tel que } \deg(P) \leqslant n\}. \tag{3.187}$$

Cela est un sous-module libre.

3.13.4 Évaluation

Soit $P \in A[X]$. A priori, P n'est qu'une suite dans A indexée par $\mathbb{N}$. Nous définissons son évaluation sur un élément $\alpha \in A$ par

$$P(\alpha) = \sum_k a_k \alpha^k. \tag{3.188}$$

Cette somme est toujours finie.

3.154.
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 a 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 6.99 et l'exemple 20.37.

Définition 3.155.
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 3.156.
Soient un anneau A et un anneau B qui contient A (comme sous-anneau). Pour tout $\alpha \in B$ nous avons

$$A[\alpha] = \{P(\alpha) \text{ tel que } P \in A[X]\} \tag{3.189}$$

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

$$\{P(\alpha) \text{ tel que } P \in A[X]\} \subset A[\alpha]. \tag{3.190}$$

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. □

3.13.5 Polynômes sur un anneau intègre

Théorème 3.157.
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

$$\deg(PQ) = \deg(P) + \deg(Q) \tag{3.191}$$

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. □

3.158.
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.

Corollaire 3.159.
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 $U(A)$. □

La **valuation** du polynôme $P = \sum_n a_n X^n$, notée $\mathrm{val}(P)$, est

$$\mathrm{val}(P) = \min\{n \text{ tel que } a_n \neq 0\}. \tag{3.192}$$

Nous avons $\mathrm{val}(P) \leqslant \deg(P)$ et $\mathrm{val}(P) = \deg(P)$ si et seulement si P est un monôme. Si $P = 0$, nous convenons que $\mathrm{val}(0) = \infty$ et $\deg(0) = -\infty$.

3.13.6 Division euclidienne

Le théorème suivant établit la **division euclidienne** dans $A[X]$ du polynôme P par un polynôme D.

Théorème 3.160.
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

$$P = QD + R \tag{3.193}$$

avec $\deg(R) < \deg(D)$.

Les polynômes Q et R sont déterminés de façon univoque par cette condition.

Définition 3.161.
*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 $P = QD$.*[52]

3.162.
Le théorème 3.160 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 a priori un coefficient dominant inversible.

Lemme 3.163 (Thème 44)**.**
Si $\mathbb{K}$ est un corps[53]*, 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 3.160. L'anneau $\mathbb{K}[X]$ est donc euclidien et par conséquent principal (proposition 3.131). □

Dans le théorème 6.36 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.

52. Ceci se rapproche tout naturellement des notions de divisibilité dans un anneau intègre général, vues en sous-section 3.8.2.
53. Définition 1.61.

Définition 3.164 ([59]).
Soit un anneau A. Deux polynômes P et Q dans $A[X]$ sont dits ***étrangers*** *entre eux si* 1 *est un pgcd*[54] *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 3.165([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). △

3.13.7 Polynôme primitif

Définition 3.166.
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 3.167 (Ordre d'un polynôme).
*Soit P un polynôme irréductible de degré n sur $\mathbb{F}_p[X]$. L'****ordre*** *de P est*

$$\min\{k \text{ tel que } P \mid X^k - 1\}. \tag{3.194}$$

Définition 3.168 (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 3.169 (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.*

3.170.
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 3.108 d'avoir des nombres premiers entre eux.

(2) Le contenu de ses coefficients est 1. Parce que le contenu est précisément le pgcd, définition 3.166.

La notion de polynôme primitif au sens du pgcd est particulière aux polynôme à coefficients dans un anneau comme le montre le lemme suivant.

Lemme 3.171.
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 corollaire 3.179.

54. Définition 1.46.

3.13.8 Racines des polynômes

Définition 3.172.
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 3.173.
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 6.83. 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 euclidienne [55] de P par μ : il existe des polynômes Q et R tels que

$$P = Q\mu + R \tag{3.195}$$

avec $\deg(R) < \deg(\mu)$. Donc R est une constante, élément de A : appelons-le a. En évaluant (3.195) en α, il vient

$$0 = P(\alpha) = Q(\alpha)\mu(\alpha) + a, \tag{3.196}$$

et nous en déduisons que $a = 0$, ce qui montre que $P = Q\mu$ et que μ divise P. □

Définition 3.174 (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.*

Pour une définition générale d'une racine simple de l'équation $f(x) = 0$, voir la définition 35.49.

La proposition 3.173 nous indique que toute racine est de multiplicité au moins 1.

Proposition 3.175.
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 3.176.
Soient P et Q des polynômes non nuls de $A[X]$ et $\alpha \in A$. Alors

(1) $\theta_\alpha(P + Q) \leqslant \min\{\theta_\alpha(P), \theta_\alpha(Q)\}$, et l'égalité a lieu si $\theta_\alpha(P) \neq \theta_\alpha(Q)$;

(2) $\theta_\alpha(PQ) \geqslant \theta_{\alpha(P)} + \theta_\alpha(Q)$, 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 3.177.
Soit A un anneau intègre et $P \in A[X]\backslash\{0\}$, un polynôme de degré n.

(1) Si $\alpha_1, \ldots, \alpha_p \in A$ sont des racines deux à deux distinctes de multiplicités $k_1, \ldots, k_p$, 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 $Q \in \mathbb{A}[X]$ tel que $P = Q(X - \alpha)^k$. Il reste à voir que $Q(\alpha) \neq 0$. Cela est une conséquence de la

55. Théorème 3.160.

proposition 3.173 : 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 $p \geqslant 2$ et nous effectuons une récurrence sur p. Nous considérons donc les $p-1$ premières racines $\alpha_1, \dots, \alpha_{p-1}$ et un polynôme $R \in \mathbb{A}[X]$ tel que $R(\alpha_i) \neq 0$ pour $i = 1, \dots, p-1$ et

$$P = \underbrace{(X-\alpha_1)^{k_1} \dots (X-\alpha_{p-1})^{k_{p-1}}}_{S} R. \tag{3.197}$$

Par hypothèse $P(\alpha_p) = S(\alpha_p)R(\alpha_p) = 0$. L'anneau $\mathbb{A}$ 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 3.176 afin de dire que le degré de α_p pour $P = SR$ est k_p. Par conséquent

$$R = (X-\alpha_p)^{k_p} T \tag{3.198}$$

avec $T(\alpha_p) \neq 0$ et enfin

$$P = \prod_{i=1}^{p} (X-\alpha_i) T. \tag{3.199}$$

De plus $T(\alpha_i) \neq 0$, sinon $R(\alpha_i)$ serait nul. □

Corollaire 3.178.
Un polynôme de degré n possède au maximum n racines distinctes.

Démonstration. Le théorème 3.177(2) dit que la somme des multiplicités des racines de P est au maximum n. Mais la proposition 3.173 dit que toutes les racines ont une multiplicité au moins un. Donc il ne peut pas y en avoir plus de n. □

Corollaire 3.179 (Conséquence du lemme de Gauss[60])**.**
Soient A un anneau factoriel et 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 pgcd*[56] *sur* Frac$(A)[X]$.

Exemple 3.180
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

$$P = \left(X - \frac{1+\sqrt{5}}{2}\right)\left(X - \frac{1-\sqrt{5}}{2}\right). \tag{3.200}$$

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 Frac $\big(\mathbb{Z}[\sqrt{5}]\big)$. △

3.13.9 Quelques identités

Lemme 3.181.
Quelques identités de polynômes.

(1) Si n est impair, alors $1+X$ divise $1+X^n$.

(2) Pour tout n nous avons $X^n - 1 = (X-1)(1+X+\cdots+X^{n-1})$.

(3) $X^n - a^n = (X-a)\sum_{i=0}^{n-1} a^i X^{n-1-i}$.

56. Définition 3.169.

Démonstration. Nous démontrons uniquement le point (2), puisque les autres ont été vus en début de chapitre[57]. Le cas $n = 1$ est évident. Procédons alors par récurrence en considérant un nombre entier impair n :

$$\begin{aligned} 1 + X^{n+2} &= 1 + X^n + X^{n+2} - X^n && \text{(3.201a)}\\ &= (1 + X)P + X^n(X^2 - 1) && \text{(3.201b)}\\ &= (1 + X)P + X^n(X + 1)(X - 1) && \text{(3.201c)}\\ &= (1 + X)\big(P + X^n(X - 1)\big). && \text{(3.201d)} \end{aligned}$$

□

3.13.10 Polynômes en plus de variables

Définition 3.182.
Nous définissons les polynômes en n variables, dont l'ensemble est noté $A[X_1, \dots, X_n]$ comme étant l'ensemble des suites indexées par $\mathbb{N}^n$ et dont seulement une quantité finie de coefficients sont non nuls.

Je vous laisse écrire la loi de multiplication et les suites auxquelles correspondent les polynômes $X_1, \dots, X_n$.

57. Voir l'égalité (3.1).

Chapitre 4

Espaces vectoriels (début)

4.1 Parties libres, génératrices, bases et dimension

Nous avons déjà défini (dans 3.63) un espace vectoriel comme étant un module sur un corps commutatif. En explicitant un peu, cela donne ceci[61].

Un espace vectoriel sur le corps $\mathbb{K}$ est un ensemble V muni de deux opérations :

— une loi de composition interne $+ : V \times V \to V$,

— une loi de composition externe $\cdot : \mathbb{K} \times V \to V$

telles que

(1) $(V, +)$ soit un groupe abélien,

(2) pour tout $u, v \in V$ et pour tout $k, k' \in \mathbb{K}$,

$$k(u+v) = (ku) + (kv) \tag{4.1a}$$
$$(kk')u = k(k'u) \tag{4.1b}$$
$$(k+k')u = (ku) + (k'u) \tag{4.1c}$$
$$1u = u \tag{4.1d}$$

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 $\{u_i\}_{i=1,\dots,n}$, l'égalité*

$$a_1u_1 + \cdots + a_nu_n = 0 \tag{4.2}$$

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 $\mathrm{Span}(A)$ 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* $\mathrm{Span}(B) = E$.

Remarque 4.4.
Ces définitions demandent des commentaires en dimension infinie[1].

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.*

Proposition 4.6 ([1])**.**
Tout élément non nul d'un espace vectoriel possédant une base[2] *se décompose de façon unique en combinaison linéaire finie d'éléments d'une base.*

Démonstration. Soit un espace vectoriel E et une base $\{e_i\}_{i\in I}$ où I est un ensemble a 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

$$v = \sum_{j\in J} v_j e_j. \tag{4.3}$$

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

$$v = \sum_{j\in J} v_j e_j = \sum_{k\in K} w_k e_k. \tag{4.4}$$

Nous posons $L = J \cup K$ et, pour $l \in L$,

$$\alpha_l = \begin{cases} v_l & \text{si } l \in J\backslash K \\ w_l & \text{si } l \in K\backslash J \\ v_l - w_l & \text{si } l \in K \cap J. \end{cases} \tag{4.5}$$

Nous avons alors

$$\sum_{l\in L} \alpha_l e_l = 0, \tag{4.6}$$

ce qui implique que $\alpha_l = 0$ pour tout $l \in L$ parce que la partie $\{e_i\}_{i\in I}$ est libre et que L est finie.

L'unicité de la décomposition de v signifie que

$$\{j \in J \text{ tel que } v_j \neq 0\} = \{k \in K \text{ tel que } w_k \neq 0\} \tag{4.7}$$

et que pour l dans cet ensemble, $v_l = w_l$.

Soit $j \in J$; il y a deux possibilités : $j \in J\backslash K$ et $j \in J \cap K$. 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 $k \in J \cap K$. □

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 $f\colon E \to E$.

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.

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.

Libre Si J est une partie finie de I et si les λæ sont des scalaires tels que $\sum_{j\in J}\lambda_j f(v_j)=0$, alors

$$0=\sum_{j\in J}\lambda_j f(v_j)=f\big(\sum_{j\in J}\lambda_j v_j\big). \tag{4.8}$$

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

$$y=\sum_{j\in J}\lambda_j v_j. \tag{4.9}$$

Nous avons alors

$$x=f(y)=\sum_{j\in J}\lambda_j f(v_j), \tag{4.10}$$

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 suffit[3]. 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,

$$\sum_{j\in J}(\lambda_j-\mu_j)f(v_j)=0. \tag{4.11}$$

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.

Surjective Soit $x\in E$. Vu que $\{f(v_i)\}_{i\in I}$ est une base, il existe des scalaires λ_j tels que

$$x=\sum_{j\in J}\lambda_j f(v_j)=f\big(\sum_{j\in J}\lambda_j v_j\big). \tag{4.12}$$

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'une 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 $\lambda_2 v_1-\lambda_1 v_1=0$. 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

3. Nous utilisons le fait que l'union de deux parties finies d'une ensemble est finie (lemme 1.17).

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

$$v_i = \sum_{k=1}^{n} \lambda_{ij} e_j \tag{4.13}$$

Vu que

$$v_{n+1} = \sum_{k=1}^{n} \lambda_{n+1,k} e_k \neq 0, \tag{4.14}$$

quitte à changer la numérotation des e_i nous pouvons supposer que $\lambda_{n+1,n} \neq 0$. Nous considérons les vecteurs

$$w_i = \lambda_{n+1,n} v_i - \lambda_{i,n} v_{n+1}. \tag{4.15}$$

En calculant un peu,

$$w_i = \lambda_{n+1,n} \sum_k \lambda_{i,k} e_k - \lambda_{i,n} \sum_k \lambda_{n+1,k} e_k \tag{4.16a}$$

$$= \sum_{k=1}^{n-1} \big(\lambda_{n+1,n}\lambda_{i,k} - \lambda_{i,n}\lambda_{n+1,}\big) e_k \tag{4.16b}$$

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

$$0 = \sum_{i=1}^{n} \alpha_i w_i = \sum_{i=1}^{n} \alpha_i \lambda_{n+1,n} v_i - \left(\sum_{i=1}^{n} \alpha_i \lambda_{i,n} \right) v_{n+1}. \tag{4.17}$$

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 (4.17) 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 maximum[4]*, 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 $\forall x \in G \backslash B$, 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 $x \in G \backslash B$; 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

$$\sum_{i=1}^{l} \lambda_i b_i + \lambda_x x = 0. \tag{4.18}$$

Si $\lambda_x = 0$ alors un de λ_i doit être non nul et l'équation (4.18) 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

$$x = \frac{1}{\lambda_x} \sum_{i=1}^{l} \lambda_i b_i. \tag{4.19}$$

Donc tous les éléments de $G \backslash B$ 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. □

4. Encore une fois, à part quelques cas triviaux, il n'est pas clair à ce point que ce maximum existe.

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 $L = \varnothing$). La partie B maximalement 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 $\mathrm{Card}(B') \leqslant \mathrm{Card}(B)$. Par symétrie on a l'inégalité inverse. Donc $\mathrm{Card}(B) = \mathrm{Card}(B')$.

(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.

□

Remarque 4.12.
Le théorème de la base incomplète 4.11(2) est ce qui permet de construire une base d'une 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.

Définition 4.13.
*La **dimension** d'un espace vectoriel de type fini est le cardinal*[5] *d'une*[6] *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

$$e_j = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \leftarrow \text{j-ème} \quad .$$

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

$$\delta_{ij} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases} \tag{4.20}$$

5. Définition 1.27.
6. Le théorème de la base incomplète 4.11(3) montre que cette définition ne souffre d'aucune ambiguïté.

Les éléments de la base canonique de $\mathbb{R}^m$ peuvent donc être écrits $e_i = \sum_{k=1}^{m} \delta_{ik} e_k$. △

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 l'autre assertion, soit une partie génératrice $\{v_i\}_{i\in I}$ où I contient n éléments. Par le théorème 4.15(2) il existe $J \subset I$ tel que $\{v_j\}_{j\in J}$ soit une base. Si l'inclusion $J \subset I$ est 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). □

Définition 4.17.
*Soit F un sous-espace vectoriel de l'espace vectoriel E. La **codimension** de F dans E est*

$$\operatorname{codim}_E(F) = \dim(E/F). \tag{4.21}$$

Problèmes et choses à faire

Voir que E/F a une structure vectoriel, 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 ZF [7].

Lemme 4.18 ([62])**.**
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) $V \cap W_1 = \{0\}$;

(2) $V + W_2 = E$.

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.

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.

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 inductif[8]. 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 1.15 nous donne alors un maximum W de $\mathcal{A}$. Ce maximum vérifie

(1) $W \cap V = \{0\}$,

(2) $W_1 \subset W \subset W_2$,

(3) pour tout $W' \in \mathcal{A}$, nous avons $W' \subset W$ parce que W 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

$$x = v + w_2. \tag{4.22}$$

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,

$$y = w' + \lambda w_2 \tag{4.23}$$

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 (4.23) permet alors d'écrire $w_2 = (y - w')/\lambda$ et finalement

$$x = v + \frac{1}{\lambda}(y - w') = \underbrace{v + \frac{1}{\lambda}y}_{\in V} - \underbrace{\frac{1}{\lambda}w'}_{\in W}. \tag{4.24}$$

La somme d'espaces vectoriels $E = V + W$ est donc établie.

□

Corollaire 4.19.
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 $v \in E\backslash V$ 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 4.18 nous donne alors un supplémentaire de V. □

Proposition 4.20 (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 :

8. Définition 1.14.

— 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 4.21 (Base incomplète, dimension quelconque)**.**
Soit une partie $\{e_i\}_{i\in I}$ génératrice de l'espace vectoriel E (ici, I est un ensemble quelconque[9]). 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. 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 4.22 ([63])**.**
*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 $S \to \mathbb{K}$ qui sont non-nulles en un nombre fini de points de S.*

Autrement dit, $\sigma : S \to \mathbb{K}$ est dans $F_{\mathbb{K}}(S)$ si $\{x \in S \text{ tel que } \delta(x) \neq 0\}$ est fini[10].

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 4.23.
L'ensemble des applications δ_s données par

$$\begin{aligned} \delta_s : S &\to \mathbb{K} \\ t &\mapsto \begin{cases} 1 & \text{si } t = s \\ 0 & \text{sinon} \end{cases} \end{aligned} \tag{4.25}$$

avec $s \in S$ forment une base[11] de $F(S)$.

Démonstration. Pour prouver que les δ_s sont générateurs, nous considérons $g : S \to \mathbb{K}$ non nul sur la partie finie $\{s_i\}_{i\in I}$ de S. Alors nous avons

$$g = \sum_{i\in I} g(s_i)\delta_{s_i}. \tag{4.26}$$

Pour prouver que les δ_s forment une partie libre, nous supposons avoir $\lambda_i \in \mathbb{K}$ tels que

$$g = \sum_{i\in I} \lambda_i \delta_{s_i} = 0 \tag{4.27}$$

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 1.16.
11. Définition 4.5.

Soit $j \in I$. Nous avons

$$0 = f(s_j) = \sum_{i \in I} \lambda_i \underbrace{\delta_{s_i}(s_j)}_{=\delta_{ij}} = \lambda_j. \tag{4.28}$$

Donc les coefficients λ_i sont tous nuls, et nous avons prouvé que la partie est libre. □

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'esemble des applications de S vers $\mathbb{K}$.

4.2 Applications linéaires

4.2.1 Définition

Définition 4.24.
Soient des espaces vectoriels E et F sur le corps $\mathbb{K}$. Une application $T\colon E \to F$ est dite ***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.*

Si vous avez bien suivi, les égalités dans la définition 4.24 sont des égalités dans F.

Lemme-définition 4.25.
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 4.26
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 un application linéaire de $\mathbb{R}^m$ dans $\mathbb{R}^m$ pour tout λ dans $\mathbb{R}$ et m dans $\mathbb{N}$. △

Exemple 4.27
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

$$U_\lambda(ax) = \lambda(ax) + v \neq a(\lambda x + v) = aU_\lambda(x).$$

△

Exemple 4.28
Soit A une matrice fixée de $\mathcal{M}_{n\times m}$. La fonction $T_A\colon \mathbb{R}^m \to \mathbb{R}^n$ définie par $T_A(x) = Ax$ est une application linéaire. En effet,

— $T_A(x + y) = A(x + y) = Ax + Ay = T_A(x) + T_A(y)$,

— $T_A(ax) = A(ax) = a(Ax) = aT_A(x)$.

△

On peut observer que, si on identifie $\mathcal{M}_{1\times 1}$ et $\mathbb{R}$, on obtient le premier exemple comme cas particulier.

Définition 4.29 (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 4.25.*
- *Une application linéaire $E \to E$ est un **endomorphisme** de E. L'ensemble des endomorphismes de E est noté* $\mathrm{End}(E)$.
- *Un endomorphisme bijectif est un **automorphisme**. L'ensemble des automorphismes de E est noté* $\mathrm{Aut}(E)$.
- *Une application linéaire bijective $E \to F$ est un **isomorphisme** d'espace vectoriel. L'ensemble des isomorphismes $E \to F$ est noté*[12] $\mathrm{GL}(E,F)$.

Remarque 4.30.
Les ensembles définis en 4.29 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 12.26.

Définition 4.31.
*Si E est un espace vectoriel, si X est un espace vectoriel, et si $f\colon X \to E$ est une application, le **noyau** de f est le noyau de f lorsque E est vu comme un groupe pour l'addition*[13]*, c'est-à-dire la partie*

$$\ker(f) = \{x \in X \text{ tel que } f(x) = 0\}. \tag{4.29}$$

Proposition 4.32.
Le noyau d'une application linéaire est un sous-espace vectoriel.

Démonstration. Soit une application linéaire $f\colon E \to F$. Si $x, y \in \ker(f)$ et si $\lambda \in \mathbb{K}$ alors

$$f(x+y) = f(x) + f(y) = 0 + 0 = 0, \tag{4.30}$$

donc $x + y \in \ker(f)$ et

$$f(\lambda x) = \lambda f(x) = 0, \tag{4.31}$$

donc $\lambda x \in \ker(f)$. □

Proposition 4.33.
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 $T\colon E \to F$ 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

$$T(v) = \sum_i v_i f_i \tag{4.32}$$

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 $T = U$.

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 2.24.

□

Lemme 4.34 ([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

$$\begin{aligned}\varphi_{i\alpha}\colon V &\to W\\ v &\mapsto v_i f_\alpha\end{aligned} \tag{4.33}$$

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 : $\dim\big(\mathcal{L}(V,W)\big) = \dim(V)\dim(W)$.

Démonstration. Il faut prouver que $\{\varphi_{i\alpha}\}$ est libre et générateur.

Générateur Soit une application linéaire $b\colon V \to W$. En décomposant $b(v)$ dans la base $\{f_\alpha\}$, nous définissons $b_\alpha\colon V \to \mathbb{K}$ par

$$b(v) = \sum_\alpha b_\alpha(v) f_\alpha. \tag{4.34}$$

Nous posons $b_{\alpha i} = b_\alpha(e_i)$. Ainsi,

$$b(v) = \sum_\alpha v_i b_{\alpha i} f_\alpha = \sum_{\alpha i} b_{\alpha i}\varphi_{i\alpha}(v). \tag{4.35}$$

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 $v \in V$:

$$0 = \sum_{i\alpha} a_{i\alpha}\varphi_{i\alpha}(v) = \sum_{i\alpha} a_{i\alpha} v_i f_\alpha, \tag{4.36}$$

mais comme les f_α forment une base, chaque terme de la somme sur α est nul :

$$\sum_i a_{i\alpha} v_i = 0. \tag{4.37}$$

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.
□

4.2.2 Linéarité et bases

Proposition 4.35 ([64]).
Soient deux espaces vectoriels E et F. Une application linéaire[14] *$f\colon E \to F$ 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. □

Proposition 4.36 ([64]).
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.

14. Définition 4.24.

(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 scalaires[15] tels que $\sum_{j\in J} \lambda_j f(v_j) = 0$. La linéarité de f donne[16]

$$f\big(\sum_{i\in J} \lambda_j v_j\big) = 0. \tag{4.38}$$

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 $j \in J$.

(2) Soit $y \in F$. Vu que f est surjective, il existe $x \in E$ tel que $f(x) = y$. Étant donné que $\{v ß\}_{i\in I}$ est générateur, il existe une partie finie $J \subset I$ et des scalaires $\lambda_j \in \mathbb{K}$ tels que

$$x = \sum_{j\in J} \lambda_j v_j. \tag{4.39}$$

En appliquant f aux deux côtés, et en tenant compte de la linéarité de f,

$$y = f(x) = \sum_{j\in J} \lambda_j f(v_j), \tag{4.40}$$

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.

□

Corollaire 4.37 ([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 $f\colon E \to F$. Par la proposition 4.36(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 4.38 et le théorème 4.39 sont valables également en dimension infinie ; ce sera une des rares incursions en dimension infinie de ce chapitre.

Proposition-définition 4.38.
*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 $f\colon E \to F$. 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 4.39 (Théorème du rang)**.**
Soient E et F deux espaces vectoriels (de dimensions finies ou non) et soit $f\colon E \to F$ une application linéaire.

Si $(u_s)_{s\in S}$ est une base de $\ker(f)$ *et si $\big(f(v_t)\big)_{t\in T}$ est une base de* $\mathrm{Image}(f)$ *alors*

$$(u_s)_{s\in s} \cup (v_t)_{t\in T} \tag{4.41}$$

15. Des éléments du corps de base $\mathbb{K}$.
16. Voir les propriétés de la définition 4.24.

est une base de E.

En dimension finie, nous avons en plus la formule suivante :

$$\operatorname{rang}(f) + \dim \ker f = \dim E, \tag{4.42}$$

c'est-à-dire que le rang[17] *de f est égal à la codimension*[18] *du noyau.*

Démonstration. Nous devons montrer que

$$(u_s)_{s\in S} \cup (v_t)_{t\in T} \tag{4.43}$$

est libre et générateur.

Soit $x \in E$. Nous définissons les nombres x_t par la décomposition de $f(x)$ dans la base $\big(f(v_t)\big)$:

$$f(x) = \sum_{t\in T} x_t f(v_t). \tag{4.44}$$

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) :

$$x - \sum_t x_t v_t = \sum_{s\in S} x_s u_s. \tag{4.45}$$

Par conséquent

$$x = \sum_s x_s u_s + \sum_t x_t v_t. \tag{4.46}$$

En ce qui concerne la liberté nous écrivons

$$\sum_t x_t v_t + \sum_s x_s u_s = 0. \tag{4.47}$$

En appliquant f nous trouvons que

$$\sum_t x_t f(v_t) = 0 \tag{4.48}$$

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 $x_s = 0$. □

Un exemple d'utilisation de ce théorème en dimension infinie sera donné dans le cadre du théorème de Fréchet-Riesz, théorème 26.17.

Proposition 4.40 ([65])**.**
Soit E, un espace vectoriel de dimension finie sur le corps $\mathbb{K}$. Soient V et W des sous-espaces vectoriels de E. Alors

$$\dim(V + W) = \dim(V) + \dim(W) - \dim(V \cap W). \tag{4.49}$$

Démonstration. Nous considérons l'application

$$\begin{aligned} \varphi\colon V \times W &\to E \\ (x, y) &\mapsto x + y. \end{aligned} \tag{4.50}$$

C'est une application linéaire dont l'image est $V + W$. Nous avons donc, pour commencer

$$\dim(V + W) = \dim\big(\operatorname{Image}(\varphi)\big). \tag{4.51}$$

17. Définition 4.38.
18. Définition 4.17.

Nous appliquons à présent le théorème du rang 4.39 à l'application φ :

$$\begin{aligned}\dim(V+W) &= \dim\big(\text{Image}(\varphi)\big) && \text{(4.52a)}\\ &= \dim(V\times W) - \dim\big(\ker(\varphi)\big) && \text{(4.52b)}\\ &= \dim(V) + \dim(W) - \dim\big(\ker(\varphi)\big). && \text{(4.52c)}\end{aligned}$$

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

$$\ker(\varphi) = \{(x,-x) \text{ tel que } x\in V\cap W\}. \tag{4.53}$$

Nous montrons à partir de cela que $\dim\big(\ker(\varphi)\big) = \dim(V\cap W)$ en montrant que l'application

$$\begin{aligned}\psi\colon V\cap W &\to \ker(\varphi)\\ x &\mapsto (x,-x)\end{aligned} \tag{4.54}$$

est un isomorphisme d'espaces vectoriels. D'abord ψ est injective parce que si $\psi(x)=\psi(y)$, alors $(x,-x)=(y,-x)$ 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 $\dim\big(\ker(\varphi)\big)=\dim(V\cap W)$. □

Corollaire 4.41.
Soient deux espaces vectoriels E et F de même dimensions finies[19]*. Pour une application linéaire $f\colon E\to F$, les trois conditions suivantes sont équivalentes :*

(1) f est injective ;
(2) f est surjective ;
(3) f est bijective.

Démonstration. Si un endomorphisme $f\colon E\to E$ est surjectif, alors $\text{rang}(f)=\dim(E)$, ce qui donne, par le théorème du rang 4.39, $\dim\big(\ker(f)\big)=0$, c'est-à-dire que f est injectif.

De la même façon, si f est injective, alors $\dim\big(\ker(f)\big)=0$, ce qui donne $\text{rang}(f)=\dim(E)$ ou encore que f est surjective. □

Exemple 4.42
Le corollaire 4.41 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 $k\geqslant 2$. Cette application est surjective mais pas injective. △

Une conséquence du théorème du rang est que les endomorphismes ont un inverse à gauche et à droite égaux (lorsqu'ils existent).

Corollaire 4.43.
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) ils 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 corollaire 4.41. 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] □

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 1.34 (2), à ceci près que nous devions montrer l'existence de l'inverse à droite.

C'est ce corollaire qui nous permet d'écrire f^{-1} sans plus de précisions dès que f est une bijection.

Exemple 4.44(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

$$f(e_k) = e_{k+1}. \tag{4.55}$$

Il est injectif, mais pas surjectif. Si on pose

$$g(e_k) = \begin{cases} e_{k-1} & \text{si } k \geqslant 1 \\ 0 & \text{si } k = 0 \end{cases} \tag{4.56}$$

alors nous avons $gf = \mathrm{Id}$, mais pas $fg = \mathrm{Id}$ parce que ce $(fg)(e_0) = 0$. △

Lemme 4.45.
Si E et F sont des espaces vectoriels et si $f\colon E \to F$ 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,

$$f\big(f^{-1}(x) + f^{-1}(y)\big) = f\big(f^{-1}(x)\big) + f\big(f^{-1}(y)\big) = x + y. \tag{4.57}$$

De la même façon,

$$f\big(\lambda f^{-1}(x)\big) = \lambda x, \tag{4.58}$$

donc $f^{-1}(\lambda x) = \lambda f^{-1}(x)$. □

Proposition 4.46.
Soient un espace vectoriel E de dimension finie, un endomorphisme $f\colon E \to E$ 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

$$x = \sum_j \lambda_j f(v_j) = f\Big(\sum_j \lambda_j v_j\Big), \tag{4.59}$$

ce qui prouve que f est surjective. Le corollaire 4.41 nous dit alors que f est une bijection. L'application inverse est également linéaire par le lemme 4.45.

Une application linéaire bijective (comme f^{-1}) transforme une base en une base par la proposition 4.36. Donc

$$f^{-1}\big(\{f(v_i)\}\big) \tag{4.60}$$

est une base. □

Proposition 4.47.
Soit un espace vectoriel E de dimension finie et deux applications linéaires $f, g\colon E \to E$ telles que $g \circ f = \mathrm{Id}$. Alors f et g sont bijectives.

Démonstration. En plusieurs étapes
f est injective Si $f(x) = f(y)$, alors en appliquant g nous avons

$$g\big(f(x)\big) = g\big(f(y)\big), \tag{4.61}$$

ce qui donne $x = y$.
f est surjective C'est maintenant le corollaire 4.41.
g est surjective Pour tout $x \in E$ nous avons $g\big(f(x)\big) = x$. Donc l'image de $f(E)$ par g est E.
g est injective C'est maintenant le corollaire 4.41.

□

4.2.4 Injection, surjection

Définition 4.48.
*Une application $S : \mathbb{R}^m \to \mathbb{R}^n$ est dite **affine** si elle est la somme d'une application linéaire et d'une application constante. Autrement dit, S est affine s'il existe $T : \mathbb{R}^m \to \mathbb{R}^n$, linéaire, telle que $S(x) - T(x)$ soit un vecteur constant dans $\mathbb{R}^n$.*

Exemple 4.49
Les exemples les plus courants d'applications affines sont les droites et les plans ne passant pas par l'origine.

Les droites Une droite dans $\mathbb{R}^2$ (ou $\mathbb{R}^3$) qui ne passe pas par l'origine est l'image d'une fonction de la forme $s(t) = ut + v$, avec $t \in \mathbb{R}$, et u et v dans $\mathbb{R}^2$ ou $\mathbb{R}^3$ selon le cas.

En choisissant des coordonnées adéquates, les droites peuvent être aussi vues comme graphes de fonctions affines. Dans le cas de $\mathbb{R}^2$, on retrouve la fonction de l'exemple 4.27, pour $n = m = 1$.

Les plans De la même façon nous savons que tout plan qui ne passe pas par l'origine dans $\mathbb{R}^3$ est le graphe d'une application affine, $P(x, y) = (a, b)^T \cdot (x, y)^T + (c, d)^T$, lorsque les coordonnées sont bien choisies.

△

Lemme 4.50 ([66])**.**
Soit une application linéaire $f : E \to F$.

(1) L'application f est injective si et seulement s'il existe $g : F \to E$ telle que $g \circ f = \mathrm{Id}\,|_E$.

(2) L'application f est surjective si et seulement s'il existe $g : F \to E$ telle que $f \circ g = \mathrm{Id}\,|_F$.

Démonstration. Nous démontrons séparément les deux affirmations.

(1) Si f est injective, alors $f : E \to \mathrm{Image}(f)$ est un isomorphisme. Si V est un supplémentaire de $\mathrm{Image}(f)$ dans F (c'est-à-dire $F = \mathrm{Image}(f) \oplus V$) alors nous pouvons poser $g(x+v) = f^{-1}(x)$ où $x + v$ est la décomposition (unique) d'un élément de F en $x \in \mathrm{Image}(f)$ et $v \in V$. Avec cela nous avons bien $g \circ f = \mathrm{Id}$.

Inversement, s'il existe $g : F \to E$ telle que $g \circ f = \mathrm{Id}$ alors $f : E \to E$ 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

$$\begin{aligned} g : F &\to E \\ \sum_k a_k f(x_k) &\mapsto \sum_k a_k x_k. \end{aligned} \tag{4.62}$$

Cela donne $f \circ g = \mathrm{Id}\,|_F$ parce que si $v \in F$ alors $v = \sum_k v_k f(x_k)$ avec $v_k \in \mathbb{K}$, et nous avons

$$(f \circ g)(v) = \sum_k v_k (f \circ g)\big(f(x_k)\big) = f\left(\sum_k v_k x_k\right) = \sum_k v_k f(x_k) = v. \tag{4.63}$$

Inversement, s'il existe $g : F \to E$ tel que $f \circ g = \mathrm{Id}$ alors f doit être surjective parce que

$$F = \mathrm{Image}(f \circ g) = f\big(\mathrm{Image}(g)\big) \subset \mathrm{Image}(f). \tag{4.64}$$

□

4.3 Matrices

Les matrices et les applications linéaires sont deux choses différentes. Une application linéaire [21] 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.

4.3.1 Définitions

Définition 4.51.
Soit un anneau $\mathbb{A}$ ainsi que des entiers m, n strictement positifs. L'ensemble $\mathbb{M}(n \times n, \mathbb{A})$ est l'ensemble des applications

$$\{1, \dots, n\} \times \{1, \dots, m\} \to \mathbb{A}, \tag{4.65}$$

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 4.52.
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.*

(2) Si $n = 1$, alors la matrice est appelée ***matrice-ligne****.*

(3) Si $m = 1$, alors la matrice est appelée ***matrice-colonne****.*

4.53.
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 4.54.
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 3.61).

Lemme-définition 4.55.
Avec la multiplication

$$\begin{aligned} \mathbb{M}(n \times p, \mathbb{A}) \times \mathbb{M}(p \times m, \mathbb{A}) &\to \mathbb{M}(n \times m, \mathbb{A}) \\ (A, B) &\mapsto (AB)_{ij} = \sum_{k=1}^{p} A_{ik} B_{kj}, \end{aligned} \tag{4.66}$$

l'espace $\mathbb{M}(n, \mathbb{K})$ est une $\mathbb{K}$-algèbre [22].

Définition 4.56.
Pour un élément $A \in \mathbb{M}(n \times m, \mathbb{A})$ nous définissons encore

La transposée $A^t_{ij} = A_{ji}$,

La trace $\mathrm{Tr}(A) = \sum_i A_{ii}$.

21. Définition 4.24.
22. Définition 3.71.

Remarque 4.57.
Quelque 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 4.118.
Ici nous avons bien défini la transposée d'une matrice, pas d'une application linéaire.

Remarque 4.58.
Quelque 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
$$\mathbb{1}_{ij} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{sinon.} \end{cases} \tag{4.67}$$
Il est vite vu que si A est une matrice carrée d'ordre n, alors $A\mathbb{1} = \mathbb{1}A = A$.

Lemme 4.59 ([1])**.**
Si A, B et C sont des matrices nous avons

(1) $(AB)^t = B^t A^t$,

(2) $\mathrm{Tr}(ABC) = \mathrm{Tr}(CAB)$.

Démonstration. La première est un simple calcul :
$$(AB)^t_{ij} = (AB)_{ji} = \sum_k A_{jk}B_{ki} = \sum_k A^t_{kj}B^t_{ik} = (B^tA^t)_{ij}. \tag{4.68}$$
Pour la seconde :
$$\mathrm{Tr}(ABC) = \sum_{ikl} A_{ik}B_{kl}C_{li} = \sum_{ikl} C_{li}A_{ik}B_{kl} = \sum_l (CAB)_{ll} = \mathrm{Tr}(CAB). \tag{4.69}$$
□

4.60.
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 11.209.

4.3.2 Application linéaire associée

Soient deux espaces vectoriels de dimension finie E, F sur le corps $\mathbb{K}$. Nous considérons les bases[23] $\{e_i\}$ pour E et $\{f_\alpha\}$ pour F.

Définition 4.61.
Nous considérons l'application
$$\begin{aligned} \psi\colon \mathbb{M}(n \times m, \mathbb{K}) &\to \mathcal{L}(E, F) \\ A &\mapsto f_A \end{aligned} \tag{4.70}$$

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.

où f_A est définie par

$$f_A(x) = \sum_{i\alpha} A_{\alpha i} x_i f_\alpha \tag{4.71}$$

si x_i sont les coordonnées de $x \in E$ dans la base $\{e_i\}$.

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.

À cette application ψ il manque cependant une propriété importante : elle n'est pas canonique. Elle dépend des bases choisies. Autrement dit : nous avons a priori autant d'applications ψ différentes qu'il y a de choix de bases sur E et F[24].

Nous allons prouver maintenant quelque 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.

4.62.
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

$$(Ax)_i = \sum_j A_{ij} x_j. \tag{4.72}$$

Autrement dit, $Ax = f_A(x)$.

Cette convention et de nombreuses autres à propos de matrice sera rappelée dans 11.11.

Proposition 4.63.
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

$$\begin{aligned} \psi\colon \mathbb{M}(n \times m, \mathbb{K}) &\to \mathcal{L}(E, F) \\ A &\mapsto f_A \end{aligned} \tag{4.73}$$

où f_A est définie par

$$f_A(x) = \sum_{i\alpha} A_{\alpha i} x_i f_\alpha \tag{4.74}$$

si x_i sont les coordonnées de $x \in E$ dans la base $\{e_i\}$.

Alors

(1) Nous avons

$$f_A(e_i)_\alpha = A_{\alpha i}. \tag{4.75}$$

(2) L'application ψ est une bijection.

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

$$f_A(e_j) = \sum_{i\alpha} A_{\alpha i} (e_j)_i f_\alpha = \sum_\alpha A_{\alpha j} f_\alpha, \tag{4.76}$$

donc $f_A(e_i)_\alpha = A_{\alpha i}$. Cela prouve la formule du point (1).

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

$$f_A(x) = \sum_{i\alpha} A_{\alpha i} x_i f_\alpha = \sum_{i\alpha} f(e_i)_\alpha x_i f_\alpha = \sum_\alpha f(\sum_i x_i e_i)_\alpha f_\alpha = \sum_\alpha f(x)_\alpha f_\alpha = f(x). \tag{4.77}$$

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.

□

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 4.64 ([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 $\{f_\alpha\}_{\alpha\in 1,\dots,m}$.

L'application déjà définie[25]

$$\psi\colon \mathbb{M}(m\times n,\mathbb{K})\to\mathcal{L}(E,F) \tag{4.78}$$

est un isomorphisme d'espaces vectoriels.

Démonstration. Le fait que ψ soit une bijection est la proposition 4.63. Nous devons montrer que c'est linéaire.

Pour $\lambda\in\mathbb{K}$ nous avons le calcul

$$\psi(\lambda A)(e_k)=f_{\lambda A}(e_k)=\sum_{\alpha i}(\lambda A)_{\alpha i}\underbrace{(e_k)_i}_{=\delta_{ki}}f_\alpha=\lambda\sum_\alpha A_{\alpha k}f_\alpha=\lambda f_A(e_j). \tag{4.79}$$

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 4.65.
Soient des espaces vectoriels E, F et G de dimensions n, m et p munis de bases[26] *$\{e_i\}$, $\{f_i\}$ et $\{g_i\}$. Nous considérons les deux applications*

$$\psi\colon \mathbb{M}(m\times n,\mathbb{K})\to\mathcal{L}(E,F) \tag{4.80}$$

et

$$\psi\colon \mathbb{M}(p\times m,\mathbb{K})\to\mathcal{L}(F,G). \tag{4.81}$$

Nous avons

$$f_A\circ f_B=f_{AB} \tag{4.82}$$

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 : $f_A\colon F\to G$ et $f_B\colon E\to F$ et la composée $f_A\circ f_B\colon E\to G$. Et puis c'est le calcul :

$$\begin{aligned}
(f_A\circ f_B)(e_k)&=f_A\Big(\sum_{ij}B_{ij}(e_k)_jf_i\Big) && \text{(4.83a)}\\
&=\sum_i B_{ik}f_A(f_i) && \text{(4.83b)}\\
&=\sum_i B_{ik}\sum_{rs}A_{rs}(f_i)_sg_r && \text{(4.83c)}\\
&=\sum_{ir}B_{ik}A_{ri}g_r && \text{(4.83d)}\\
&=\sum_r(AB)_{rk}g_r && \text{(4.83e)}\\
&=f_{AB}(e_k). && \text{(4.83f)}
\end{aligned}$$

Donc $f_A\circ f_B=f_{AB}$ comme il se doit. □

Nous pouvons particulariser au cas où $E=F=G$.

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.

Proposition 4.66.
Si E est un espace vectoriel muni d'une base $\{e_i\}$, alors l'application

$$\psi\colon \mathbb{M}(n,\mathbb{K}) \to \mathrm{End}(E) \tag{4.84}$$

est un isomorphisme d'algèbre[27] *et d'anneaux*[28].

Démonstration. Le fait que ψ soit un isomorphisme d'algèbre est juste la combinaison entre les proposition 4.64 et 4.65.

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 $\psi(\delta) = \mathrm{Id}$. Juste un calcul :

$$f_\delta(x) = \sum_{ij} \delta_{ij} x_j e_i = \sum_i x_i e_i = x. \tag{4.85}$$

Donc oui, f_δ est l'identité. □

Voila. 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 $\mathrm{End}(\mathbb{K}^n)$ qui est un isomorphisme d'anneaux et d'algèbres.

Nous verrons que ce ψ respecte encore les inverses[29] et les déterminants[30].

4.67.
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 certains propriétés.

Cependant si les espaces vectoriels E et F sont munis de bases, alors il y a une application

$$\psi\colon \mathbb{M}(m \times n,\mathbb{K}) \to \mathcal{L}(E,F) \tag{4.86}$$

qui a toutes les propriétés imaginables[31].

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'une[32].

4.3.3 Déterminant

Définition 4.68.
Si $A \in \mathbb{M}(n,\mathbb{K})$ nous définissons le ***déterminant*** *de A par la formule*

$$\det(A) = \sum_{\sigma\in S_n} (-1)^\sigma \prod_{i=1}^{n} A_{i\sigma(i)} \tag{4.87}$$

27. Définition 3.71.
28. Définition 1.38
29. Proposition 4.84.
30. Proposition 11.53.
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.

où la somme est effectuée sur tous les éléments du groupe symétrique[33] 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

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - cb. \tag{4.88}$$

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

$$\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12} \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13} \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}. \tag{4.89}$$

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 4.69 ([1])**.**
Si A *et* B *sont des matrices, alors*

$$(AB)^t = B^t A^t. \tag{4.90}$$

Démonstration. Il suffit de calculer les éléments de matrice :

$$(AB)^t_{ij} = (AB)_{ji} = \sum_k A_{jk} B_{ki} = \sum_k B^t_{ik} A^t_{kj} = (B^t A^t)_{ij}. \tag{4.91}$$

□

Lemme 4.70 ([1, 67])**.**
Si A *est une matrice, alors* $\det(A) = \det(A^t)$*.*

Démonstration. Nous commençons par écrire la définition du déterminant :

$$\det(A^t) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^{n} (A^t)_{i,\sigma(i)} = \sum_\sigma \epsilon(\epsilon) \prod_i A_{\sigma(i),i}. \tag{4.92}$$

Pour chaque σ séparément, nous utilisant la proposition 1.58 pour ré-indexer le produit :

$$\prod_i A_{\sigma(i),i} = \prod_i A_{i,\sigma^{-1}(i)}. \tag{4.93}$$

33. Pour le groupe symétrique, c'est la définition 2.60, le fait que ce soit un groupe fini est le lemme 2.62, et pour la somme sur un groupe fini c'est la définition 1.56..

Nous profitons du fait que l'application $\varphi\colon S_n \to S_n$ donnée par $\varphi(\sigma) = \sigma^{-1}$ soit une permutation de S_n pour appliquer la définition 1.56 et faire la somme sur σ^{-1} :

$$\det(A^t) = \sum_\sigma \epsilon(\sigma) \prod_i A_{i,\sigma^{-1}(i)} = \sum_\sigma \epsilon(\sigma^{-1}) \prod_i A_{i,\sigma(i)} = \det(A) \tag{4.94}$$

où nous avons utilisé le fait que $\epsilon(\sigma^{-1}) = \epsilon(\sigma)$ (corollaire 2.74). □

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 4.71 ([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 :

$$C_{ij} = \begin{cases} (A^t)_{ij} & \text{si } j \neq k, j \neq l \\ (A^t)_{ik} & \text{si } j = l \\ (A^t)_{il} & \text{si } j = k \end{cases} = \begin{cases} A_{ji} & \text{si } j \neq k, j \neq l \\ A_{ki} & \text{si } j = l \\ A_{li} & \text{si } j = k. \end{cases} \tag{4.95}$$

Ensuite nous prouvons que $C^t = B$ en écrivant les éléments de C^t :

$$(C^t)_{ij} = C_{ji} = \begin{cases} A_{ij} & \text{si } i \neq k, i \neq l \\ A_{kj} & \text{si } i = l \\ A_{lj} & \text{si } i = k. \end{cases} \tag{4.96}$$

Cette dernière expression est la matrice A après permutation des lignes $L_k \leftrightarrow L_l$, c'est-à-dire a matrice B. □

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

$$(E_{ij})_{kl} = \delta_{ik}\delta_{jl}. \tag{4.97}$$

Proposition 4.72 (Permuter des lignes ou des colonnes $L_k \leftrightarrow L_l$[68, 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

$$\det(A) = -\det(B). \tag{4.98}$$

(2) Si B est la matrice obtenue à partir de A par la permutation de lignes $L_k \leftrightarrow L_l$. Alors

$$B = SA \tag{4.99}$$

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

$$\det(SA) = \det(S)\det(A). \tag{4.100}$$

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 2.60). Nous avons

$$B_{ij} = A_{i\alpha(j)}, \tag{4.101}$$

ou encore : $A_{ij} = B_{i\alpha(j)}$. Par définition,

$$\det(A) = \sum_{\sigma\in S_n} \epsilon(\sigma) \prod_{i=1}^{n} A_{i\sigma(i)} \tag{4.102}$$

C'est le moment d'utiliser la proposition 1.57 à propos de somme sur des groupes avec $G = S_n$, $h = \alpha$ et

$$f(\sigma) = \epsilon(\sigma) \prod_i A_{i,\sigma(i)}. \tag{4.103}$$

Nous savons que $\epsilon(\alpha) = -1$ et que ϵ est un homomorphisme par la proposition 2.73(1), donc

$$f(\alpha\sigma) = \epsilon(\alpha\sigma) \prod_i A_{i,(\alpha\sigma)(i)} = -\epsilon(\sigma) \prod_i B_{i,\sigma(i)}. \tag{4.104}$$

Avec ça, nous concluons :

$$\det(A) = \sum_{\sigma\in S_n} f(\sigma) = \sum_{\sigma} f(\alpha\sigma) = -\sum_{\sigma\in S_n} \epsilon(\sigma) \prod_{i=1}^{n} B_{i\sigma(i)} = -\det(B). \tag{4.105}$$

(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 4.71 nous dit que $C^t = B'$. En utilisant le lemme 4.70 sur le déterminant de la transposée,

$$\det(B') = \det(C^t) = \det(C) = -\det(A^t) = -\det(A). \tag{4.106}$$

Voila 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 :

$$(SA)_{ij} = \sum_m S_{im}A_{mj} = A_{ij} + \sum_m (\delta_{ki}\delta_{lm} + \delta_{li}\delta_{lm} - \delta_{ki}\delta_{km} - \delta_{li}\delta_{lm})A_{mj} \tag{4.107a}$$

$$= A_{ij} + \delta_{ki}A_{lj} + \delta_{li}A_{kj} - \delta_{ki}A_{kj} - \delta_{li}A_{lj}. \tag{4.107b}$$

Si $i \neq j$ et $i \neq l$, alors $(SA)_{ij} = A_{ij}$. Si $i = k$, alors

$$(SA)_{kj} = A_{kj} + A_{lj} - A_{kj} = A_{lj}, \tag{4.108}$$

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,

$$\det(S) = \sum_{\sigma\in S_n} \epsilon(\sigma) \prod_{i=1}^{n} S_{i\sigma(i)} \tag{4.109a}$$

$$= \sum_{\sigma} \epsilon(\sigma) \prod_i \left(\delta_{i\sigma(i)} + \delta_{ki}\delta_{l\sigma(i)} + \delta_{li}\delta_{k\sigma(i)} - \delta_{ki}\delta_{k\sigma(i)} - \delta_{li}\delta_{l\sigma(i)}\right). \tag{4.109b}$$

Nous utilisons l'associativité et la commutativité du produit pour séparer les facteurs $i = k$ et $i = l$ des autres :

$$\det(S) = \sum_{\sigma} \epsilon(\sigma) \prod_{\substack{i\neq k\\ i\neq l}} \delta_{i\sigma(i)}(\delta_{k\sigma(k)} + \delta_{l\sigma(k)} - \delta_{k\sigma(k)})(\delta_{l\sigma(l)} + \delta_{k\sigma(l)} - \delta_{l\sigma(l)}). \tag{4.110}$$

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 $\sigma = \mathrm{Id}$ et la permutation $\sigma = (k, l)$. Pour $\sigma = \mathrm{Id}$, nous avons

$$\prod_{\substack{i\neq k\\ i\neq l}} \delta_{ii}(\delta_{kk} + \delta_{lk} - \delta_{kk})(\delta_{ll} + \delta_{kl} - \delta_{ll}) = 0. \tag{4.111}$$

Dernier espoir : $\sigma = (k, l)$. Pour ce terme nous avons $\epsilon(\sigma) = -1$ et

$$\prod_{\substack{i\neq k\\ i\neq l}} \delta_{ii}(\delta_{kl} + \delta_{ll} - \delta_{kl})(\delta_{lk} + \delta_{kk} - \delta_{lk}) = 1. \tag{4.112}$$

Au final dans $\det(S)$ il n'y a de non nul que le terms $\sigma = (k, l)$ et il vaut -1. Donc

$$\det(S) = -1. \tag{4.113}$$

(4) Il s'agit de mettre bout à bout les points déjà prouvés :

$$\det(SA) = -\det(A) = \det(S)\det(A). \tag{4.114}$$

□

Corollaire 4.73 ([68]).
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 exempe

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}. \tag{4.115}$$

Proposition 4.74 ([68]).
Soient $A \in \mathbb{M}(n, \mathbb{K})$, et $v \in \mathbb{K}^n$. Si B est la matrice A avec la substitution $L_j \to L_j + v$ et C est la matrice A avec la substitution $L_j \to v$, alors

$$\det(B) = \det(A) + \det(C). \tag{4.116}$$

Démonstration. En utilisant l'associativité de la multiplication,

$$\begin{aligned}
\det(B) &= \sum_{\sigma\in S_n} \epsilon(\sigma) \prod_{i=1}^{n} B_{i\sigma(i)} && \text{(4.117a)}\\
&= \sum_{\sigma} \epsilon(\sigma) \big(\prod_{i\neq j} B_{i\sigma(i)}\big) B_{j\sigma(j)} && \text{(4.117b)}\\
&= \sum_{\sigma} \epsilon(\sigma) \big(\prod_{i\neq j} A_{i\sigma(i)}\big)(A_{j\sigma(j)} + v_{\sigma(j)}) && \text{(4.117c)}\\
&= \sum_{\sigma} \epsilon(\sigma) \prod_{i} A_{i\sigma(i)} + \sum_{\sigma} \epsilon(\sigma) \prod_{i\neq j} C_{i\sigma(i)} v_{\sigma(j)} && \text{(4.117d)}\\
&= \det(A) + \sum_{\sigma} \epsilon(\sigma) \prod_{i\neq j} C_{i\sigma(i)} C_{j\sigma(j)} && \text{(4.117e)}\\
&= \det(A) + \det(C). && \text{(4.117f)}
\end{aligned}$$

Justifications :

— 4.117d parce que pour $i \neq j$ nous avons $A_{i\sigma(i)} = C_{i\sigma(i)}$

— 4.117e parce que $v_{\sigma(j)} = C_{j\sigma(j)}$.

□

Proposition 4.75 (Combinaison de lignes ou colonnes $L_k \to L_k + \lambda L_l$[68])**.**
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 $L_k \to L_k + \lambda L_l$ ou $C_k \to C_k + \lambda C_l$, alors

$$\det(A) = \det(B). \tag{4.118}$$

(2) Si B est la matrice A dans laquelle nous avons fait la substitution $L_k \to L_k + \lambda L_l$, alors

$$B = UA \tag{4.119}$$

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

$$\det(UA) = \det(U)\det(A). \tag{4.120}$$

Démonstration. Point par point.

(1) Soit la matrice C obtenue à partir de A par $L_k \to \lambda L_l$. En considérant le vecteur $v = \lambda L_l$, nous sommes dans la situation de la proposition 4.74. Donc

$$\det(B) = \det(A) + \det(C). \tag{4.121}$$

Mais dans la matrice C, nous avons $L_k = \lambda L_l$, ce qui implique $\det(C) = 0$ par le corollaire 4.73. Donc $\det(A) = \det(B)$ comme il se devait.

(2) Encore un calcul :

$$(UA)_{ij} = \sum_m \big(\delta_{im} + \lambda(E_{kl})_{im}\big)A_{mj} = A_{ij} + \lambda\sum_m \delta_{ki}\delta_{lm}A_{mj} = A_{ij} + \lambda\delta_{li}A_{kj}. \tag{4.122}$$

Cela donne, pour $i = k$ la ligne

$$(UA)_{kj} = A_{kj} + \lambda A_{lj}, \tag{4.123}$$

ce qui correspond bien à $L_k \to L_k + \lambda L_l$.

(3) Nous calculons le déterminant de $U = \delta + \lambda E_{kl}$ avec $k \neq l$. Nous avons dans un premier temps :

$$\det(U) = \sum_{\sigma\in S_n} \epsilon(\sigma)\prod_{i=1}^{n}(\delta_{i\sigma(i)} + \lambda\delta_{ki}\delta_{l\sigma(i)}). \tag{4.124}$$

Vu que nous avons toujours $\delta_{ki}\delta_{li} = 0$, le terme $\sigma = \mathrm{Id}$ donne 1.
Pour les $\sigma \neq \mathrm{Id}$, le facteur $\lambda\delta_{ki}\delta_{l\sigma(i)}$ ne s'annulle pas uniquement si $i = k$ et $\sigma(i) = k$. Donc le seul terme non nul autre que $\sigma = \mathrm{Id}$ peut provenir de $\sigma = (k, l)$. Pour ce terme, nous isolons les termes $i = l$ et $i = k$:

$$(\delta_{k\sigma(k)} + \lambda\delta_{kk}\delta_{k\sigma(k)})(\delta_{l\sigma(l)} + \lambda\delta_{kl}\delta_{k\sigma(l)}). \tag{4.125}$$

Le dernier facteur est nul.

(4) En mettant bout à bout les résultats prouvés,

$$\det(UA) = \det(A) = \det(U)\det(A). \tag{4.126}$$

□

Proposition 4.76 (Multiplication par un scalaire d'une ligne ou colonne $L_k \to \lambda L_k$[68])**.**
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) En considérant la matrice $T = \delta + (\lambda - 1)E_{kk}$, nous avons

$$B = TA, \tag{4.127}$$

c'est-à-dire que a matrice T est une matrice de multiplication de ligne par un scalaire.

(3) Nous avons $\det(T) = \lambda$.

(4) Et aussi : $\det(TA) = \det(T)\det(A)$

Démonstration. Point par point.

(1) La matrice B est donnée par les éléments

$$B_{ij} = \begin{cases} A_{ij} & \text{si } j \neq k \\ \alpha A_{ij} & \text{si } j = kn \end{cases} \tag{4.128}$$

c'est-à-dire $B_{ij} = \big(1 + (\alpha - 1)\delta_{jk}\big)A_{ij}$. Nous mettons cela dans la définition du déterminant de B :

$$\det(B) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^{n} B_{i\sigma(i)} = \sum_{\sigma} \prod_{i} \big(1 + (\alpha - 1)\delta_{\sigma(i)k} A_{i\sigma(i)}\big). \tag{4.129}$$

L'associativité du produit dans $\mathbb{K}$ nous permet de séparer le produit de la façon suivante :

$$\prod_{i=1}^{n} \big(1 + (\alpha - 1)\delta_{\sigma(i)k}\big)A_{i\sigma(i)} = \prod_{i} \big(1 + (\lambda - 1)\delta_{\sigma(i)k}\big) \prod_{i} A_{i\sigma(i)} = \lambda \prod_{i} A_{i\sigma(i)}. \tag{4.130}$$

En remettant dans (4.129), nous trouvons $\det(B) = \det(A)$.

(2) C'est un cas particulier de la proposition 4.75(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

$$\det(T) = \sum_{\sigma} \epsilon(\sigma) \prod_{i=1}^{n} \big(\delta_{i\sigma(i)} + (\lambda - 1)\delta_{ki}\delta_{k\sigma(i)}\big). \tag{4.131}$$

Si $i \neq \sigma(i)$, alors non seulement $\delta_{i\sigma(i)} = 0$, mais en plus $\delta_{ki}\delta_{k\sigma(i)} = 0$. Donc suel $\sigma = \mathrm{Id}$ reste dans la somme sur $\sigma \in S_n$. Il reste donc

$$\det(T) = \prod_{i=1}^{n} \big(1 + (\lambda - 1)\delta_{ki}\big) = \left(\prod_{i \neq k} 1\right)\big(1 + (\lambda - 1)\big) = \lambda \tag{4.132}$$

où nous avons utilisé encore l'associativité pour isoler le facteur $i = k$.

(4) Il faut mettre bout à bout les résultats déjà faits :

$$\det(TA) = \lambda \det(A) = \det(T)\det(A). \tag{4.133}$$

□

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 4.72.

— Combinaisons de lignes $L_k \to L_k + \lambda L_l$: $U(n; k, l, \lambda) = \delta + \lambda E_{kl}$, proposition 4.75.

— Multiplication d'une ligne par un scalaire $L_k \to \lambda L_k$: $T = \delta + (\lambda - 1)E_{kk}$, proposition 4.76.

Ces matrices seront dans la suite notées G. Et elles vérifient la grosse propriété

$$\det(GA) = \det(G)\det(A) \tag{4.134}$$

pour toute matrice A.

Proposition 4.77 (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

$$G_1 \dots G_N A = \delta. \tag{4.135}$$

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

$$T(1; 1, \frac{1}{A_{11}})A = \delta \tag{4.136}$$

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 (corollaire 4.73). Il existe donc un k tel que $A_{k1} \neq 0$.

Par la proposition 4.72, la matrice

$$B^{(1)} = S(n + 1; k, 1)A \tag{4.137}$$

est une matrice telle que $B^{(1)}_{11} = A_{k1} \neq 0$. Ensuite, par la proposition 4.76 la matrice

$$B^{(2)} = T(n + 1; 1, \frac{1}{A_{k1}})B^{(1)} \tag{4.138}$$

vérifie $B^{(2)}_{11} = 1$.

Vu que la multiplication par la matrice $U(n+1; k; l; \lambda)$ fait par la proposition 4.75 la substitution $L_k \to L_k + \lambda L_l$, la matrice

$$B^{(3)} = \prod_{k=2}^{n+1} U(n + 1; k, 1, -B^{(1)}_{k1})B^{(1)} \tag{4.139}$$

a toute sa première colonne nulle à l'exception de $B^{(3)}_{11} = 1$.

Nous n'avons pas donné de nom ni démontré de théorèmes à propos de la substitution $C_k \to C_k + \lambda C_l$. En passant éventuellement par les transposées et en utilisant les lemmes 4.69 et 4.70 nous obtenons une matrice $U'(n + 1; k, l, \lambda)$ ayant la propriété que la matrice

$$B^{(4)} = \prod_{k=2}^{n+1} U'(n + 1; k, 1, -B^{(3)}_{1k})B^{(3)} \tag{4.140}$$

vérifie $B^{(4)}_{1j} = B^{(4)}_{j1} = 0$ pour tout j sauf $j = 1$. En d'autres termes, la matrice $B^{(4)}$ est de la forme

$$B^{(4)} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix} \tag{4.141}$$

où A' est une matrice de taille n.

Voyons quelque propriétés de A'. Nous savons que

$$B^{(4)} = \prod_i G_i A \tag{4.142}$$

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

$$\det(B^{(4)}) = \prod_i \det(G_i)\det(A), \tag{4.143}$$

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

$$G'_1 \dots G'_M A' = \delta \tag{4.144}$$

où les G'_i sont de taille n, ainsi que le δ. En remarquant que

$$S(n+1;k,l) = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & S(n;k-1,l-1) & \\ 0 & & & \end{pmatrix}, \tag{4.145}$$

et pareillement pour les matrices T et U, nous voyons qu'en prenant

$$G_i = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & G'_i & \\ 0 & & & \end{pmatrix}, \tag{4.146}$$

nous avons

$$\prod_{i=1}^{M} G_i B^{(3)} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & \prod_{i=1}^{M} G'_i A' & \\ 0 & & & \end{pmatrix} = \delta_{n+1} \tag{4.147}$$

où nous avons mis un indice sur le dernier δ pour être plus explicite. □

Proposition 4.78.
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 Gauss et obtenir des matrices $G_1, \dots, G_{N_1}$ telles que

$$G_1 \dots G_{N_1} A = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A^{(1)} & \\ 0 & & & \end{pmatrix}. \tag{4.148}$$

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

$$G_1 \dots G_N A = \delta, \tag{4.149}$$

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 zéros[34]. □

34. En réalité, le processus tel que nous l'avons décrit ne s'arrête que lorsque la première colonne est remplie de zéros.

4.3.7 Matrices inversibles

Proposition-définition 4.79.
Soit une matrice $A \in \mathrm{M}(n,\mathbb{K})$. Si les matrices B_1 et B_2 de $\mathrm{M}(n,\mathbb{K})$ vérifient

$$AB_1 = B_1A = \delta \tag{4.150}$$

et

$$AB_2 = B_2A = \delta, \tag{4.151}$$

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 1.34. 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 $B_1 = B_2$. □

Lemme 4.80 ([68]).
Si $A \in \mathrm{M}(n,\mathbb{K})$, alors il existe au plus une matrice $B \in \mathrm{M}(n,\mathbb{K})$ telle que $AB = \delta$.

Démonstration. Soient des matrices $B, C \in \mathrm{M}(n,\mathbb{K})$ telles que $AB = AC = \delta$. Nous allons montrer que $B = C$.

Pour cela nous considérons les applications linéaires $f_A, f_B, f_C \in \mathrm{End}(\mathbb{K})$ associées par la proposition 4.63. Vu que $AB = \delta$, par la proposition 4.65, nous avons $f_A \circ f_B = f_{AB} = \mathrm{Id}$. La proposition 4.47 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 4.36. La proposition 4.46 dit alors que $\{f_B(e_i)\}$ est une base. Nous décomposons $f_B(e_k) - f_C(e_k)$ dans cette base :

$$f_B(e_k) - f_C(e_k) = \sum_j \alpha_j f_B(e_j) \tag{4.152}$$

où les α_j dépendent a priori de k. Vu que $f_A \circ (f_B - f_C) = 0$, nous avons

$$0 = f_A\big(f_B(e_k) - f_C(e_k)\big) = \sum_j (f_A \circ f_B)(e_j) = \sum_j \alpha_j e_j. \tag{4.153}$$

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 4.63(2). □

Proposition 4.81 ([68]).
Si $A, B \in \mathrm{M}(n,\mathbb{K})$ 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

$$AC = ABA - A + AB = AB = \delta. \tag{4.154}$$

Donc C est également un inverse à droite de A. Le lemme 4.80 donne alors $C = B$. □

Corollaire 4.82.
Soit $A \in \mathrm{M}(n,\mathbb{K})$. Si il existe $B \in \mathrm{M}(n,\mathbb{K})$ tel que $AB = \delta$, alors A est inversible et son inverse est B.

Démonstration. Il s'agit d'une paraphrase de la proposition 4.81 et de la définition 4.79. □

Lemme 4.83.
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

$$AB(AB^{-1}) = \delta, \tag{4.155}$$

ce qui dirait que $B(AB^{-1})$ serait un inverse de A. □

Proposition 4.84.
Une matrice est inversible si et seulement si son application linéaire associée est inversible. Dans ce cas, nous avons

$$f_A^{-1} = f_{A^{-1}}. \tag{4.156}$$

Démonstration. Dans le sens direct, si A est inversible nous avons $AA^{-1} = \delta$. Donc

$$f_A \circ f_{A^{-1}} = f_{AA^{-1}} = f_\delta = \mathrm{Id} \tag{4.157}$$

où nous avons utilisé la proposition 4.65 pour la composition et la proposition 4.66 pour l'identité. L'égalité (4.157) 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

$$f_\delta = \mathrm{Id} = f_A \circ f_B = f_{AB}. \tag{4.158}$$

Le fait que l'application $\psi\colon A \to f_A$ soit une bijection[35] implique que $AB = \delta$, c'est-à-dire que A est inversible et que $B = A^{-1}$. □

4.3.8 Inversibilité et déterminant

Proposition 4.85.
Une matrice au déterminant non nul est inversible.

Démonstration. Si A est une matrice telle que $\det(A) \neq 0$, alors la proposition 4.77 nous donne des matrices $G_1, \dots, G_N$ telles que

$$G_1 \dots G_N A = \delta. \tag{4.159}$$

Donc la matrice $G_1 \dots G_N$ est un inverse de A par le corollaire 4.82. □

Proposition 4.86.
Si une matrice A a une ligne ou une colonne de zéros, alors

(1) $\det(A) = 0$,

(2) A n'est pas inversible.

Démonstration. Par définition nous avons

$$\det(A) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^{n} A_{i\sigma(i)}. \tag{4.160}$$

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

$$(AB)_{kk} = \sum_l A_{kl} B_{lk}. \tag{4.161}$$

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. □

Proposition 4.87.
Une matrice dont le déterminant est nul n'est pas inversible.

35. Proposition 4.63(2).

Démonstration. Par la proposition 4.78, 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 4.86 implique que la matrice

$$G_1 \dots G_N A \tag{4.162}$$

n'est pas inversible. Vu les déterminants des matrices G_i, la proposition 4.85 implique que $G_1 \dots G_N$ est inversible. Si A était inversible, nous aurions

$$G_1 \dots G_N A A^{-1} (G_1 \dots G_N)^{-1} = \delta, \tag{4.163}$$

c'est-à-dire que $A^{-1}(G_1 \dots G_N)^{-1}$ serait un inverse de la matrice (4.162). Cette dernière n'ayant pas d'inverse, nous concluons que A n'en a pas non plus. □

Théorème 4.88.
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 4.85 et dans l'autre sens c'est la proposition 4.87. □

4.3.9 Quelques ensembles de matrices particuliers

Certains ensembles de matrices ont une importance particulière, que nous développerons plus tard.

Définition 4.89 (Groupe linéaire de matrices)**.**
On note $\mathrm{GL}(n, \mathbb{A})$ *l'ensemble des matrices carrées d'ordre* n *à coefficients dans* $\mathbb{A}$*, qui sont inversibles. En d'autres termes,* $\mathrm{GL}(n, \mathbb{A}) = U(\mathbb{M}(n, \mathbb{A}))$.

Définition 4.90 (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* $\mathrm{O}(n, \mathbb{A})$ *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 4.91.
Soient des matrices $A, B \in \mathbb{M}(n, \mathbb{K})$ *telles que* $\det(A) \neq 0 \neq \det(B)$*. Alors*

$$\det(AB) = \det(A)\det(B). \tag{4.164}$$

Démonstration. La proposition 4.77 nous donne des matrices de permutations de lignes et de colonnes $G_1, \dots, G_N$ et $G'_1, \dots, G'_N$ telles que [36]

$$G_1 \dots G_N A = \delta \tag{4.165a}$$
$$G'_1 \dots G'_N B = \delta. \tag{4.165b}$$

Nous avons

$$(G'_1 \dots G'_N) \underbrace{(G_1 \dots G_N)A}_{=\delta} B = \delta. \tag{4.166}$$

En prenant le déterminant des deux côtés et en tenant compte de (4.134),

$$1 = \det(\delta) = \det\left(G'_1 \dots G'_N G_1 \dots G_N AB\right) = \det(G'_1 \dots G'_N)\det(G_1 \dots G_N)\det(AB). \tag{4.167}$$

Mais en même temps, les équations 4.165 donnent

$$\det(G_1 \dots G_N) = \det(A)^{-1} \tag{4.168a}$$
$$\det(G'_1 \dots G'_N) = \det(B)^{-1}. \tag{4.168b}$$

36. 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.

Cela pour dire que

$$1 = \det(A)^{-1}\det(B)^{-1}\det(AB), \tag{4.169}$$

et donc ce qu'il nous fallait. □

Proposition 4.92.
Soient des matrices $A, B \in \mathbb{M}(n, \mathbb{K})$ telles que $\det(A) = 0$ et $\det(B) \neq 0$. Alors

$$\det(AB) = \det(BA) = \det(A)\det(B). \tag{4.170}$$

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

$$0 = \det(A) = \det(G_1 \dots G_N BA) = \det(G_1 \dots G_N)\det(BA). \tag{4.171}$$

Donc $\det(BA) = 0$. □

Proposition 4.93.
Soient des matrices A et B sur un corps commutatif. Alors

$$\det(AB) = \det(A)\det(B). \tag{4.172}$$

Démonstration. Les propositions 4.91 et 4.92 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 4.88). Le produit AB n'est alors pas inversible non plus [37]. La proposition 4.88, utilisée dans le sens inverse, nous dit alors que $\det(AB) = 0$.

Au final dans le cas $\det(A) = \det(B) = 0$ nous avons $0 = \det(AB) = \det(A)\det(B) = 0$. □

Faisons maintenant le cas général des manipulations de lignes et colonnes.

Proposition 4.94.
Soit une matrice carré $A \in \mathbb{M}(n, \mathbb{K})$. La matrice B obtenue par la substitution simultanée

$$C_j \to \sum_k a_{kj} C_k \tag{4.173}$$

a pour déterminant

$$\det(B) = \det(a)\det(A). \tag{4.174}$$

Démonstration. L'élément B_{ij} de la matrice B est une combinaison linéaire de tous les éléments de sa ligne :

$$B_{ij} = \sum_k a_{kj} A_{ik} = (Aa)_{ij}. \tag{4.175}$$

Donc $B = Aa$. La proposition 4.93 nous dit alors que $\det(B) = \det(a)\det(A)$. □

4.3.11 Transvections

Nous nommons E_{ij} la matrice remplie de zéros sauf à la case ij qui vaut 1. Autrement dit

$$(E_{ij})_{kl} = \delta_{ik}\delta_{jl}. \tag{4.176}$$

Définition 4.95.
*Une **matrice de transvection** est une matrice de la forme*

$$T_{ij}(\lambda) = \mathrm{Id} + \lambda E_{ij} \tag{4.177}$$

avec $i \neq j$.

37. Citez le lemme 4.83 si vous voulez justifier ça.

*Une **matrice de dilatation** est une matrice de la forme*

$$D_i(\lambda) = \mathrm{Id} + (\lambda - 1)E_{ii}. \tag{4.178}$$

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*

$$(P_\sigma)_{ij} = \delta_{i\sigma(j)}. \tag{4.179}$$

Lemme 4.96.
La matrice $T_{ij}(\lambda)A = (\mathbb{1} + \lambda E_{ij})A$ est la matrice A à qui on a effectué la substitution

$$L_i \to L_i + \lambda L_j. \tag{4.180}$$

La matrice $AT_{ij}(\lambda)$ est la substitution

$$C_j \to C_j + \lambda C_i. \tag{4.181}$$

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 $E_{ij}A$:

$$(E_{ij}A)_{kl} = \sum_m (E_{ij})_{km}A_{ml} \tag{4.182a}$$
$$= \sum_m \delta_{ik}\delta_{jm}A_{ml} \tag{4.182b}$$
$$= \delta_{ik}A_{jl}. \tag{4.182c}$$

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

$$A + \lambda E_{ij}A \tag{4.183}$$

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

$$(AE_{ij}) = A_{ki}\delta_{jl}. \tag{4.184}$$

Pour les matrices de permutation, nous avons

$$(AP_\sigma)_{kl} = A_{k\sigma(l)} \tag{4.185}$$

et

$$(P_\sigma A)_{kl} = \sum_m \delta_{k\sigma(m)}A_{ml} = \sum_m \delta_{\sigma^{-1}(k)m}A_{ml} = A_{\sigma^{-1}(k)l}. \tag{4.186}$$

□

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 4.97 ([68]).
*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 4.98 ([69]).
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.

Proposition 4.99.
Le rang d'une matrice est la taille de son plus grand mineur non nul.

Lemme 4.100.
Soit $\mathbb{K}$ un corps commutatif[38]*. 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*

$$f_A(x_i) \neq 0 \tag{4.187}$$

pour $x \leqslant r$ et

$$f_A(x_i) = 0 \tag{4.188}$$

pour $i > r$.

Ici, f_A est l'application linéaire associée à la matrice A par l'application (4.70).

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

$$v_i = f_A(e_i). \tag{4.189}$$

Les vecteurs v_i engendrent V, donc nous pouvons en extraire une base par le théorème 4.15(1). Soit donc $\{v_j\}_{i\in J}$ 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 incomplète[39], mais les vecteurs ainsi complétant la base ne sont pas garantis de s'annuler par f_A. Voir l'exemple 4.101.

L'idée est d'utiliser le noyau de f_A qui est un sous-espace vectoriel par la proposition 4.32. Soit une base[40] $\{z_k\}$ 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 4.39 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. □

Exemple 4.101
Soit la matrice

$$A = \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}. \tag{4.190}$$

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

$$f_A(e_1) = \begin{pmatrix} 1 \\ 2 \end{pmatrix}. \tag{4.191}$$

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

$$f_A(v) = f_A(e_2) = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \neq 0. \tag{4.192}$$

38. Comme toujours.
39. Théorème 4.11(2).
40. Cette base contient $n - r$ éléments, mais ce n'est pas très important pour la suite.

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 $\{e_1, e_1 - e_2\}$. △

Proposition 4.102.
Le rang d'une application linéaire est égal au rang de sa matrice dans n'importe quelle base.

4.3.13 Matrices équivalentes et semblables

Définition 4.103.
Deux relations d'équivalence entre les matrices.

(1) *Deux matrices A et B sont **équivalentes** dans $\mathbb{M}(n,\mathbb{K})$ s'il existe $P, Q \in \mathrm{GL}(n,\mathbb{K})$ telles que $A = PBQ^{-1}$.*

(2) *Deux matrices sont **semblables** s'il existe une matrice $P \in \mathrm{GL}(n,\mathbb{K})$ telle que $A = PBP^{-1}$.*

Lemme 4.104.
Une matrice de rang[41] *r dans $\mathbb{M}(n,\mathbb{K})$ est équivalente à la matrice par blocs*

$$J_r = \begin{pmatrix}\mathbb{1}_r & 0\\ 0 & 0\end{pmatrix}. \tag{4.193}$$

Démonstration. Nous devons prouver que pour toute matrice $A \in \mathbb{M}(n,\mathbb{K})$ de rang r, il existe $P, Q \in \mathrm{GL}(n,\mathbb{K})$ 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 4.100.

Nous considérons la matrice inversible P telle que $Pe_i = f_i$; ses colonnes sont donc précisément les f_i, si bien que

$$APe_i = Af_i = \begin{cases}0 & \text{si } i > r\\ \neq 0 & \text{sinon.}\end{cases} \tag{4.194}$$

La matrice AP se présente donc sous la forme

$$AP = \begin{pmatrix}M & 0\\ * & 0\end{pmatrix} \tag{4.195}$$

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

$$QAPe_i = \begin{cases}e_i & \text{si } i < r\\ 0 & \text{sinon.}\end{cases}. \tag{4.196}$$

Cela signifie que QAP est la matrice J_r. □

Corollaire 4.105 (Équivalence et rang)**.**
Deux matrices sont équivalentes[42] *si et seulement si elles sont de même rang.*

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 4.104, deux matrices de même rang r sont équivalentes à J_r. Elles sont donc équivalentes entre elles.

41. Définition 4.99.
42. Définition 4.103(1).

Inversement, supposons que A et B soient deux matrices équivalentes : $A = PBQ^{-1}$ avec P et Q inversibles. Alors

$$\begin{aligned}\text{Image}(PBQ^{-1}) &= \{PBQ^{-1}v \text{ tel que } v \in \mathbb{K}^n\} && (4.197a)\\ &= PB\underbrace{\{Q^{-1}v \text{ tel que } v \in \mathbb{K}^n\}}_{=\mathbb{K}^n} && (4.197b)\\ &= P\big(B(\mathbb{K}^n)\big). && (4.197c)\end{aligned}$$

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 $P\big(B(\mathbb{K}^n)\big)$ est la même que celle de $B(\mathbb{K}^n)$. Par conséquent

$$\dim\Big(\text{Image}(PBQ^{-1})\Big) = \dim\big(B(\mathbb{K}^n)\big) = \text{rang}(B). \tag{4.198}$$

Le membre de gauche de cela n'est autre que $\text{rang}(A) = \dim\big(\text{Image}(PBQ^{-1})\big)$. □

4.3.14 Algorithme des facteurs invariants

Proposition 4.106 (Algorithme des facteurs invariants[43])**.**
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

$$U = P\begin{pmatrix} d_1 & & & \\ & \ddots & & 0 \\ & & d_s & \\ & 0 & & 0 \end{pmatrix}Q \tag{4.199}$$

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'amenons en $(1, 1)$ par les permutations

$$\begin{aligned}C_1 &\leftrightarrow C_{j_0}\\ L_1 &\leftrightarrow L_{i_0}\end{aligned} \tag{4.200}$$

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

$$u_{i1} = qu_{11} + r_i, \tag{4.201}$$

et nous faisons

$$L_i \to L_i - qL_1, \tag{4.202}$$

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 content [43]. 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}.

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.

43. S'il est zéro, nous passons à la ligne suivante

Une fois la première colonne ramenée à la forme

$$C_1 = \begin{pmatrix} u_{11} \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \tag{4.203}$$

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 [44]

$$U = \begin{pmatrix} u_{11} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A & \\ 0 & & & \end{pmatrix} \tag{4.204}$$

Si l'élément u_{11} ne divise pas un des éléments de A, disons a_{ij}, alors nous faisons

$$C_1 \to C_1 - C_j. \tag{4.205}$$

Cela nous détruit un peu la première colonne, mais ne change pas u_{11}. Nous avons maintnant

$$U = \begin{pmatrix} u_{11} & 0 & \dots & 0 \\ 0 & & & \\ * & & & \\ u_{ij} & & A & \\ * & & & \\ 0 & & & \end{pmatrix} \tag{4.206}$$

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

$$U = \begin{pmatrix} u_{11} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A & \\ 0 & & & \end{pmatrix}, \tag{4.207}$$

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 (4.207) 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

$$U = \begin{pmatrix} u_{11} & & 0 \\ & u_{22} & \\ 0 & & B \end{pmatrix}. \tag{4.208}$$

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 4.96). □

44. Nous nommons toujours par la même lettre U la matrice originale et la modifiée, comme il est d'usage en informatique.

4.4 Espaces de polynômes

Attention : les polynômes en soi sont définis par la définition 3.145.
Pour chaque $k > 0$ donné nous définissons

$$\mathcal{P}^k_{\mathbb{R}} = \{p : \mathbb{R} \to \mathbb{R} \,|\, p : x \mapsto a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k,\ a_i \in \mathbb{R},\ \forall i = 0, \ldots, k\}. \tag{4.209}$$

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 $\mathcal{P}^k_{\mathbb{R}}$ est donc un espace vectoriel muni des opérations héritées de $\mathcal{P}_{\mathbb{R}}$.

La base canonique de l'espace $\mathcal{P}^k_{\mathbb{R}}$ est donné par les monômes $\mathcal{B} = \{x \mapsto x^j \,|\, j = 0, \ldots, k\}$. 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 $\mathcal{P}^k_{\mathbb{R}}$ vers des autres espaces vectoriels

L'isomorphisme canonique $\phi : \mathcal{P}^k_{\mathbb{R}} \to \mathbb{R}^{k+1}$ Nous définissons ϕ par les relations suivantes

$$\phi(x^j) = e_{j+1}, \qquad \forall j \in \{0, \ldots, k\}.$$

Cela veut dire que pour tout p dans $\mathcal{P}^k_{\mathbb{R}}$, avec $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k$, 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 4.107

Soit $k = 5$ on a

$$\phi(-8 - 7x - 4x^2 + 4x^3 + 2x^5) = \begin{pmatrix} -8 \\ -7 \\ -4 \\ 4 \\ 0 \\ 2 \end{pmatrix}. \tag{4.210}$$

△

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 $\mathcal{P}^k_{\mathbb{R}}$ 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 $d : \mathcal{P}^k_{\mathbb{R}} \to \mathcal{P}^{k-1}_{\mathbb{R}}$ L'application de dérivation d fait exactement ce qu'on s'attend d'elle

$$d(x^0) = d(1) = 0, \qquad d(x^j) = j x^{j-1}, \quad \forall j \in \{1, \ldots, k\}.$$

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 4.108
Soit $k = 3$ on a

$$d(-8 - 12x + 4x^3) = -12(1) + 4(3x^2) = -12 + 12x^2. \tag{4.211}$$

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. △

L'intégration $I : \mathcal{P}^k_{\mathbb{R}} \to \mathcal{P}^{k+1}_{\mathbb{R}}$ Nous pouvons définir une application que est «à une constante prés» l'application inverse de la dérivation. Cette application est définie sur les éléments de base par

$$I(x^j) = \frac{x^{j+1}}{j+1}. \tag{4.212}$$

Bien entendu la raison d'être et la motivation de cette définition apparaîtra lorsque nous développerons une théorie générale de l'intégration.

Exemple 4.109
Soit $k = 4$ on a

$$I(6 + 2x + x^2 + x^4) = 6x + x^2 + \frac{x^3}{3} + \frac{x^5}{5}. \tag{4.213}$$

△

Remarquez que, étant donné que dans la définition de I nous avons décidé d'intégrer entre zéro et x, tous les polynômes dans $\mathcal{P}^{k+1}_{\mathbb{R}}$ qui sont l'image par I d'un polynôme de $\mathcal{P}^k_{\mathbb{R}}$ 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 $\mathcal{P}^{k+1}_{\mathbb{R}}$, en particulier $\mathcal{B}_1 = \{x \mapsto x^j \,|\, j = 1, \dots, k\} \subset \mathcal{B}$ 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 12.1.2, nous verrons que toutes les normes ne sont pas équivalentes sur l'espace des polynômes.

4.5 Théorème de Sylvester

Théorème 4.110 (de Sylvester)**.**
Soit Q une forme quadratique réelle de signature (p, q). Alors pour toute base orthonormée on a

$$p = \text{Card}\{i \text{ tel que } Q(e_i) > 0\} \tag{4.214a}$$
$$q = \text{Card}\{i \text{ tel que } Q(e_i) < 0\}. \tag{4.214b}$$

Le rang de Q est $p + q$.

Si A est la matrice de Q dans une base, alors il existe une matrice inversible P telle que

$$P^t A P = \begin{pmatrix} -\mathbb{1}_q & & \\ & \mathbb{1}_p & \\ & & 0 \end{pmatrix}. \tag{4.215}$$

4.6 Dualité

Proposition 4.111.
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 4.112.
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 12.25, la remarque 12.36 et la définition 12.38.

Définition 4.113.
Si E est un espace vectoriel et si $\{e_i\}$ est une base de E, alors nous définissons la ***base duale*** *de E^* par*

$$e_i^*(e_j) = \delta_{ij} \tag{4.216}$$

est sa prolongation par linéarité.

Notons que si $v \in E$ est un vecteur, ça n'a aucun sens a priori de parler de v^*. Il s'agit bien de définir *toute* la base $\{e_i^*\}$ à partir de toute la base $\{e_i\}$.

4.6.1 Orthogonal

Définition 4.114.
*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*

$$F^\perp = \{\alpha \in E^* \text{ tel que } \forall x \in F, \alpha(x) = 0\}. \tag{4.217}$$

Cette définition d'orthogonal via le dual n'est pas du pur snobisme. En effet, la définition « usuelle » qui ne parle pas de dual,

$$F^\perp = \{y \in E \text{ tel que } \forall x \in F, y \cdot x = 0\}, \tag{4.218}$$

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 4.114, au contraire, est intrinsèque : elle ne dépend que de la structure d'espace vectoriel.

Si $B \subset E^*$, on note B^o son orthogonal :

$$B^o = \{x \in E \text{ tel que } \omega(x) = 0 \, \forall \omega \in B\}. \tag{4.219}$$

Notons qu'on le note B^o 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 4.115.
Soient un espace vectoriel E et un sous-espace vectoriel F. Nous avons

$$\dim F + \dim F^\perp = \dim E. \tag{4.220}$$

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 $i \leqslant p$ et si $k \geqslant 1$, 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 $i \leqslant p$. Donc $\omega = \sum_{k=p+1}^n \omega_k e_k^*$. □

La proposition 12.114 donnera une version plus terre à terre de la proposition 4.115 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 $t\colon E \to E$ est une application linéaire, de dire que sa transposée soit l'application linéaire $t^t\colon E \to E$ 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 $\langle x, Ay\rangle = \langle A^t x, y\rangle$.

Hélas nous allons voir que cette façon de définir une transposée est mauvaise.

Soit une application linéaire $t\colon E \to E$ 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

$$t_1(e_i)_j = \sum_k (A^t)_{jk}(e_i)_k = A^t_{ji} = A_{ij}. \tag{4.221}$$

Pour calculer $t_2(e_i)_j$, c'est un peu plus laborieux :

$$t_2(e_i) = \sum_\alpha Q^{-1}_{\alpha i} t_2(f_\alpha) = \sum_{\beta\gamma\alpha} Q^{-1}_{\alpha i} B^t_{\gamma\beta} \underbrace{(t_\alpha)_\beta}_{\delta_{\alpha\beta}} f_\gamma = \sum_{\beta\gamma} Q^{-1}_{\beta i} B^t_{\gamma\beta} f_\gamma \tag{4.222a}$$

$$= (B^t Q^{-1})_{\gamma i} Q_{j\gamma} e_j \tag{4.222b}$$

$$= \sum_j (QB^tQ^{-1})_{ji} e_j. \tag{4.222c}$$

Donc $t_2(e_i)_j = (QB^tQ^{-1})_{ji}$. En tenant compte du fait que $B = Q^{-1}AQ$ nous avons

$$t_2(e_i)_j = (QQ^tA^t(Q^{-1})^tQ^{-1})_{ji}. \tag{4.223}$$

Cela est égal à l'expression (4.221) 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 4.116([33])
Soit la base canonique $\{e_1, e_2\}$ de $\mathbb{R}^2$. Nous considérons l'application linéaire $t\colon \mathbb{R}^2 \to \mathbb{R}^2$ définie par

$$t(e_1) = e_1 \tag{4.224a}$$

$$t(e_2) = 0. \tag{4.224b}$$

La matrice de t dans cette base est

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}. \tag{4.225}$$

Elle est symétrique : elle vérifie $A^t = A$. Si nous comptions 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

$$t(f_2) = t(e_1) + t(e_2) = e_1 = f_1. \tag{4.226}$$

Donc la matrice de t dans cette base est

$$B = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}. \tag{4.227}$$

Et là, nous avons $B^t \neq B$. Donc en comptant sur cette base pour définir la transposée de t nous aurions $t^t \neq t$. △

4.117.
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 11.80.

4.6.3 Transposée : la bonne approche

Définition 4.118.
Si $f\colon E \to F$ est une application linéaire entre deux espaces vectoriels, la ***transposée*** *est l'application $f^t\colon F^* \to E^*$ donnée par*

$$f^t(\omega)(x) = \omega\big(f(x)\big). \tag{4.228}$$

pour tout $\omega \in F^*$ et $x \in E$.

Lemme 4.119.
Soit E muni de la base $\{e_i\}$ et F muni de la base $\{g_i\}$ et une application $f\colon E \to F$. 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,

$$f^t(g_i^*) = \sum_j (f^t)_{ij} e_j^*, \tag{4.229}$$

et

$$f(e_k) = \sum_l A_{kl} g_l. \tag{4.230}$$

Du coup, si $x = \sum_k x_k e_k$, nous avons

$$f^t(g_i^*)x = \sum_{kl} x_k g_i^* A_{kl} g_l = \sum_{kl} x_k A_{kl} \delta_{il} = \sum_k x_k A_{ki} = \sum_k (A^t)_{ik} x_k. \tag{4.231}$$

D'autre part,

$$\sum_k (A^t)_{ik} g_k^* x = \sum_{kl} (A^t)_{ik} g_k^* x_l e_l = \sum_k (A^t)_{ik} x_k. \tag{4.232}$$

Le fait que (4.231) et (4.232) donnent le même résultat prouve le lemme. □

En corollaire, 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 4.120 (Gilles Dubois)**.**
Si $f\colon E \to F$ est une application linéaire, alors

$$\operatorname{rang}(f) = \operatorname{rang}(f^t). \tag{4.233}$$

Démonstration. Nous posons $\dim \ker(f) = p$ et donc $\operatorname{rang}(f) = n - p$. 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

$$g_i = f(e_{p+i}) \tag{4.234}$$

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

$$\sum_{k=1}^{n-p} a_k f(e_{p+k}) = 0, \tag{4.235}$$

alors $f\big(\sum_k a_k e_{p+k}\big) = 0$, 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

$$\{\underbrace{g_1, \dots, g_{n-p}}_{\text{images}}, \underbrace{g_{n-p+1}, \dots, g_r}_{\text{complétion}}\} \tag{4.236}$$

de F.

Nous prouvons maintenant que $\operatorname{rang}(f^t) \geqslant n-p$ 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

$$f^t(g_i^*)e_k = g_i^*(fe_k), \tag{4.237}$$

Si $k = 1, \dots, p$, alors $fe_k = 0$ et donc $g_i^*(fe_k) = 0$; si $k = p + l$ alors

$$f^t(g_i^*)e_k = g_i^*(fe_{k+l}) = g_i^*(g_l) = \delta_{i,l} = \delta_{i,k-p} = \delta_{k,i+p}. \tag{4.238}$$

Donc $f^t(g_i^*) = e_{i+p}^*$. Cela prouve que les formes $f^t(g_i^*)$ sont libres et donc que

$$\operatorname{rang}(f^t) \geqslant n - p = \operatorname{rang}(f). \tag{4.239}$$

En appliquant le même raisonnement à f^t au lieu de f, nous trouvons

$$\operatorname{rang}\big((f^t)^t\big) \geqslant \operatorname{rang}(f^t) \tag{4.240}$$

et donc, vu que $(f^t)^t = f$, nous obtenons $\operatorname{rang}(f) = \operatorname{rang}(f^t)$.

□

Proposition 4.121 ([70]).
Si f est une application linéaire entre les espaces vectoriels E et F, alors nous avons

$$\operatorname{Image}(f^t) = \ker(f)^\perp. \tag{4.241}$$

Démonstration. Soient donc l'application $f\colon E \to F$ et sa transposée $f^t\colon F^* \to E^*$. Nous commençons par prouver que $\operatorname{Image}(f^t) \subset (\ker f)^\perp$. Pour cela nous prenons $\omega \in \operatorname{Image}(f^t)$, 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

$$\begin{aligned}
\dim\big(\operatorname{Image}(f^t)\big) &= \operatorname{rang}(f^t) && && \text{(4.242a)}\\
&= \operatorname{rang}(f) && \text{lemme 4.120} && \text{(4.242b)}\\
&= \dim(E) - \dim\ker(f) && \text{théorème 4.39} && \text{(4.242c)}\\
&= \dim\big((\ker f)^\perp\big) && \text{proposition 4.115.} && \text{(4.242d)}
\end{aligned}$$

□

Lemme 4.122 ([66]).
Soit $\mathbb{K}$ un corps, E et F deux $\mathbb{K}$-espaces vectoriels de dimension finie et une application linéaire $f\colon E \to F$. L'application f est injective si et seulement si sa transposée[45] *f^t est surjective.*

Démonstration. Supposons que f soit injective. Alors par le lemme 4.50, il existe $g\colon F \to E$ tel que $g \circ f = \mathrm{Id}\,|_E$. Nous avons alors aussi $(g \circ f)^t = \mathrm{Id}\,|_{E^*}$, mais $(g \circ f)^t = f^t \circ g^t$, donc f^t est surjective.

Inversement, nous supposons que $f^t\colon F^* \to E^*$ 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 $s\colon E^* \to F^*$ tel que $f^t \circ s = \mathrm{Id}\,|_{E^*}$. En passant à la transposée,

$$s^t \circ f = \mathrm{Id}\,|_E, \tag{4.243}$$

qui implique que f est injective. □

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 $f_i \in E^*$,

$$f_i(P) = P(a_i). \tag{4.244}$$

Lemme 4.123.
Ces formes forment une base de E^*.

Démonstration. Nous prouvons que l'orthogonal est réduit au nul :

$$\mathrm{Span}\{f_0, \dots, f_n\}^\perp = \{0\} \tag{4.245}$$

pour que la proposition 4.115 conclue. Si $P \in \mathrm{Span}\{f_i\}^\perp$, 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. □

Les **polynômes de Lagrange** sont les polynômes de la base (pré)duale de la base $\{f_i\}$.

Proposition 4.124.
Les polynômes de Lagrange sont donnés par

$$P_i = \prod_{k \neq i} \frac{X - a_k}{a_i - a_k}. \tag{4.246}$$

Démonstration. Il suffit de vérifier que $f_j(P_i) = \delta_{ij}$. Nous avons

$$f_j(P_i) = P_i(a_j) = \prod_{k \neq i} \frac{a_j - a_k}{a_i - a_k}. \tag{4.247}$$

Si $j \neq i$ alors un des termes est nul. Si au contraire $i = j$, tous les termes valent 1. □

4.6.5 Dual de $\mathbb{M}(n, \mathbb{K})$

Proposition 4.125 ([43]).
Soit $\mathbb{K}$, un corps. Les formes linéaires sur $\mathbb{M}(n, \mathbb{K})$ sont les applications de la forme

$$\begin{aligned} f_A\colon \mathbb{M}(n, \mathbb{K}) &\to \mathbb{K} \\ M &\mapsto \mathrm{Tr}(AM). \end{aligned} \tag{4.248}$$

45. Définition 4.118.

Démonstration. Nous considérons l'application

$$\begin{aligned} f\colon \mathbb{M}(n,\mathbb{K}) &\to \mathbb{M}(n,\mathbb{K})^* \\ A &\mapsto f_A \end{aligned} \tag{4.249}$$

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 $(E_{ij})_{kl} = \delta_{ik}\delta_{jl}$:

$$0 = f_A(E_{ij}) = \sum_k (AE_{ij})_{kk} = \sum_{kl} A_{kl}(E_{ij})_{lk} = \sum_{kl} A_{kl}\delta_{il}\delta_{jk} = A_{ij}. \tag{4.250}$$

Donc $A = 0$. □

Corollaire 4.126 ([43]).
Soit $\mathbb{K}$ un corps et $\phi \in \mathbb{M}(n,\mathbb{K})^*$ telle que pour tout $M, N \in \mathbb{M}(n,\mathbb{K})$ on ait

$$\phi(MN) = \phi(NM). \tag{4.251}$$

Alors il existe $\lambda \in \mathbb{K}$ tel que $\phi = \lambda \operatorname{Tr}$.

Démonstration. La proposition 4.125 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

$$\operatorname{Tr}(AMN) = \operatorname{Tr}(ANM) \tag{4.252}$$

pour toutes matrices $M, N \in \mathbb{M}(n,\mathbb{K})$. L'invariance cyclique de la trace[46] appliqué au membre de droite nous donne $\operatorname{Tr}(AMN) = \operatorname{Tr}(MAN)$, ce qui signifie que

$$\operatorname{Tr}\big((AM - MA)N\big) = 0 \tag{4.253}$$

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

$$AM = MA \tag{4.254}$$

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,

$$A_{li}\delta_{jm} = \delta_{il}A_{jm} \tag{4.255}$$

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,

$$\phi(X) = f_{\lambda\mathbb{1}}(X) = \lambda \operatorname{Tr}(X). \tag{4.256}$$

□

Corollaire 4.127 ([43]).
Soit $\mathbb{K}$ un corps. Tout hyperplan de $\mathbb{M}(n,\mathbb{K})$ coupe $\mathrm{GL}(n,\mathbb{K})$.

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 4.125 nous donne $A \in \mathbb{M}$ telle que $\phi = f_A$; nous notons r le rang de A. Par le lemme 4.104 nous avons $A = PJ_rQ$ avec $P, Q \in \mathrm{GL}(n,\mathbb{K})$ et

$$J_r = \begin{pmatrix} \mathbb{1}_r & 0 \\ 0 & 0 \end{pmatrix}. \tag{4.257}$$

46. Lemme 4.59.

Pour tout $M \in \mathbb{M}$ nous avons

$$\phi(M) = \mathrm{Tr}(AM) = \mathrm{Tr}(PJ_rQM) = \mathrm{Tr}(J_rQMP), \tag{4.258}$$

la dernière égalité découlant de l'invariance cyclique de la trace[47]. Ce que nous cherchons est $M \in \mathrm{GL}(n,\mathbb{K})$ telle que $\phi(M) = 0$. Nous commençons par trouver $N \in \mathrm{GL}(n,\mathbb{K})$ telle que $\mathrm{Tr}(J_rN) = 0$. Celle-là est facile : c'est

$$N = \begin{pmatrix} 0 & 1 \\ \mathbb{1}_{n-1} & 0 \end{pmatrix}. \tag{4.259}$$

Les éléments diagonaux de J_rN sont tous nuls. Par conséquent en posant $M = Q^{-1}NP^{-1}$ nous avons notre matrice inversible dans le noyau de ϕ. □

4.7 Représentation de groupe

Définition 4.128 (Représentation)**.**
Soit un groupe G et un espace vectoriel V. Nous disons qu'une application $\rho\colon G \to \mathrm{GL}(V)$ est une ***représentation*** *de G sur V si pour tout $g, h \in G$ nous avons*

$$\rho(g) \circ \rho(g) = \rho(gh). \tag{4.260}$$

Très souvent, nous disons que la représentation est le couple (V, ρ).

Définition 4.129.
Une représentation[48] *est* ***fidèle*** *si elle est injective en tant que application $G \to \mathrm{GL}(V)$. 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 4.130.
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

$$\begin{aligned} \rho\colon G &\to \mathrm{GL}(\mathbb{K}^n) \\ A &\mapsto f_A \end{aligned} \tag{4.261}$$

où f_A est l'application linéaire associée à A est une représentation de G.

47. Lemme 4.59.
48. Définition 4.128.

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

$$\mathrm{Card}(HK) = \frac{|H| \cdot |K|}{|H \cap K|}. \tag{5.1}$$

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 avions $hkh^{-1} \in K$, $\forall h, k \in H \times K$.

Théorème 5.2 (Théorème de Cauchy[71])**.**
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

$$\begin{aligned} \varphi\colon G &\to S_n \\ \varphi(x)g &\mapsto xg \end{aligned} \tag{5.2}$$

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 $x = y$. □

Lemme 5.4.
Soit p un diviseur premier de n. Alors le groupe symétrique S_n se plonge dans $\mathrm{GL}_n(\mathbb{F}_p)$.

Démonstration. Soit $\{e_i\}$ la base canonique de $\mathbb{F}_p$. Nous avons le morphisme injectif $\varphi\colon S_n \to \mathrm{GL}(n, \mathbb{F})$ donné par $\varphi(\sigma)e_i = e_{\sigma(i)}$. □

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 $\mathrm{GL}(n, \mathbb{F}_p)$.

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 rang[1] 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 premières 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

$$\begin{aligned}\mathrm{Card}\left(\mathrm{GL}(n,\mathbb{F}_p)\right) &= (p^n-1)(p^n-p)\dots(p^n-p^{n-1}) && \text{(5.3a)}\\ &= p\cdot p^2\cdots p^{n-1}(p^n-1)(p^{n-1}-1)\dots(p-1) && \text{(5.3b)}\\ &= p^{\frac{n(n-1)}{2}}m && \text{(5.3c)}\end{aligned}$$

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

$$|T| = p^{\frac{n(n-1)}{2}}, \tag{5.4}$$

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 $n \geqslant 0$. 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 2.31 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

$$gSg^{-1} \cap H \tag{5.5}$$

soit un p-Sylow de H.

1. Définition 4.38.

Démonstration. Nous considérons l'ensemble G/S sur lequel H agit. Si $a \in G$, le stabilisateur de $[a]$ dans G/S est

$$\begin{aligned} \text{Fix}\big([a]\big) &= \{h \in H \text{ tel que } [ha] = [a]\} && (5.6a)\\ &= \{h \in H \text{ tel que } a^{-1}ha \in S\} && (5.6b)\\ &= aSa^{-1} \cap H. && (5.6c)\end{aligned}$$

Nous cherchons $a \in G$ tel que l'entier

$$\frac{\text{Card}(H)}{\text{Card}\big(aSa^{-1} \cap H\big)} \tag{5.7}$$

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 (2.79)) nous dit que

$$\frac{|H|}{|aSa^{-1} \cap H|} = \text{Card}\big(\mathcal{O}_{[a]}\big). \tag{5.8}$$

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

$$p \mid \text{Card}(G/S) = \frac{|G|}{|S|} \tag{5.9}$$

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. □

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-Sylow[2]*.*

(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,

$$H = aSa^{-1} \cap H \tag{5.10}$$

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

$$E_S = \{T \in E \text{ tel que } s \cdot T = T \forall s \in S\}. \tag{5.11}$$

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

$$|E| \equiv |E_S| \mod p. \tag{5.12}$$

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

$$sTs^{-1} = T \tag{5.13}$$

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

$$g = s_1 t_1 \cdots s_r t_r \tag{5.14}$$

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

$$gtg^{-1} = s_1 t_1 \dots s_r t_r t t_r^{-1} s_r^{-1} \dots t_1^{-1} s_1^{-1} \in T. \tag{5.15}$$

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,

$$S = aTa^{-1} = T. \tag{5.16}$$

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

$$(gsg^{-1})^q = gs^q g^{-1} = e. \tag{5.17}$$

Pour avoir $gs^q g^{-1} = e$, 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 ([72])**.**
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 ([72])**.**
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 $H\backslash\{e\}$ 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 $H\backslash\{e\}$ 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. □

Corollaire 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. □

5.2 Groupe monogène

Le théorème suivant donne quelques informations à propos de groupes monogènes. Il impliquera dans le corollaire 20.13 qu'un groupe monogène d'ordre n possède $\varphi(n)$ générateur où φ est la fonction indicatrice d'Euler définie en 20.9.

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 $gg' = q^{n+n'} = g'g$. Nous considérons un générateur a de G (qui existe parce que G est monogène) et le morphisme surjectif

$$\begin{aligned} f\colon \mathbb{Z} &\to G \\ p &\mapsto a^p. \end{aligned} \tag{5.18}$$

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 2.25) nous indique que

$$\mathbb{Z}/\ker f = \mathbb{Z}/n\mathbb{Z} = \text{Image } f = G. \tag{5.19}$$

□

Le lemme suivant donne une démonstration alternative, avec une construction plus explicite de l'isomorphisme.

Lemme 5.17 ([1])**.**
À propos de groupes monogènes[3]

(1) Soit un groupe monogène G d'ordre fini n dont g est un générateur. Alors il existe un isomorphisme

$$\phi\colon G \to (\mathbb{Z}/n\mathbb{Z}, +) \tag{5.20}$$

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

$$\phi\colon G \to (\mathbb{Z}, +) \tag{5.21}$$

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 2.10.

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 $\{k + pn \text{ tel que } p \in \mathbb{Z}\}$.

Nous construisons l'isomorphisme $\phi\colon G \to \mathbb{Z}/n\mathbb{Z}$ de la façon suivante :

$$\phi(g^m) = [m]_n. \tag{5.22}$$

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 $k \geqslant l$. 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 ([73]).
Pour chaque $x \in (\mathbb{Z}/n\mathbb{Z})^*$ nous considérons l'application

$$\begin{aligned} \sigma_x\colon \mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z} \\ y &\mapsto xy. \end{aligned} \tag{5.23}$$

L'application

$$\sigma\colon \big((\mathbb{Z}/n\mathbb{Z})^*,\ \cdot\ \big) \to \operatorname{Aut}\big(\mathbb{Z}/n\mathbb{Z}, +\big) \tag{5.24}$$

ainsi définie est un isomorphisme de groupes.

L'énoncé de ce théorème s'écrit souvent rapidement par

$$\operatorname{Aut}(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^*, \tag{5.25}$$

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

$$f([r]) = f(r[1]) = rf([1]) = [r]f([1]). \tag{5.26}$$

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 $\big((\mathbb{Z}/n\mathbb{Z})^*,\ \cdot\ \big)$. Nous montrons à présent que [4]

$$\begin{aligned}\sigma\colon\ \mathrm{Aut}((\mathbb{Z}/n\mathbb{Z},+)) &\to \big((\mathbb{Z}/n\mathbb{Z})^*,\ \cdot\ \big)\\ f &\mapsto f([1])\end{aligned} \tag{5.27}$$

est un isomorphisme.

Nous commençons par la surjectivité. Soit $[a] \in (\mathbb{Z}/n\mathbb{Z})^*$. Les élément $[a]$ 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

$$f\big(g([1])\big) = f\big(g([1])[1]\big) = g([1])f([1]) = \sigma(f)\sigma(g). \tag{5.28a}$$

□

Ce dernier résultat s'étend aux groupes cycliques.

Proposition 5.19.
Si G est un groupe cyclique [5] *d'ordre n, alors*

$$\mathrm{Aut}(G) = (\mathbb{Z}/n\mathbb{Z})^*. \tag{5.29}$$

Corollaire 5.20.
Si p divise $q-1$ alors $\mathrm{Aut}(\mathbb{F}_q)$ possède un unique sous-groupe d'ordre p.

Démonstration. Si a est un générateur de $\mathbb{F}_q^*$ alors le groupe

$$\mathrm{gr}\left(a^{\frac{q-1}{p}}\right) \tag{5.30}$$

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 3.30 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 : [28].

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 2.11.

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,

$$m = p^\alpha m' \tag{5.31a}$$
$$q = p^\beta q' \tag{5.31b}$$

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. □

Proposition 5.22.
Soit G un groupe abélien fini et $x \in G$, un élément d'ordre maximum. Alors

(1) Il existe un morphisme $\varphi\colon G \to \mathrm{gr}(x)$ tel que $\varphi(x) = x$.

(2) Il existe un sous-groupe K de G tel que $G = \mathrm{gr}(x) \oplus K$.

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 $G = \mathrm{gr}(x)$, 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 $\varphi\colon H \to \mathrm{gr}(x)$ tel que $\varphi(x) = x$. Soit $y \in G\backslash H$, d'ordre b. Nous allons trouver un morphisme $\hat{\varphi}\colon \mathrm{gr}(H, y) \to \mathrm{gr}(x)$ telle que $\hat{\varphi}(x) = x$.

Pour cela nous commençons par construire les applications suivantes :

$$\begin{aligned} \tilde{\varphi}\colon \mathbb{Z}/b\mathbb{Z} \times H &\to \mathrm{gr}(x) \\ (\bar{k}, h) &\mapsto x^{kl}\varphi(h) \end{aligned} \tag{5.32}$$

où l est encore à déterminer, et

$$\begin{aligned} p\colon \mathbb{Z}/b\mathbb{Z} \times H &\to \mathrm{gr}(y, H) \\ (\bar{k}, h) &\mapsto y^k h. \end{aligned} \tag{5.33}$$

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

$$\begin{array}{ccccc} \ker(p) & \hookrightarrow & \mathbb{Z}/b\mathbb{Z} \times H & \xrightarrow{p} & \mathrm{gr}(y, H) \\ & & \downarrow{\scriptstyle \tilde{\varphi}} & \swarrow{\scriptstyle \hat{\varphi}} & \\ & & \mathrm{gr}(x) & & \end{array} \tag{5.34}$$

que l'on voudra être commutatif. Vu que p est surjective, les théorèmes d'isomorphismes nous disent que

$$\mathrm{gr}(y, H) \simeq \frac{\mathbb{Z}/b\mathbb{Z} \times H}{\ker p}. \tag{5.35}$$

Si $[\bar{k}, h]$ est la classe de $(\bar{k}, h)$ modulo $\ker(p)$ alors nous voudrions définir $\hat{\varphi}$ par

$$\hat{\varphi}\big([\bar{k}, h]\big) = \tilde{\varphi}(\bar{k}, h). \tag{5.36}$$

Pour que cela soit bien définit, il faut que si $(\bar{r}, z) \in \ker p$,

$$\hat{\varphi}\big([\bar{k}\bar{r}, hz]\big) = \hat{\varphi}\big([\bar{k}, h]\big), \tag{5.37}$$

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

$$\ker(p) \subset \ker(\tilde{\varphi}). \tag{5.38}$$

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

$$\ker(p) = \{(-m\beta, y^{m\beta}) \text{ tel que } m \in \mathbb{Z}\}. \tag{5.39}$$

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

$$\tilde{\varphi}(\beta, y^{-\beta}) = x^{\beta l}\varphi(y^{-\beta}) = x^{\beta l + \alpha}. \tag{5.40}$$

Par conséquent nous choisissons $l = -\alpha/\beta$. Nous devons maintenant vérifier que ce choix est légitime, c'est-à-dire que a divise bl et que α/β est un entier.

Étant donné que y est d'ordre b,

$$e = \varphi(y^b) = \varphi(y^{-\beta b/\beta}) = \varphi(y^{-\beta})^{b/\beta} = x^{b\beta/\alpha}. \tag{5.41}$$

Par conséquent a divise $\frac{b\alpha}{\beta} = -bl$.

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 $\varphi\colon G \to \text{gr}(x)$ tel que $\varphi(x) = x$. La première partie nous en assure l'existence. Nous montrons que

$$\begin{aligned} \psi\colon G &\to \text{gr}(x) \oplus \ker(\varphi) \\ g &\mapsto \big(\varphi(g), g\varphi(g)^{-1}\big) \end{aligned} \tag{5.42}$$

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,

$$\varphi\big(g\varphi(g)^{-1}\big) = \varphi(g)\varphi(g)^{-1} = e. \tag{5.43}$$

L'application ψ est un morphisme parce que, en utilisant le fait que G est abélien,

$$\begin{aligned} \psi(g_1g_2) &= \big(\varphi(g_1g_2), g_1g_2\varphi(g_1g_2)^{-1}\big) && \text{(5.44a)} \\ &= \big(\varphi(g_1)\varphi(g_2), g_1\varphi(g_1)^{-1}g_2\varphi(g_2)^{-1}\big) && \text{(5.44b)} \\ &= \psi(g_1)\psi(g_2). && \text{(5.44c)} \end{aligned}$$

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 2.25) appliqué à φ nous avons

$$|G| = |\,\text{gr}(x)| \cdot |\ker(\varphi)|. \tag{5.45}$$

□

Théorème 5.23.
Tout groupe abélien fini (non trivial) se décompose en

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/d_r\mathbb{Z} \tag{5.46}$$

avec $d_1 \geqslant 1$ et d_i divise d_{i+1} pour tout $i = 1, \ldots, r-1$.

De plus la liste $(d_1, \ldots, d_r)$ vérifiant ces propriétés est unique.

Démonstration. Soit x_1 un élément d'ordre maximal dans G. Soit n_1 son ordre et

$$H_1 = \mathrm{gr}(x_1) = \mathbb{F}_{n_1}. \tag{5.47}$$

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

$$G = \mathbb{F}_{d_1} \oplus \ldots \oplus \mathbb{F}_{d_r} = \mathbb{F}_{s_1} \oplus \ldots \oplus \mathbb{F}_{s_q}. \tag{5.48}$$

L'exposant de G est d_r et s_q. Donc $d_r = s_q$. Les complémentaires étant égaux nous avons

$$\mathbb{F}_{d_1} \oplus \ldots \oplus \mathbb{F}_{d_{r-1}} = \mathbb{F}_{s_1} \oplus \ldots \oplus \mathbb{F}_{s_{q-1}}. \tag{5.49}$$

En continuant nous trouvons $r = q$ et $d_i = s_i$. □

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 simple[6].

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),

$$n_q \in [1]_q. \tag{5.50}$$

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

$$1 < p = |H| < pq = |G|, \tag{5.51}$$

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. □

Avant le lire le théorème suivant, n'oubliez pas de lire la définition d'un produit semi-direct 2.76.

Théorème 5.25 ([74]).
Soient deux nombres premiers distincts[7] *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*

$$G = \mathbb{Z}/q\mathbb{Z} \times_\varphi \mathbb{Z}/p\mathbb{Z} \tag{5.52}$$

où $\varphi(\bar{1})$ est d'ordre p dans $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$.

6. Pas de sous-groupes normaux non triviaux, 2.5.
7. Le cas $p = q$ sera traité par la proposition 5.28.

(3) Si p et q sont premiers entre eux, le produit est direct[8].

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 $n_q = 1 \mod q$. Donc d'abord n_q vaut 1, p ou q. Ensuite $n_q = q$ est exclu par la condition $n_q = 1 \mod q$; la possibilité $n_q = p$ est également impossible parce que $p = 1 \mod q$ 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 entraine que (théorème de Lagrange 2.31) $|H \cap K|$ 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

$$\begin{aligned} \psi\colon H \times K &\to HK \\ (h,k) &\mapsto hk \end{aligned} \tag{5.53}$$

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

$$h^{-1}h' = (k'k^{-1})^{-1} \in H \cap K = \{e\}. \tag{5.54}$$

Par conséquent $|pq| = |H \times K| = |HK|$, et $HK = G$. Le corollaire 2.78 nous indique que

$$G = H \times_\varphi K \tag{5.55}$$

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 $\varphi\colon \mathbb{Z}/p\mathbb{Z} \to \text{Aut}(\mathbb{Z}/q\mathbb{Z})$ 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

$$G = \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/pq\mathbb{Z}. \tag{5.56}$$

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 2.25, nous avons

$$|\varphi(\mathbb{Z}/p\mathbb{Z})| = \frac{|\mathbb{Z}/p\mathbb{Z}|}{|\ker\varphi|}, \tag{5.57}$$

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 corollaire 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 $\varphi\colon \mathbb{Z}/p\mathbb{Z} \to \text{Aut}(\mathbb{Z}/q\mathbb{Z})$ 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 $\mathbb{Z}/p\mathbb{Z} \to \text{Aut}(\mathbb{Z}/q\mathbb{Z})$. 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

$$\begin{aligned} f\colon \mathbb{Z}/q\mathbb{Z} \times_\varphi \mathbb{Z}/p\mathbb{Z} &\to \mathbb{Z}/q\mathbb{Z} \times_{\varphi'} \mathbb{Z}/p\mathbb{Z} \\ (h,k) &\mapsto (h, \alpha(k)) \end{aligned} \tag{5.58}$$

où $\alpha = \varphi'^{-1} \circ \varphi$ est un isomorphisme de groupes. Le calcul est immédiat :

$$\begin{aligned} f(h_1,k_1)f(h_2mk_2) &= \big(h_1, \alpha(k_1)\big)(h_2, \alpha(k_2)) && \text{(5.59a)}\\ &= \big(h_1\varphi'(\alpha(k_1))h_2m\alpha(k_1k_2)\big) && \text{(5.59b)}\\ &= f\big(h_1\varphi(k_1)h_2, k_1k_2\big) && \text{(5.59c)}\\ &= f\big((h_1,k_1),(h_2,k_2)\big). && \text{(5.59d)} \end{aligned}$$

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 $q = 1 \mod p$. Par exemple $7 = 1 \mod 3$.

Proposition 5.26 ([23]).
Soit G un groupe fini d'ordre pq où p et q sont deux nombres premiers distincts vérifiant

$$\begin{cases} p \neq 1 \mod q & \text{(5.60a)}\\ q \neq 1 \mod p. & \text{(5.60b)} \end{cases}$$

Alors G est cyclique, abélien et

$$G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}. \tag{5.61}$$

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 $n_p = 1 \mod p$. 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 $q \neq 1 \mod p$. 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 exposée 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

$$\begin{aligned} (xyx^{-1})y^{-1} &\in T && \text{(5.62a)}\\ x(yx^{-1})y^{-1}) &\in S, && \text{(5.62b)} \end{aligned}$$

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 $S \operatorname{cat} T$ 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

$$|ST| = |S||T| = pq = |G|. \tag{5.63}$$

Par conséquent $G = ST$. En nous rappelant du fait que $S \cap T = \{e\}$ et que S et T sont normaux, le lemme 2.16 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

$$G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}. \tag{5.64}$$

□

Théorème 5.27 (Théorème de Burnside[28])**.**
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 :

$$\mathcal{Z}_G = \{z \in G \text{ tel que } \sigma_x(z) = z \forall x \in G\} = \text{Fix}_G(G). \tag{5.65}$$

Nous utilisons l'équation aux classes (2.54) pour dire que $|G| = |\mathcal{Z}_G| \mod p$. 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 $x \in G \backslash \mathcal{Z}$. Alors le stabilisateur de x pour l'action adjointe contient au moins $\mathcal{Z}$ et x, c'est-à-dire que $|\text{Fix}_G(x)| \geqslant p + 1$. 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 2.60. Voir aussi le thème 59.

5.6.1 Le groupe alterné

Définition 5.29.
Le groupe A_n des permutations paires[9] *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 caractéristique*[10] *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'indice*[11] *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 2.25, il existe un isomorphisme

$$f : S_n/\ker(\epsilon) \to \text{Image}(\epsilon). \tag{5.66}$$

9. Définition 2.71.
10. Définition 2.4.
11. Définition 2.30.

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 3.29, 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 $\varphi\colon S_n \to S_n/H$:

$$S_n \xrightarrow{\varphi} S_n/H \xrightarrow{\theta} \{-1,1\}. \tag{5.67}$$

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 2.73. L'enchaînement (5.67) nous montre que $H = \ker(\theta\circ\varphi) = \ker(\epsilon) = A_n$. □

Proposition 5.31 ([75]).
Le groupe symétrique S_n peut être écrit comme un produit semi-direct[12] *du groupe alterné :*

$$S_n = A_n \times_\varphi \mathbb{Z}/2\mathbb{Z} \tag{5.68}$$

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

$$1 \xrightarrow{i} A_n \xrightarrow{i} S_n \xrightarrow{\epsilon} \{\pm 1\} \longrightarrow 1 \tag{5.69}$$

où les i représentent des inclusions et ϵ est la signature définie en 2.65. Grâce à cette suite et au fait que la signature soit un isomorphisme à partir de la partie $\{\mathrm{Id}, \sigma\}$ (pour σ d'ordre 2, par exemple $\sigma = (12)$), le théorème 2.77 nous dit que

$$S_n \simeq A_n \times_\varphi \{\mathrm{Id}, \sigma\} \tag{5.70}$$

où φ est l'action adjointe de $\{\mathrm{Id}, \sigma\}$ sur A_n. □

Proposition 5.32.
Si $\beta \in S_n$ est une transposition, nous avons les égalités suivante d'ensembles :

$$S_n = A_n \cup A_n\beta = A_n \cup \beta A_n. \tag{5.71}$$

Démonstration. Les parties A_n et βA_n ont le même nombre d'éléments. En effet, l'application

$$\begin{aligned} \varphi\colon A_n &\to A_n\beta \\ \sigma &\mapsto \sigma\beta \end{aligned} \tag{5.72}$$

est une bijection.

De plus ces deux ensembles sont disjoints à cause de la proposition 2.73. 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

$$A_n \cup A_n\beta \tag{5.73}$$

contient $|S_n|/2 + |S_n|/2 = |S_n|$ éléments. C'est donc S_n. □

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. □

Proposition 5.34 ([76]).
Soit $n \geqslant 3$. Les 3-cycles $c_i = (1,2,i)$ avec $i = 3,\dots,n$ engendrent le groupe alterné A_n.

12. Définition 2.76.

Démonstration. Soit H, le groupe engendré par les c_i. D'abord nous avons

$$c_i = (1,2,i) = (1,2)(2,i), \tag{5.74}$$

de telle sorte que $\epsilon(c_i) = 1$. Par conséquent nous avons $H \subset A_n$. Nos montrons par récurrence que $A_n \subset H$.

Pour $n = 3$ il suffit de vérifier que $A_3 = \{\mathrm{Id}, c_3, c_3^2\}$. 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. □

Proposition 5.35.
Lorsque $n \geqslant 5$, 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 $n \geqslant 5$, nous pouvons prendre s et t, des éléments distincts dans $\{1,\dots,n\}\backslash\{j_1,j_2,j_3\}$ 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 2.72 et 2.70) et est donc dans A_n. Les supports de τ et φ étant disjoints, ces derniers commutent et nous avons

$$(\tau\alpha)\sigma(\tau\alpha)^{-1} = \tau(\alpha\sigma\alpha^{-1})\tau^{-1} = \tau\varphi\tau^{-1} = \varphi. \tag{5.75}$$

Donc σ et φ sont conjugués par $\tau\alpha$ qui est dans A_n. □

Théorème 5.36 ([23])**.**
Le groupe alterné A_n est simple[13] *pour $n \geqslant 5$.*

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 $k \in \{1,\dots,n\}\backslash\{i,j,\sigma^{-1}(i)\}$ et $m = \sigma(k)$. Nous considérons la permutation $\alpha = (ijk)$. Étant donné que N est normal l'élément

$$\theta = (\alpha^{-1}\sigma\alpha)\sigma^{-1} \tag{5.76}$$

est dans N. De plus en utilisant le lemme 2.66 et le fait que $\alpha^{-1} = (ikj)$ nous avons

$$\theta = (ikj)(j\sigma(j)m). \tag{5.77}$$

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 2.5.

— $m \neq i$, $m \neq j$ 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

$$\theta = (ik)(j\sigma(j)). \tag{5.78}$$

C'est a priori un 2×2-cycle. Mais si de plus $\sigma(j) = i$, alors

$$\theta = (ijk) \tag{5.79}$$

qui est un 3-cycle ; et si $\sigma(j) = k$, alors

$$\theta = (ikj) \tag{5.80}$$

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

$$\theta = (i, j, \sigma(j), m, k) \tag{5.81}$$

est un 5-cycle. Si $\sigma(j) = i$, alors

$$\theta = (ikj)(jim) = (imk) \tag{5.82}$$

qui est un 3-cycle. Si $\sigma(j) = k$, alors

$$\theta = (ikj)(jkm) = (ikm) \tag{5.83}$$

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 $e \in \{1, \dots, n\} \backslash \{a, b, c, d\}$ et nous avons

$$\underbrace{(abe)^{-1}\theta(abe)}_{\in N}\theta^{-1} = (aeb)(ab)(cd)(abe)(an)(cd) = (abe) \in N. \tag{5.84}$$

Si θ est le 5-cycle $(abcde)$, alors l'élément suivant est dans N :

$$(abc)^{-1}\theta(abc)\theta^{-1} = (acb)(abcde)(abc)(aedcb) = (acd). \tag{5.85}$$

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. □

Nous en déduisons immédiatement que si $n \geqslant 5$, 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 alterné[14] 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. □

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 :

$$\begin{aligned}\varphi\colon G &\to S(G)\\ g &\mapsto t_g\end{aligned} \tag{5.86}$$

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 Image(φ) est donc un sous-groupe de $S(G)$, et φ est un isomorphisme vers ce groupe. □

Lemme 5.39.
Si $n \geqslant 3$, 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 avions $st = ts$ 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 $\{\mathrm{Id}\}$.

□

Proposition 5.40 ([77, 72])**.**
Tout groupe simple[15] *d'ordre* 60 *est isomorphe au groupe alterné A_5.*

15. Définition 2.5.

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 :

$$g \cdot S = gSg^{-1}. \tag{5.90}$$

Cela donne donc un morphisme $\theta\colon G \to S_6$. Le noyau de θ est un sous-groupe normal. En effet si $k \in \ker\theta$ et si $g \in G$ nous avons

$$\begin{aligned}(gkg^{-1}) \cdot S &= gkg^{-1}Ggk^{-1}g^{-1} && \text{(5.91a)}\\ &= gkTk^{-1}g^{-1} && \text{(5.91b)}\\ &= gTg^{-1} && \text{(5.91c)}\\ &= S && \text{(5.91d)}\end{aligned}$$

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

$$G = D(G) \subset D(S_6) = A_6 \tag{5.92}$$

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

$$\theta\big(g\theta^{-1}(\sigma)g^{-1}\big) = \theta(g)\sigma\theta(g)^{-1} \in A_6. \tag{5.93}$$

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

$$[\sigma] = \{h\sigma \text{ tel que } h \in H\}. \tag{5.94}$$

Évidemment A_6 agit sur X de façon naturelle. Au niveau de la cardinalité,

$$\operatorname{Card}(X) = \frac{|A_6|}{|G|} = \frac{360}{60} = 6. \tag{5.95}$$

Le groupe A_6 agit sur X qui a 6 éléments. Nous avons donc une application $\varphi\colon A_6 \to A_6$. 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. □

5.6.2 Sous-groupes normaux

5.41 ([78]).
Soit le groupe V_4 engendré par les bitranspositions de S_4. Nous savons de l'exemple 2.69(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 $\mathrm{Fix}_{S_n}(a)$ *(avec* $a \in \{1,\dots,n\}$*) sont conjugués entre eux.*

Démonstration. Soit $\sigma \in \mathrm{Fix}(a)$ 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

$$(s\sigma s^{-1})(b) = (s\sigma)(a) = s(a) = b. \tag{5.96}$$

Donc $s\,\mathrm{Fix}(a)s^{-1} \subset \mathrm{Fix}(b)$.

Dans l'autre sens, si $\sigma \in \mathrm{Fix}(b)$ alors $s^{-1}\sigma s \in \mathrm{Fix}(a)$. Mais $\sigma = s(s^{-1}\sigma s)s^{-1}$, donc $\sigma \in s\,\mathrm{Fix}(a)s^{-1}$. □

Proposition 5.43 (Sous-groupes normaux de S_n [78]).
Les sous-groupes normaux de S_n *ne sont pas légions.*

(1) Pour $n = 4$*, le sous-groupes normaux de* S_4 *sont* $\{\mathrm{Id}\}$*,* V_4*,* A_4 *et* S_4*.*

(2) Pour $n \neq 4$*, les sous-groupes normaux de* S_n *sont* $\{\mathrm{Id}\}$*,* A_n *et* S_n*.*

Démonstration. Les cas $n \leqslant 2$ sont un peu triviaux, donc nous faisons $n \geqslant 3$. Soit H normal dans S_n et $s \neq \mathrm{Id}$ 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 2.70), 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 2.69). Nous en concluons que $sts^{-1}t^{-1}$ est un produit de deux transpositions appartenant H.

Nous venons de prouver que H contient au moins un produit de deux transpositions. Et ce produit est différent de Id parce que $sts^{-1}t^{-1} = \mathrm{Id}$ impliquerait $st = ts$.

Soient donc deux transpositions $t_1, t_2 \in H$ telles que $t_1t_2 \neq \mathrm{Id}$. Les supports de t_1 et t_2 ont soit 1 soit aucun éléments communs.

Premier cas Supposons $t_1 = (a,b)$, $t_2 = (b,c)$ avec a,b,c distincts dans $\{1,\dots,n\}$. Dans ce cas $t_1t_2 = (a,b,c)$ 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 2.69) 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

$$4 \leqslant |H| \leqslant 24. \tag{5.97}$$

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 $H = A_n$ (proposition 5.30(3)). Quid de $|H| = 8$?
D'après le corollaire 2.32 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 $x = \mathrm{Id}$. 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 $n \geqslant 5$ Soit un élément e distinct de a, b, c et d. Par notre liste préférée des classes de conjugaisons (exemple 2.69(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 :

$$(ce)(ab)(ab)(cd) = (ce)(cd) = (ecd). \tag{5.98}$$

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 $\{\mathrm{Id}\}$ 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 $\sigma^2 = \mathrm{Id}$ ou $\sigma^2 = \sigma$. Aucun élément de S_3 ne vérifie $\sigma^2 = \sigma$ (à part l'identité). Donc $\sigma^2 = \mathrm{Id}$, ce qui fait que σ est une transposition. Donc

$$H = \{\mathrm{Id}, (12)\} \tag{5.99}$$

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 cyclique[16] (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

$$H = \mathbb{Z}_3 \times_\varphi \mathbb{Z}_2 \tag{5.100}$$

où $\varphi\colon \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3)$ et $\varphi(1)$ est d'ordre 2 dans $\mathrm{Aut}(\mathbb{Z}_3)$. 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 $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) = (\mathbb{Z}/3\mathbb{Z})^*$, et que via cette identification, $\varphi(1) = 2 \in (\mathbb{Z}/3\mathbb{Z})^*$ au sens où $\varphi(1)x = 2x$. Nous avons alors $\varphi(1)^2 x = 4x = x$ 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 $\mathbb{Z}_2 = \big(\{0, 1\}, +\big)$ alors que là nous écrivons $\mathbb{Z}_2 = \big(\{-1, 1\}, \cdot\big)$. 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 $S_n = A_n \times_\varphi \mathbb{Z}_2$; 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 2.11.

Le groupe A_3 possède $|S_3|/2 = 3$ éléments. Il est vite vu que $A_3 = \{\mathrm{Id}, (12)(31), (12)(32)\}$: ce sont trois éléments de signature paire dans S_3 ; donc c'est S_3. La correspondance $\mathrm{Id} \mapsto 0$, $(12)(13) \mapsto 1$, $(13)(12) \mapsto 2$ donne un isomorphisme avec $(\mathbb{Z}_3, +)$.

Pour $n \geqslant 5$ 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 a priori pas un groupe) donnée par $g \cdot [s] = [gs]$.

Morphisme $\varphi\colon S_n \to S_E$ Le φ définit par l'action est un morphisme parce que

$$\varphi(g_1g_2)[s] = [g_1g_2s] = \varphi(g_1)[g_2s] = \varphi(g_1)\varphi(g_2)[s]. \tag{5.101}$$

Mais il faut également vérifier que pour chaque $g \in G$, l'application $\varphi(g)\colon E \to E$ 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 $gs_1 = gs_2h$, ce qui prouve que $s_1 = s_2h$ 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.

$\ker(\varphi)$ est normal Soit $z \in \ker(\varphi)$, c'est-à-dire que $\varphi(z) = \mathrm{Id}_E$. Alors pour $\sigma \in S_n$ nous avons $\varphi(\sigma z\sigma^{-1}) = \varphi(\sigma)\varphi(z)\varphi(\sigma^{-1}) = \mathrm{Id}_E$.

$\ker(\varphi) = \bigcap_{g\in S_n} gHg^{-1}$ 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

$$\varphi(z)[s] = [zs] = [zhs^{-1}s] = [s], \tag{5.102}$$

ce qui prouve que $\varphi(z) = \mathrm{Id}$.

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 $|\ker(\varphi)| \leqslant |H|$ parce que $\ker(\varphi)$ est une intersection dont un des termes est H lui-même. Nous avons alors les inégalités

$$|\ker(\varphi)| \leqslant |H| = (n-1)! < |A_n|. \tag{5.103}$$

Mais le seul sous-groupes normaux de S_n sont A_n et S_n et $\{\mathrm{Id}\}$ (proposition 5.43). Donc $\ker(\varphi) = \mathrm{Id}$ et φ est une injection entre deux ensembles finis de même cardinalité. Cela fait de φ une bijection et donc un isomorphisme de groupes

$$\varphi\colon S_n \to S_E. \tag{5.104}$$

Soit une fonction de numérotation $\psi\colon E \to \{1, \ldots, n\}$. Avec cela nous définissons un isomorphisme de groupes

$$\begin{aligned} \tilde{\psi}\colon S_E &\to S_n \\ \sigma &\mapsto \psi\sigma\psi^{-1}. \end{aligned} \tag{5.105}$$

Fixateur Nous montrons à présent que $(\tilde{\psi} \circ \varphi)(H) = \mathrm{Fix}\big(\psi[\mathrm{Id}]\big)$ 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 $\psi[\mathrm{Id}]$:

$$(\tilde{\psi} \circ \varphi)(h)\psi[\mathrm{Id}] = \psi \circ \varphi(h)[\mathrm{Id}] = \psi[h] = \psi[\mathrm{Id}]. \tag{5.106}$$

Donc $(\tilde{\psi} \circ \varphi)(H) \subset \mathrm{Fix}\big(\psi[\mathrm{Id}]\big)$.

Pour l'autre inclusion, soit $\sigma \in S_n$ tel que $\sigma\psi[\mathrm{Id}] = \psi[\mathrm{Id}]$. Vu que $\sigma \in S_n$ nous avons $s \in S_E$ tel que $\sigma = \tilde{\psi}(s)$. Pour ce s nous avons donc

$$\big(\tilde{\psi}(s) \circ \psi\big)[\mathrm{Id}] = \psi[\mathrm{Id}], \tag{5.107}$$

d'où nous déduisons $s[\mathrm{Id}] = [\mathrm{Id}]$. Cela prouve que s stabilise $[\mathrm{Id}]$ dans S_E. Donc $s = \varphi(h)$ pour un certain $h \in H$, et au final $\sigma = \tilde{\psi}\big(\varphi(h)\big)$.

Conclusion L'application $\tilde{\psi} \circ \varphi \colon H \to S_n$ est une application dont l'image est le fixateur d'un point. Plus précisément,

$$\tilde{\psi} \circ \varphi \colon H \to \mathrm{Fix}\big(\psi[\mathrm{Id}]\big) \tag{5.108}$$

est un isomorphisme de groupe. Mais le stabilisateur d'un point dans S_n est S_{n-1}.

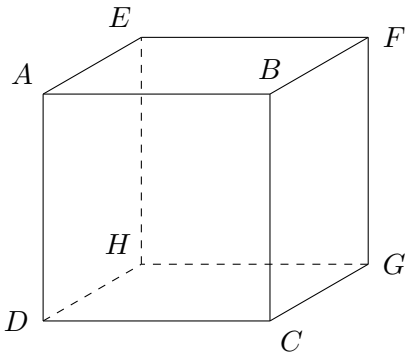
□

5.7 Isométriques du cube

Les isométries du cube proviennent de [43].

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-groupes de G constitué des éléments de déterminant positif. Nous notons

$$\mathcal{D} = \{D_1, \dots, D_4\} \tag{5.109}$$



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

$$\rho \colon G \to S_4. \tag{5.110}$$

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,

$$\overrightarrow{ON} = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} \quad \overrightarrow{OF} = \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}. \tag{5.111}$$

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, $d\big(f(B), f(G)\big) = d(B, G)$, 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 :

$$\ker(\rho) = \{\mathrm{Id}, s_0\}. \tag{5.112}$$

Le premier théorème d'isomorphisme 2.25 nous permet d'écrire le quotient de groupes :

$$\frac{G}{\{\mathrm{Id}, s_0\}} \simeq S_4. \tag{5.113}$$

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

$$\begin{aligned}\varphi\colon \frac{G}{\{\mathrm{Id}, s_0\}} &\to G^+ \\ [g] &\mapsto \begin{cases} g & \text{si } \det(g) > 0 \\ g \circ s_0 & \text{sinon} \end{cases}\end{aligned} \tag{5.114}$$

est un isomorphisme de groupes. Et enfin nous pouvons écrire

$$G^+ \simeq S_4. \tag{5.115}$$

Nous allons maintenant utiliser le corollaire 2.78 pour montrer que $G = G^+ \times_\sigma \ker(\rho)$. Les conditions sont remplies :

— $\ker(\rho)$ normalise G^+ parce que $\ker(\rho)$ ne contient que $\pm\mathbb{1}$.

— $\ker(\rho) \cap G^+ = \{\mathrm{Id}\}$.

— $\ker(\rho)G^+ = G$ 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

$$G \simeq S_4 \times_\sigma \mathbb{Z}/2\mathbb{Z}. \tag{5.116}$$

Mais étant donné que la conjugaison par s_0 est triviale, le produit semi-direct est un produit direct :

$$G \simeq S_4 \times \mathbb{Z}/2\mathbb{Z}. \tag{5.117}$$

Il est maintenant du meilleur gout de pouvoir identifier géométriquement ces éléments. Les éléments de $\mathbb{Z}/2\mathbb{Z} = \{\mathrm{Id}, s_0\}$ 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 2.69.

(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 :

$$B \to D \to E \to B. \tag{5.118}$$

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 précédente [17], 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 20.31 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 [43] 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 1.73.

Définition 6.2 ([79]).
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 $(\mathbb{K}, \leqslant)$ et $a \in \mathbb{K}$ alors $a^2 \geqslant 0$. En effet si $a \geqslant 0$ alors $a^2 = a \times a \geqslant 0$ directement par la définition 1.73(1b). Si $a \leqslant 0$ alors $-a \geqslant 0$ et

$$a^2 = (-a)^2 \geqslant 0. \tag{6.1}$$

Vu que $-1 < 0$, il ne peut donc pas être écrit comme un carré. A fortiori comme somme de carrés. □

6.1.2 Automorphismes de $\mathbb{R}$ et $\mathbb{C}$

Proposition 6.4 ([80, 1]).
L'identité est l'unique automorphisme du corps $\mathbb{R}$.

Démonstration. Soit un automorphisme $\sigma : \mathbb{R} \to \mathbb{R}$. Comme pour tout automorphisme,

$$\sigma(a) = \sigma(1a) = \sigma(1)\sigma(a). \tag{6.2}$$

Donc $\sigma(1) = 1$.

Identité sur les rationnels De plus

$$\sigma(n) = \sigma(1 + \ldots + 1) = \sigma(1) + \ldots + \sigma(1) = n, \tag{6.3}$$

et

$$\sigma\left(\frac{1}{n}\right) + \ldots + \sigma\left(\frac{1}{n}\right) = \sigma\left(\frac{1}{n} + \ldots + \frac{1}{n}\right) = \sigma(1) = 1. \tag{6.4}$$

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 $\mathbb{Q}$,

$$q_i + \epsilon > \sigma(x). \tag{6.5}$$

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,

$$q_i < \sigma(x) < q_i + \epsilon \tag{6.6}$$

pour tout $\epsilon > 0$ dans $\mathbb{Q}$ et $i > N$. Ce ϵ étant fixé nous pouvons prendre la limite des inégalités (6.6) :

$$x \leqslant \sigma(x) \leqslant x + \epsilon. \tag{6.7}$$

Cela étant valable pour tout $\epsilon > 0$ dans $\mathbb{Q}$, nous avons bien $x = \sigma(x)$.

□

Remarque 6.5.
Certains[80] 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 $\mathbb{K} \to \mathbb{R}$ 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

$$\phi\big(\phi^{-1}(x) + \phi^{-1}(y)\big) = x + y \tag{6.8}$$

parce que ϕ est un morphisme. D'autre part,

$$\phi\big(\phi^{-1}(x) + \phi^{-1}(y)\big) = \phi(a + b). \tag{6.9}$$

Donc

$$\phi^{-1}(x + y) = \phi^{-1}\big(\phi(a) + \phi(b)\big) = \phi^{-1}\big(\phi(a + b)\big) = a + b = \phi^{-1}(x) + \phi^{-1}(y). \tag{6.10}$$

Proposition 6.6.
Un automorphisme du corps $\mathbb{C}$ qui fixe $\mathbb{R}$ est soit l'identité soit la conjugaison complexe[1].

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,

$$-1 = \sigma(-1) = \sigma(ii) = \sigma(i)^2. \tag{6.11}$$

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 $\sigma = \mathrm{Id}$. 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. □

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 20.5) comment nous pouvons définir $\mathbb{F}_{p^n}$ lorsque p est premier, ainsi que l'unicité d'un tel corps.

Nous avons par exemple

$$\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\} \tag{6.12}$$

avec la loi $2 = 0$.

Notons que $\mathbb{F}_p$ est un corps 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 3.87 que $\mathbb{F}_p$ est un corps lorsque p est premier. □

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 3.78).

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

$$\mathbb{Z}1_{\mathbb{A}} \subset \mathbb{P} \subset \mathbb{K}. \tag{6.13}$$

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 1.70).

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 3.55. L'ensemble $\mathbb{F}_p$ étant un corps, c'est le corps premier de $\mathbb{K}$. □

Proposition 6.12.
Soit $\mathbb{K}$ un corps et $\mathbb{P}$ son sous-corps premier. Si $\sigma \in \mathrm{Aut}(\mathbb{K})$ alors $\sigma|_{\mathbb{P}} = \mathrm{Id}$, 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. Si $x \in \mathbb{F}_p$ alors $x^p = x$. Si $x \in (\mathbb{F}_p)^*$, alors $x^{p-1} = 1$.

En particulier si $x \in \mathbb{F}_p^*$ alors $x^{-1} = x^{p-2}$.

Démonstration. Étant donné que $\mathbb{F}_p$ est un corps commutatif et que p est premier, la proposition 3.58 nous indique que $\sigma(x) = x^p$ est un automorphisme. La proposition 6.12 nous indique alors que

$$a^p = a. \tag{6.14}$$

Si a est inversible alors $a^{p-1} = a^p a^{-1} = 1$. □

Remarque 6.14.
Une autre façon d'énoncer le petit théorème de Fermat 6.13 est que si p est premier et si a est premier avec p, alors $a^{p-1} \in [1]_p$. Le nombre a n'est pas premier avec p uniquement lorsque a est multiple de p. Dans ce cas c'est $a = 0$ dans $\mathbb{F}_p$ et donc $a^{p-1} = 0$.

Exemple 6.15
Soit $\mathbb{K} = \mathbb{F}_{29}$. Le nombre 29 étant premier, $\mathbb{K}$ est un corps premier. C'est le corps des entiers modulo 29. Nous avons donc

$$-142 = -113 = -84 = -55 = -26 = 3 = 32 = 61 = 90 = 119. \tag{6.15}$$

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,

$$x^{-a} = (x^a)^{27} = x^{27a}. \tag{6.16}$$

Le nombre $27a$ peut être grand par rapport à 29. Mais en réutilisant le fait que $1 = x^{28}$, on obtient

$$x^{-a} = x^{[27a]_{28}}. \tag{6.17}$$

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. △

6.2 Théorème des deux carrés

Proposition 6.16.
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. □

6.2.1 Un peu de structure dans $\mathbb{Z}[i]$

Lemme 6.17.
L'application

$$\begin{aligned} N\colon \mathbb{Z}[i] &\to \mathbb{N} \\ a + bi &\mapsto a^2 + b^2 \end{aligned} \tag{6.18}$$

est un stathme euclidien pour $\mathbb{Z}[i]$.

Démonstration. Soient $t, z \in \mathbb{Z}[i]\backslash\{0\}$ dont le quotient s'écrit

$$\frac{z}{t} = x + iy \tag{6.19}$$

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 hasard [2]. Alors nous avons

$$|\frac{z}{t} - q| \leqslant \frac{|1+i|}{2} = \frac{\sqrt{2}}{2} < 1. \tag{6.20}$$

On pose $r = z - qt$ qui est bien un élément de $\mathbb{Z}[i]$. De plus

$$|r| = |z - qt| = |t||\frac{z}{t} - q| < |t|, \tag{6.21}$$

c'est-à-dire que $|r|^2 < |t|^2$ et donc $N(r) < N(t)$. □

Étant donné que $\mathbb{Z}[i]$ est euclidien, il est principal (proposition 3.131).

Lemme 6.18.
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

$$1 = N(zz') = N(z)N(z'), \tag{6.22}$$

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

$$\mathbb{Z}[i]^* = \{\pm 1, \pm i\}. \tag{6.23}$$

□

Définition 6.19 ([81])**.**
*Un **monoïde** est un triple $(E, *, e)$ où E est un ensemble, e est un élément de E et $*: E \times E \to E$ est une loi de composition telle que pour tout $x, y \in E$,*

(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 6.20.
L'ensemble $\Sigma = \{a^2 + b^2$ tel que $a, b \in \mathbb{N}\}$ est un sous-monoïde [3] 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

$$N(zz') = N(z)N(z') = nm. \tag{6.24}$$

Donc nm est l'image de zz' par N, ce qui prouve que $nm \in \Sigma$. □

Théorème 6.21 (Théorème des deux carrés, version faible)**.**
Un nombre premier est somme de deux carrés si et seulement si $p = 2$ ou $p \in [1]_4$.

Remarque 6.22.
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 $[1]_4$.

2. Dans l'exemple 3.130, nous prenions toujours l'inférieur parce que le stathme tenait compte de la positivité.
3. Définition 6.19.

Démonstration. Soit p un nombre premier dans Σ. Si $a = 2k$, alors $a^2 = 4k^2$ et $a^2 = 0 \mod 4$. Si au contraire a est impair, $a = 2k + 1$ et $a^2 = 4k^2 + 1 + 4k = 1 \mod 4$. 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 $0 \mod 4$ ne sont pas premiers ; parmi les $2 \mod 4$, 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 $p = 1 \mod 4$. Il reste à faire le contraire : démontrer que si un nombre premier p vaut $1 \mod 4$, alors il est premier. Nous considérons l'anneau

$$\mathbb{Z}[i] = \{a + bi \text{ tel que } a, b \in \mathbb{Z}\}. \tag{6.25}$$

puis l'application

$$\begin{aligned} N\colon \mathbb{Z}[i] &\to \mathbb{N} \\ a + bi &\mapsto a^2 + b^2. \end{aligned} \tag{6.26}$$

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 6.18).

Le lemme 6.17 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 3.131).

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

$$p^2 = N(p) = N(z)N(z'). \tag{6.27}$$

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 3.102 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

$$\mathbb{Z}[i]/(p) = (\mathbb{Z}[X]/(p))/(X^2 + 1) = \mathbb{F}_p[X]/(X^2 + 1). \tag{6.28}$$

Nous avons donc équivalence des propositions suivantes :

$$p \in \Sigma \tag{6.29a}$$
$$\mathbb{F}_p[X]/(X^2 + 1) \text{ n'est pas intègre} \tag{6.29b}$$
$$X^2 + 1 \text{ n'est pas irréductible dans } \mathbb{F}_p \tag{6.29c}$$
$$X^2 + 1 \text{ admet une racine dans } \mathbb{F}_p \tag{6.29d}$$
$$-1 \in (\mathbb{F}_p^*)^2 \tag{6.29e}$$
$$\exists y \in \mathbb{F}_p^* \text{ tel que } y^2 = -1. \tag{6.29f}$$

Le point (6.29c) vient de la proposition 6.16. 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,

$$(-1)^{(p-1)/2} = (y^2)^{(p-1)/2} = y^{p-1} = 1 \tag{6.30}$$

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

$$1 = (-1)^{(p-1)/2}, \tag{6.31}$$

c'est-à-dire $\frac{p-1}{2} = 0 \mod 2$ ou encore $p = 1 \mod 4$. □

Théorème 6.23 (Théorème des deux carrés[43])**.**
Soit $n \geqslant 2$ un nombre dont nous notons

$$n = \prod_{p\in\mathcal{P}} p^{v_p(n)} \tag{6.32}$$

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 (6.32) 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
$$\prod_{p\in\mathcal{P}\cap[1]_4} p^{v_p(n)} \in \Sigma. \tag{6.33}$$
- Le seul nombre premier dans $[2]_4$ est 2. C'est un élément de Σ.
- Le produit
$$\prod_{p\in\mathcal{P}\cap[3]_4} p^{v_p(n)} \tag{6.34}$$
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 6.20.

Condition nécessaire. Soit p, un nombre premier. Nous voulons montrer que

$$\{v_p(n) \text{ tel que } n \in \Sigma\} \subset [2]_2. \tag{6.35}$$

Pour montrer cela nous allons procéder par récurrence sur les ensembles

$$E_k = \{v_p(n) \text{ tel que } n \in \Sigma\} \cap \{0, \dots, k\}. \tag{6.36}$$

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 $v_p(n) \leqslant k+1$ 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

$$n = a^2 + b^2 = (a + bi)(a - bi) \tag{6.37}$$

Vu que $\mathbb{Z}[i]$ est principal, le lemme de Gauss 3.112 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

$$p^2 \mid a^2 + b^2 = n. \tag{6.38}$$

Posons $a = pa'$ et $b = pb'$ avec $a', b' \in \mathbb{N}$. Nous avons

$$\frac{n}{p^2} = \frac{p^2a'^2 + p^2b'^2}{p^2} = a'^2 + b'^2 \in \Sigma. \tag{6.39}$$

Mais par construction,

$$v_p\left(\frac{n}{p^2}\right) = v_p(n) - 2 < k. \tag{6.40}$$

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

$$\begin{cases} x = a_1 \mod p & \text{(6.41a)} \\ x = a_2 \mod q & \text{(6.41b)} \end{cases}$$

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 corollaire qui établira l'isomorphisme d'anneaux $\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$. Voir les-mathematiques.net.

Lemme 6.24 (Lemme chinois [82])**.**
Soient n_1, n_2 deux entiers premiers entre eux. Soient $a_1, a_2 \in \mathbb{Z}$. Les solutions du système

$$\begin{cases} x = a_1 \mod n_1 & \text{(6.42a)} \\ x = a_2 \mod n_2 & \text{(6.42b)} \end{cases}$$

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 Bézout[4]

$$u_1n_1 + u_2n_2 = 1, \tag{6.43}$$

et

$$a = \big(a_1u_2n_2 + a_2u_1n_1\big) \mod (n_1). \tag{6.44}$$

Alors $x = a \mod (n_1n_2)$.

Démonstration. Vérifions que le x donné par $x = a \mod (n_1n_2)$ est bien une solution. D'abord

$$\begin{aligned} a \mod n_2 &= a_1u_2n_2 \mod n_1 && \text{(6.45a)} \\ &= a_1(1 - u_1n_1) \mod n_1 && \text{(6.45b)} \\ &= a_1 \mod n_1 && \text{(6.45c)} \end{aligned}$$

où nous avons utilisé l'identité de Bézout (6.43). La vérification de $a \mod n_2 = a_2 \mod n_2$ est la même.

Soit maintenant $x \in \mathbb{Z}/n_1n_2\mathbb{Z}$ une solution du système (6.42) et a donné par la formule (6.44). Alors

$$\begin{aligned} (x - a) \mod n_1 &= \Big(a_1 - (a_1n_2u_2 + a_2u_1n_1)\Big) \mod n_1 && \text{(6.46a)} \\ &= a_1 - a_1u_2n_2 \mod n_1 && \text{(6.46b)} \\ &= 0, && \text{(6.46c)} \end{aligned}$$

donc $(x - a) \mod n_1 = 0$, ce qui signifie que $x - a$ est divisible par n_1. De la même façon, $(x - a) \mod n_2 = 0$ 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 $x = a \mod n_1n_2$. □

4. voir le théorème 3.13

Théorème 6.25 (Théorème chinois)**.**
Soient p, q deux naturels premiers entre eux. Si $p, q \geqslant 2$ alors l'application

$$\begin{aligned} \phi\colon \mathbb{Z}/pq\mathbb{Z} &\to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ [x]_{pq} &\mapsto \big([x]_p, [x]_q\big) \end{aligned} \tag{6.47}$$

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,

$$\begin{aligned} \phi([q]_{pq} + [y]_{pq}) &= \phi\big((x+y) \mod pq\big) && \text{(6.48a)} \\ &= \big([x+y]_p, [x+y]_q\big) && \text{(6.48b)} \\ &= \big([x]_p + [y]_p, [x]_q + [y]_q\big) && \text{(6.48c)} \\ &= \big([x]_p, [x]_q\big) + \big([y]_p, [y]_q\big) && \text{(6.48d)} \\ &= \phi(x) + \phi(y). && \text{(6.48e)} \end{aligned}$$

En ce qui concerne le produit, c'est le même jeu : nous obtenons

$$\phi\big([xy]_{pq}\big) = \phi([x]_{pq}])\phi([y]_{pq}) \tag{6.49}$$

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

$$\phi([x]_{pq}) = \big([y_1]_p, [y_2]_q\big) \tag{6.50}$$

revient à demander que $[x]_p = [y_1]_p$ et $[x]_q = [y_2]_q$, c'est-à-dire que x résolve le système

$$\begin{cases} x = y_1 \mod p & \text{(6.51a)} \\ x = y_2 \mod q. & \text{(6.51b)} \end{cases}$$

Le lemme chinois 6.24 nous assure qu'une solution existe.

En ce qui concerne l'injectivité, nous supposons que x et y soient deux entiers tels que

$$\phi([x]_{pq}) = \phi([y]_{pq}). \tag{6.52}$$

Nous en déduisons le système

$$\begin{cases} x \mod p = y \mod p & \text{(6.53a)} \\ x \mod q = y \mod q & \text{(6.53b)} \end{cases}$$

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

$$kp + lq = 0. \tag{6.54}$$

Étant donné que p et q sont premiers entre eux, la seule possibilité est $k = l = 0$, c'est-à-dire $x = y$. □

Théorème 6.26 (Théorème chinois)**.**
Soit A un anneau commutatif, $n \geqslant 2$, 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 $1 \leqslant i \leqslant n$.

Démonstration. Pour $i \in \{1, \dots, n\}$ nous notons J_i le produit $J_i = \prod_{k \neq i} I_k$. Étant donné que chaque I_i est un idéal, nous avons $I_k \subset J_i$ lorsque $i \neq k$.

Soit i fixé. Pour tout $j \neq i$, puisque $I_i + I_j = A$, nous pouvons trouver $a_j \in I_i$ et $b_j \in I_j$ tels que $a_j + b_j = 1$. Nous avons alors

$$1 = \prod_{j \neq i} (a_j + b_j). \tag{6.55}$$

Par ailleurs, $I_i + J_i = A$ parce que J_i contient I_k avec $k \neq i$ et $I_i + I_k = A$. Nous pouvons donc prendre $\alpha_i \in I_i$ et $\beta_i \in J_i$ tels que

$$\alpha_i + \beta_i = 1 = \prod_{j\neq i}(a_j + b_j). \tag{6.56}$$

Nous considérons alors l'élément $x = \beta_1 x_1 + \cdots + \beta_n x_n$. Il vient alors

$$x - x_1 = (\beta_1 - 1)x_1 + \beta_2 x_2 + \cdots + \beta_n x_n \tag{6.57a}$$
$$= -\alpha_1 x_1 + \beta_2 x_2 + \cdots + \beta_n x_n. \tag{6.57b}$$

Mais $\alpha_1 \in I_1$ et tous les autres termes sont dans les J_i avec $i \neq 1$, donc aussi dans I_1 par définition des J_i. (Par exemple, $\beta_2 \in J_2 \subset I_1$. Nous en déduisons $x - x_1 \in I_1$.

L'argument que nous venons de donner pour justifier que $x - x_1 \in I_1$ peut être généralisé à tous les indices. En effet, soit k un indice quelconque ; nous avons

$$x - x_k = (\beta_k - 1)x_k + \sum_{i\neq k} \beta_i x_i \tag{6.58a}$$
$$= -\alpha_k x_k + \sum_{i\neq k} \beta_i x_i; \tag{6.58b}$$

et $\alpha_k \in I_k$ et pour tout $i \neq k$, $\beta_i \in J_i \subset I_k$) ; donc $x - x_k \in I_k$. □

Remarque 6.27.
Ce théorème chinois est bien une généralisation du lemme chinois 6.24. En effet, l'élément x dont il est question est solution du problème $x = x_i \mod I_i$. 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 corollaire 3.14.

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 3.145.

Proposition 6.28.
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 3.109.

Théorème 6.29 (Théorème chinois)**.**
Si P et Q sont deux polynômes premiers entre eux, alors nous avons l'isomorphisme

$$\mathbb{K}[X]/(P, Q) \simeq \mathbb{K}[X]/(P) \times \mathbb{K}[X]/(Q). \tag{6.59}$$

6.3.1 Irréductibilité

Définition 6.30 ([83])**.**
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 3.88 si et seulement s'il est irréductible au sens de la définition 6.30 parce que seules les constantes (non nulles) sont inversibles dans $\mathbb{K}[X]$.

Exemple 6.31
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

$$P = (X^2 + 1)(X^2 + 2), \tag{6.60}$$

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 6.32.
*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.*

Note : les constantes ne sont donc pas des polynômes scindés.

Proposition 6.33 (Critère d'Eisenstein)**.**
Soit le polynôme $P = \sum_{k=0}^{n} a_n X^n$ 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 3.169) 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 (3.112) 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 corollaire 3.179 nous dit alors que P est irréductible sur $\mathbb{Z}[X]$. □

Exemple 6.34
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 $\mathbb{Q}[X]$. △

6.3.2 Idéaux

Soit $P \in \mathbb{K}[X]$ un polynôme. Nous notons (P) l'idéal engendré par P :

$$(P) = \{PR \text{ tel que } R \in \mathbb{K}[X]\}. \tag{6.61}$$

Lemme 6.35.
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. □

Théorème 6.36.
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 3.163 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 3.160 de la division euclidienne[5], 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. □

Nous voyons que n'importe quel polynôme de degré minimum dans un idéal génère l'idéal. Une importante conséquence du théorème 6.36 que nous verrons plus bas est que tout polynôme annulateur d'un endomorphisme est divisé par le polynôme minimal (proposition 11.135).

Corollaire 6.37.
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 6.36, par conséquent la proposition 3.104(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 $\sum_{k=0}^{n-1} a_k \bar{X}^n = 0$ alors un représentant de cette classe doit être de la forme SP dans $\mathbb{K}[X]$, c'est-à-dire

$$\sum_{k=0}^{n-1} a_k X^k = SP, \tag{6.62}$$

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

$$\bar{X}^{n+l} = \bar{X}^n \bar{X}^l = (\bar{P} - \bar{Q})\bar{X}^l = \bar{Q}\bar{X}^l. \tag{6.63}$$

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. □

6.38.
Ce corollaire prendra une nouvelle jeunesse lorsque nous parlerons de polynômes d'endomorphismes, en particulier la proposition 11.145 va donner des précisions.

Lemme 6.39 ([84])**.**
Soit un isomorphisme de corps $\tau : \mathbb{K} \to \mathbb{K}'$. Alors

(1) L'application étendue

$$\begin{aligned} \tau : \mathbb{K}[X] &\to \mathbb{K}'[X] \\ \sum_i a_i X^i &\mapsto \sum_i \tau(a_i) X^i \end{aligned} \tag{6.64}$$

5. Ici $\mathbb{K}$ est un corps et donc l'hypothèse d'inversibilité est automatiquement vérifiée.

est un isomorphisme d'anneaux ;

(2) pour tout $P \in \mathbb{K}[X]$, le passage au quotient

$$\begin{aligned}\phi_\tau\colon \mathbb{K}[X]/(P) &\to \mathbb{K}'[X]/\big(\tau(P)\big)\\ \bar{Q} &\mapsto \overline{\tau(Q)}\end{aligned} \tag{6.65}$$

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 a formule (3.173). 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 :

$$\tau(PQ) = \tau\Big(\sum_k \big(\sum_{l=0}^{k} P_l Q_{k-l}\big)X^k\Big) \tag{6.66a}$$
$$= \sum_k X^k \sum_{l=0}^{k} \tau(P_l Q_{k-l}) \tag{6.66b}$$
$$= \sum_k X^k \sum_{l=0}^{k} \tau(P_l)\tau(Q_{k-l}) \tag{6.66c}$$
$$= \sum_k X^k \sum_{l=0}^{k} \tau(P)_l \tau(Q)_{k-l} \tag{6.66d}$$
$$= \sum_i \big(\tau(P)_i X^i\big) \sum_j \big(\tau(Q)_j X^j\big) \tag{6.66e}$$
$$= \tau(P)\tau(Q). \tag{6.66f}$$

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,

$$\phi_\tau(Q_2) = \overline{\tau(Q_2)} = \overline{\tau(Q_1) + \tau(RP)} \tag{6.67a}$$
$$= \overline{\tau(Q_1) + \tau(R)\tau(P)} \tag{6.67b}$$
$$= \overline{\tau(Q_1)}. \tag{6.67c}$$

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

$$\tau(Q_1) = \tau(Q_2) + R\tau(P) \tag{6.68}$$

pour un certain $R \in \mathbb{K}'[X]$. Vu que $\tau\colon \mathbb{K}[X] \to \mathbb{K}'[X]$ est un isomorphisme, nous pouvons y appliquer τ^{-1} pour trouver :

$$Q_1 = Q_2 + \tau^{-1}(R)P, \tag{6.69}$$

ce qui signifie que $\bar{Q}_1 = \bar{Q}_2$.

Surjection Un élément de $\mathbb{K}'[X]/\big(\tau(P)\big)$ 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 6.40 (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

$$P_1Q_1 + \cdots + P_nQ_n = 1. \tag{6.70}$$

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 :

$$xP + yQ = 0; \tag{6.71}$$

cette dernière pourra être écrite en termes de la matrice de Sylvester, voir sous-section 11.3.7.

Lemme 6.41.
Soient $(P_i)_{i=1,\dots,n} \in \mathbb{K}[X]$ des polynômes étrangers deux à deux. Alors les polynômes

$$Q_i = \prod_{j \neq i} P_j \tag{6.72}$$

sont étrangers entre eux[6]*.*

Lemme 6.42 ([85])**.**
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 $\phi \in \mathbb{A}[X]$.

6.3.4 Lemme et théorème de Gauss

Théorème 6.43 (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 Bézout[7] 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

$$R = PUR + QVR = PUR + VPS = P(UR + VS), \tag{6.73}$$

ce qui signifie que P divise R. □

Le lemme suivant est une généralisation du lemme de Gauss dans $\mathbb{Z}$ (lemme 3.112).

Lemme 6.44 (Lemme de Gauss[57])**.**
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

$$\pi_p \colon \mathbb{Z}[X] \to (\mathbb{Z}/p\mathbb{Z})[X]. \tag{6.74}$$

6. Et non seulement deux à deux.
7. théorème 6.40.

Par définition $abPQ = P_1Q_1 \in \mathbb{Z}[X]$; en prenant la projection,

$$\pi_p(P_1)\pi_p(Q_1) = \pi_p(P_1Q_1) = \pi_P(ab)\pi_p(PQ) = 0 \tag{6.75}$$

parce que $\pi_p(ab) = 0$. Étant donné que $(\mathbb{Z}/p\mathbb{Z})[X]$ est intègre (théorème 3.157), 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. □

6.3.5 Polynômes sur un corps et pgcd

Nous savons qu'un corps est un anneau intègre (lemme 1.64). De plus l'ensemble des polynômes sur un anneau intègre est lui-même un anneau intègre (théorème 3.157). Donc la notion de pgcd à utiliser dans le cas de $\mathbb{K}[X]$ est celle de la définition 1.46.

Lemme 6.45 (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 pgcd[8] *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,

$$\delta_1 = AB\delta_1. \tag{6.76}$$

Mais $\mathbb{K}[X]$ possède la propriété de simplification par la proposition 1.54(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. □

6.46.
En général, lorsque nous dirons « le » pgcd d'un ensemble, nous parlerons du pgcd unitaire, qui existe et est bien défini par le lemme 6.45.

Lemme 6.47 ([86])**.**
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.

⇒ 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 6.40, il existe donc U et V tels que $A_1U + B_1V = 1$. En multipliant par G, nous obtenons l'égalité voulue : $AU + BV = G$.

8. Définition 1.46.

$\Leftarrow$ 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 commun 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 6.48 ([86]).
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 $A \mid P$, 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 6.43 : $B|Q_1$.

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 6.49 ([86]).
Quelques propriétés du PGCD dans les polynômes. Soient des polynômes $P, Q, R \in \mathbb{K}[X]$.

(1) Nous avons l'égalité[9]

$$\operatorname{pgcd}(P, PQ + R) = \operatorname{pgcd}(P, R). \tag{6.77}$$

(2) Si Q et R sont premiers entre eux,

$$\operatorname{pgcd}(P, QR) = \operatorname{pgcd}(P, Q) \operatorname{pgcd}(P, R) \tag{6.78}$$

(3) Si P et Q sont premiers entre eux,

$$\operatorname{pgcd}(P, QR) = \operatorname{pgcd}(P, R) \tag{6.79}$$

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

$$R = AB_2 - PQ = AB_2 - AB_1Q = A(B_2 - B_1Q), \tag{6.80}$$

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

$$PQ + R = AB_1Q + AB_2 = A(B_1Q + B_2), \tag{6.81}$$

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 : $G_1 = \operatorname{pgcd}(P, Q)$ et $G_2 = \operatorname{pgcd}(P, R)$. Il faut montrer que G_1G_2 est le pgcd de P et QR ; pour cela nous allons utiliser le lemme 6.47.

9. Notez l'analogie avec le lemme 3.18.

$\exists U, V$ **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 6.47). On a de même : $G_2 = PU_2 + RV_2$. En prenant le produit :

$$G_1G_2 = (PU_1 + QV_1)(PU_2 + RV_2) = P(PU_1U_2 + RU_1V_2 + QV_1V_2) + QR(V_1V_2). \quad (6.82)$$

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 3.11).

$G_1G_2 \mid QR$ En effet : $G_1|Q$ et $G_2|R$ donc $G_1G_2|QR$.

$G_1G_2 \mid P$ 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 6.48 conclu 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 6.40 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 :

$$1 = PU + QV = AB_1U + QV. \quad (6.83)$$

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 $A|R$ par le théorème de Gauss 6.43.

Dans l'autre sens, si $A|R$ alors on a évidemment : $A|QR$.

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 6.50.
Soit $\mathbb{L}$ un corps[10] *fini et $\mathbb{K}$ un sous corps de $\mathbb{L}$. Alors il existe $s \in \mathbb{N}$ tel que*

$$\text{Card}(\mathbb{L}) = \text{Card}(\mathbb{K})^s. \quad (6.84)$$

Démonstration. Le corps $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel de dimension finie. Si s est la dimension alors nous avons la formule (6.84) parce que chaque élément de $\mathbb{L}$ est un s-uple d'éléments de $\mathbb{K}$. □

Définition 6.51 ([87])**.**
Soit $\mathbb{K}$ un corps commutatif. Une ***extension*** *de $\mathbb{K}$ est un couple $(\mathbb{L}, j)$ où $\mathbb{L}$ est un corps et $j : \mathbb{K} \to \mathbb{L}$ 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 $\mathbb{K}$.

Définition 6.52.
Une extension est ***algébrique*** *de $\mathbb{K}$ est une extension dont tous les éléments sont racines de polynômes dans $\mathbb{K}[X]$.*

Exemple 6.53
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. △

10. Définition 1.61.

Lemme 6.54.
Si $(\mathbb{L}, i)$ est une extension de $\mathbb{K}$, alors $\mathbb{L}$ est un espace vectoriel sur $\mathbb{K}$.

Démonstration. Il faut définir le produit d'un élément de $\mathbb{L}$ par un élément de $\mathbb{K}$; si $\lambda \in \mathbb{K}$ et $x \in \mathbb{L}$ nous la définissons par

$$\lambda \cdot x = i(\lambda)x \tag{6.85}$$

où la multiplication du membre de droite est celle du corps $\mathbb{L}$. □

Définition 6.55.
*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 6.56
L'ensemble $\mathbb{C}$ est une extension de $\mathbb{R}$ et son degré est $[\mathbb{C} : \mathbb{R}] = 2$. △

Proposition 6.57 (Composition des degrés[88])**.**
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 :

$$[\mathbb{L}_2 : \mathbb{K}] = [\mathbb{L}_2 : \mathbb{L}_1][\mathbb{L}_1 : \mathbb{K}]. \tag{6.86}$$

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 (6.86) 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

$$a = \sum_\alpha a_\alpha w_\alpha \tag{6.87}$$

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 :

$$a = \sum_{\alpha i} a_{\alpha i} v_i w_\alpha, \tag{6.88}$$

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

$$\sum_{\alpha i} a_{\alpha i} v_i w_\alpha = 0. \tag{6.89}$$

En récrivant sous la forme

$$\sum_\alpha \Big(\sum_i a_{\alpha i} v_i \Big) w_\alpha = 0, \tag{6.90}$$

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 : $a_{\alpha i} = 0$. □

6.4.1 Un petit exemple d'extension algébrique

Nous avons défini le concept d'extension algébrique en 6.52. Nous allons en construire un petit exemple très piéton.

D'abord la proposition 1.130 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 1.87. Cela étant posé, nous y allons.

Proposition 6.58 ([89]).
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 1.37) 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 $a, b, a', b' \in \mathbb{Q}$,

$$(a + b\sqrt{2}) + (a'b'\sqrt{2}) = (a + a') + (b + b')\sqrt{2} \in \mathbb{L}. \tag{6.91}$$

— Les neutres 0 et 1 sont dans $\mathbb{L}$.

— Si $\alpha \in \mathbb{L}$, alors $-\alpha \in \mathbb{L}$:

$$-(a + b\sqrt{2}) = -a - b\sqrt{2}. \tag{6.92}$$

— La partie $\mathbb{L}$ est stable pour le produit parce que

$$(a + b\sqrt{2})(a' + b'\sqrt{2}) = (aa' + 2bb') + (ab' + ba')\sqrt{2}. \tag{6.93}$$

— 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 1.95. Donc pour tout $a, b \in \mathbb{R}$, le nombre

$$\frac{1}{a + b\sqrt{2}} \tag{6.94}$$

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 1.87. Nous pouvons donc faire le coup de multiplier le numérateur et le dénominateur par le binôme conjugué :

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}. \tag{6.95}$$

Cela est un rationnel. Donc le 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 $\mathbb{L}$. □

Proposition 6.59.
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 $\mathbb{Q}[X]$.

□

6.4.2 Extension algébrique et polynôme minimal

Lemme-définition 6.60 (Polynôme minimal)**.**
Soit $\mathbb{L}$ une extension de $\mathbb{K}$ et $a \in \mathbb{L}$. Nous considérons la partie

$$I_a = \{P \in \mathbb{K}[X] \text{ tel que } P(a) = 0\} \tag{6.96}$$

que nous supposons non réduite à $\{0\}$ [11]

(1) La partie I_a est un idéal principal dans $\mathbb{K}[X]$

(2) L'idéal I_a possède un unique générateur unitaire.

*Cet unique générateur unitaire est le **polynôme minimal** de a sur $\mathbb{K}$.*

Démonstration. Le fait que I_a soit un idéal est la définition du produit sur l'anneau des polynômes. Le théorème 6.36 fait le reste du travail : nous savons que $\mathbb{K}[X]$ est un anneau principal et donc que tous ses idéaux sont principaux (c'est la définition).

Le théorème 6.36 dit également que I_a possède un unique générateur unitaire. □

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 ». En effet, il n'existe peut-être pas de polynôme annulateur.

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 $\mathbb{Q}[X]$. △

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 [12] *sur $\mathbb{K}$;*

(2) Le polynôme μ_a est premier [13] *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 inversibles [14]. 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

$$0 = P(a)Q(a). \tag{6.97}$$

Vu que nous sommes sur un corps, nous avons la règle du produit nul [15] 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 récrivant $\mu_a = PQ$ avec cela nous avons :

$$\mu_a = S\mu_a Q \tag{6.98}$$

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.

11. 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.
12. Définition 6.30.
13. Définition 3.164.
14. Et d'ailleurs, le sont, mais ce n'est pas important ici.
15. Parce que un corps est un anneau intègre par le lemme 1.64 et qu'un anneau intègre est justement un anneau sur lequel nous avons la règle du produit nul, voir la définition 1.54.

(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

$$0 = \mu_a(a) = P(a)k, \tag{6.99}$$

donc $P(a) = 0$. Mais alors

$$Q(a) = P(a)R_2(a) = 0, \tag{6.100}$$

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 $\mathbb{Q}$.*

Lemme 6.64.
Soient un corps $\mathbb{K}$, une extension $\mathbb{L}$ de $\mathbb{K}$ et $\alpha \in \mathbb{L}$, un élément algébrique sur $\mathbb{K}$. Si μ est le polynôme minimal de α sur $\mathbb{K}$ alors

$$\begin{aligned}\varphi\colon \mathbb{K}[\alpha] &\to \mathbb{K}[X]/(\mu)\\ Q(\alpha) &\mapsto \bar{Q}\end{aligned} \tag{6.101}$$

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 6.60.

Ensuite, le fait que $\mathbb{K}[X]/(\mu)$ soit un corps est le corollaire 6.37. 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 le proposition 3.156. 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

$$Q_1(\alpha) = Q_2(\alpha) + R(\alpha), \tag{6.102}$$

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 $\varphi\big(kQ(\alpha)\big) = \overline{kQ}$. 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 $\varphi\big(Q_1(\alpha) + Q_2(\alpha)\big) = \varphi\big((Q_1 + Q_2)(\alpha)\big) = \overline{Q_1 + Q_2} = \bar{Q}_1 + \bar{Q}_2$.

□

Proposition 6.65 ([33]).
Soit une extension algébrique[16] *$\mathbb{L}$ du corps $\mathbb{K}$.*

16. Définition 6.52.

(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 6.52 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 6.60 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 $\mu_1 = \mu$. □

6.4.3 Extensions algébriques et éléments transcendants

6.4.3.1 Élements algébriques et transcendants

Lemme-définition 6.66 ([90])**.**
Soit une extension $\mathbb{L}$ de $\mathbb{K}$ et $\alpha \in \mathbb{L}$. Nous considérons l'application

$$\begin{aligned}\varphi\colon \mathbb{K}[X] &\to \mathbb{L}\\ P &\mapsto P(\alpha).\end{aligned} \tag{6.103}$$

Alors

(1) *L'application φ est un morphisme d'anneaux*[17]*.*

(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 3.148 déjà prouvé.

Pour le morphisme de $\mathbb{K}$-espace vectoriel, il faut seulement ajouter le calcul

$$\varphi(\lambda P) = (\lambda P)(\alpha) = \lambda P(\alpha) = \lambda\varphi(P). \tag{6.104}$$

Notons la justification suivante qui n'est pas tout à fait triviale :

$$(\lambda P)(\alpha) = \sum_k (\lambda P)_k \alpha^k = \sum_k \lambda P_k \alpha^k = \lambda P(\alpha) \tag{6.105}$$

qui utilise la définition 3.146. □

Exemple 6.67
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 abstraire que la définition.

17. Définition 1.38.

Lemme 6.68.
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 $P(a) = 0$.

Il est bon de remarquer que cette définition est équivalente à celle donnée dans le lemme-définition 6.66 ...

Démonstration. Nous considérons l'application φ de la définition 6.66. 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 6.69.
*Soit $\mathbb{K}$ un corps et $\mathbb{L}$ une extension de $\mathbb{K}$. On dit que l'extension est **algébriquement close** si tout polynôme non-constant à coefficients dans $\mathbb{K}$ admet des racines dans $\mathbb{L}$.*

Définition 6.70.
*Une **clôture algébrique** du corps $\mathbb{K}$ est une extension algébriquement close de $\mathbb{K}$ dont tous les éléments sont algébriques sur $\mathbb{K}$.*

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 6.71.
Le corps $\mathbb{C}$ n'est pas une clôture algébrique 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 1.82. 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 1.29. Enfin l'ensemble des polynômes à coefficients sur $\mathbb{Q}$ est l'union des polynômes de degré fixés, donc dénombrable par la proposition 1.30.

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 corollaire 3.178. 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. □

L'existence d'une clôture algébrique pour tout corps est le théorème de Steinitz.

6.4.4 Extensions et polynômes

Nous savons déjà depuis la définition 3.145 ce qu'est $A[X]$ pour tout anneau A et donc a fortiori pour un corps.

Définition 6.72.
Soit un corps commutatif[18]. Nous notons $\mathbb{K}(X)$ le corps des fractions[19] de $\mathbb{K}[X]$.

Lemme-définition 6.73.
Si $R \in \mathbb{K}(X)$, avec $R = P/Q$ et si $\mathbb{L}$ est une extension[20] de $\mathbb{K}$ contenant l'élément α, alors nous définissons

$$R(\alpha) = P(\alpha)Q(\alpha)^{-1}. \tag{6.106}$$

Cela est une bonne définition au sens où elle ne dépend pas du choix du représentant (P, Q) pris dans la classe P/Q.

18. Sauf mention du contraire, tous les corps du Frido sont commutatifs.
19. Définition 1.67.
20. Définition 6.51.

Démonstration. Supposons $R = P_1/Q_1 = P_2/Q_2$. Par définition des classes (définition 1.67) nous avons

$$P_1Q_2 = Q_1P_2. \tag{6.107}$$

Vu que l'évaluation est un morphisme $\mathbb{K}[X] \to \mathbb{K}$ [21] nous pouvons évaluer l'équation (6.107) en α :

$$P_1(\alpha)Q_2(\alpha) = Q_1(\alpha)P_2(\alpha). \tag{6.108}$$

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

$$P_1(\alpha)Q_1(\alpha)^{-1} = P_2(\alpha)Q_2(\alpha)^{-1}, \tag{6.109}$$

c'est-à-dire

$$(P_1/Q_1)(\alpha) = (P_2/Q_2)(\alpha). \tag{6.110}$$

□

Proposition-définition 6.74 ([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

(1) $\mathbb{K}(\alpha)_{\mathbb{L}}$ est un sous-corps de $\mathbb{L}$,

(2) $\mathbb{K}(\alpha)_{\mathbb{L}}$ est une extension [22] 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 une homomorphisme de corps $j : \mathbb{K} \to \mathbb{K}(\alpha)_{\mathbb{L}}$. 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 $j_{\mathbb{L}}$. □

Lemme 6.75.
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

$$\alpha = x + y\sqrt{n}. \tag{6.111}$$

Exemple 6.76
Nous avons

$$\mathbb{Q}(\sqrt{2})_{\mathbb{R}} = \{a + b\sqrt{2}\}_{a,b\in\mathbb{Q}} \tag{6.112}$$

où à droite nous calculons les sommes et 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 $\sqrt{2}\sqrt{2} = 2$. △

Lemme 6.77.
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 corps [23]

$$\psi : \mathbb{Q}(\sqrt{2})_{\mathbb{R}} \to \mathbb{Q}(\sqrt{3})_{\mathbb{R}}. \tag{6.113}$$

21. Lemme 3.148. Certes ce lemme ne parle que d'anneaux, mais à y bien penser, dans le passage de (6.107) à (6.107), nous ne considérons que les structures d'anneaux sur $\mathbb{K}[X]$ et $\mathbb{K}$.
22. Définition 6.51.
23. Définition 1.38. Oui, c'est un bête morphisme d'anneaux. Il n'y a pas plus de structure dans un corps que dans un anneau.

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

$$\psi(\alpha)^2 - 1 = \psi(\alpha^2) - \psi(1) = \psi(\alpha^2 - 1) = \psi(0) = 0. \tag{6.114}$$

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 $\mathbb{Q}(\sqrt{3})_{\mathbb{R}}$. □

Exemple 6.78

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 évidemment [24] $\mathbb{K}(\alpha)_{\mathbb{L}_2} = \mathbb{K}(\alpha)_{\mathbb{L}}$.

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

$$\{a + b\sqrt{2}\}_{a,b\in\mathbb{Q}}, \tag{6.115}$$

de $\mathbb{R}$.

Mais cette fois nous définissons la multiplication suivante :

$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + 3bd + (ad + bc)\sqrt{2}. \tag{6.116}$$

Cela est un corps parce que tout élément non nul est inversible. En effet, l'équation

$$(a + b\sqrt{2})(x + y\sqrt{2}) = 1 \tag{6.117}$$

donne

$$\begin{pmatrix} a & 3b \\ b & a \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \tag{6.118}$$

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

$$a^2 - 3b^2 = 0. \tag{6.119}$$

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 (6.117) soit satisfaite.

Tout cela nous a donné une 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

$$\begin{aligned} \psi\colon \mathbb{K} &\to \mathbb{Q}(\sqrt{3})_{\mathbb{R}} \\ a + b\sqrt{2} &\mapsto q + b\sqrt{3} \end{aligned} \tag{6.120}$$

est un isomorphisme de corps. Pour le produit, nous avons

$$\begin{aligned} \psi\big((a + b\sqrt{2})(c + d\sqrt{2})\big) &= \psi\big(qc + 3bd + (ad + bc)\sqrt{2}\big) && \text{(6.121a)} \\ &= ac + 3bd + (ad + bc)\sqrt{3} && \text{(6.121b)} \\ &= (a + b\sqrt{3})(c + d\sqrt{3}) && \text{(6.121c)} \\ &= \psi(a + b\sqrt{2})\psi(c + d\sqrt{2}). && \text{(6.121d)} \end{aligned}$$

Remarques :

— L'application ψ est bien définie grâce au lemme 6.75 couplé au théorème 3.36 appliqué à $n = 2$ et $n = 3$.

24. Vérifiez-le tout de même.

— Dans le membre de gauche de (6.121a), $b\sqrt{2}$ est un produit dans $\mathbb{R}$ (d'où l'importance du lemme 6.75 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 (6.121b) et (6.121c), tous les produits sont dans $\mathbb{R}$.

En comparant avec le lemme 6.77, nous avons alors

$$\mathbb{Q}(\sqrt{2})_{\mathbb{K}} = \mathbb{Q}(\sqrt{3})_{\mathbb{R}} \neq \mathbb{Q}(\sqrt{2})_{\mathbb{R}} \tag{6.122}$$

△

6.79.
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 a 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 réellement [25]), 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 6.80 ([1])**.**
Soit une extension $\mathbb{L}$ du corps $\mathbb{K}$ et $\alpha \in \mathbb{L}$. Alors nous avons les isomorphismes de corps suivants :

(1) $\mathbb{K}(\alpha)_{\mathbb{L}} = \text{Frac}\left(\mathbb{K}[\alpha]_{\mathbb{L}}\right)$,

(2) $\mathbb{K}(\alpha)_{\mathbb{L}} = \{R(\alpha)_{\mathbb{L}}$ *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 1.68 nous dit alors que l'application suivante est un morphisme injectif de corps :

$$\begin{aligned} \epsilon\colon \text{Frac}\left(\mathbb{K}[\alpha]\right) &\to \mathbb{K}(\alpha) \\ P/Q &\mapsto PQ^{-1}. \end{aligned} \tag{6.123}$$

Pour rappel, la notation P/Q est bien une notation pour la classe d'équivalence du couple (P,Q) pour la relation définie en 1.67.

Par ailleurs, la partie $\epsilon\Big(\text{Frac}\left(\mathbb{K}[\alpha]\right)\Big)$ est inclue 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

$$\mathbb{K}(\alpha) \subset \epsilon\Big(\text{Frac}\left(\mathbb{K}[\alpha]\right)\Big). \tag{6.124}$$

L'application ϵ est donc surjective sur $\mathbb{K}(\alpha)$. Vu qu'elle était déjà injective, elle est bijective.

25. En lisant quelque pages de Wikipédia, vous pourrez briller en société, mais ne tentez pas le coup à l'agrégation.

Pour la seconde partie, veuillez lire la définition 1.69 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

$$R(\alpha) = P(\alpha)Q(\alpha)^{-1}. \tag{6.125}$$

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

$$\{R(\alpha) \text{ tel que } R \in \mathbb{K}(X)\} \subset \mathbb{K}(\alpha). \tag{6.126}$$

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. □

Pourquoi cela ne contredit pas l'exemple 6.78 ? Lorsque nous écrivons

$$\mathbb{K}(\alpha) = \{R(\alpha) \text{ tel que } R \in \mathbb{K}(X)\}, \tag{6.127}$$

certes $\mathbb{K}(X)$ 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 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 6.78, et en réalité $\mathbb{K}(\alpha)$ peut ne pas être ce que l'on croit.

Le corollaire suivant montre que les choses s'arrangent.

Corollaire 6.81.
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

$$\mathbb{K}(\alpha)_{\mathbb{L}_1} = \mathbb{K}(\alpha)_{\mathbb{L}_2}. \tag{6.128}$$

Démonstration. La proposition 6.80 nous dit que

$$\mathbb{K}(\alpha)_{\mathbb{L}_1} = \{R(\alpha)_{\mathbb{L}_1} \text{ tel que } R \in \mathbb{K}(X)\} \tag{6.129a}$$
$$\mathbb{K}(\alpha)_{\mathbb{L}_2} = \{R(\alpha)_{\mathbb{L}_2} \text{ tel que } R \in \mathbb{K}(X)\}. \tag{6.129b}$$

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. □

Ce que ce corollaire 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 6.82.
Soit un corps $\mathbb{K}$, une extension $\mathbb{L}$ et un élément $\alpha \in \mathbb{L}$. Nous considérons l'application

$$\begin{aligned} \varphi\colon \mathbb{K}[X] &\to \mathbb{L} \\ P &\mapsto P(\alpha). \end{aligned} \tag{6.130}$$

(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 minimal[26] de α sur $\mathbb{K}$.

Démonstration. Point par point.

26. Définition 6.60.

(1) Nous savons que $\mathbb{K}[\alpha] = \{Q(\alpha) \text{ tel que } Q \in \mathbb{K}[X]\}$ (c'est la proposition 3.156). Donc φ est surjective sur $\mathbb{K}[\alpha]$, et est donc bijective. Elle est un isomorphisme [27] parce que le lemme 6.66 dit déjà que c'est un morphisme.

(2) Nous supposons encore que α est transcendant et nous considérons l'application

$$\begin{aligned}\psi\colon \mathbb{K}(X) &\to \mathbb{K}(\alpha)\\ P &\mapsto R(\alpha).\end{aligned} \tag{6.131}$$

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 6.80(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 $\mathbb{K}(X) = \text{Frac}\big(\mathbb{K}[X]\big)$.

(3) C'est le lemme-définition 6.60.

□

Proposition 6.83.
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 divise [28] *tout polynôme annulateur.*

Autrement dit, l'idéal engendré par le polynôme minimal est l'idéal des polynômes annulateurs.

Démonstration. Nous considérons l'idéal

$$I = \{Q \in \mathbb{K}[X] \text{ tel que } Q(a) = 0\}. \tag{6.132}$$

Le fait que cela soit un idéal est simplement dû à la définition du produit : $(PQ)(a) = P(a)Q(a)$. Par le théorème 6.36, 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 6.84.
Toute extension finie est algébrique.

Démonstration. Soient un corps $\mathbb{K}$, une extension $\mathbb{L}$ de degré [29] 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 6.85 (Propriétés d'extensions algébriques[1])**.**
Soit $\mathbb{K}$ un corps commutatif [30] *et a un élément algébrique sur $\mathbb{K}$, de polynôme minimal μ_a de degré n. Alors*

27. 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 ».
28. Définition 3.161.
29. Définition 6.55.
30. Juste en passant nous rappelons que tous les corps considérés ici sont commutatifs

(1) *En considérant l'application d'évaluation*

$$\begin{aligned}\varphi_a\colon \mathbb{K}[X] &\to \mathbb{L}\\ Q &\mapsto Q(a),\end{aligned} \tag{6.133}$$

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 :*

$$\big[\mathbb{K}[a] : \mathbb{K}\big] = n. \tag{6.134}$$

(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) $\mathbb{K}[a] \simeq \mathbb{K}[X]/(\mu_a)$ *(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.

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 6.60, 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 :

$$Q(X) = Q_1(X) + X^n Q_2(X) \tag{6.135}$$

où Q_1 est de degré $n-1$ et Q_2 de degré $p-n$. Nous évaluons cette égalité en a :

$$Q(a) = Q_1(a) + S(a)Q_2(a). \tag{6.136}$$

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 6.40 affirme l'existence d'éléments $U, V \in \mathbb{K}[X]$ tels que

$$U\mu_a + VQ = 1 \tag{6.137}$$

dans $\mathbb{K}[X]$. Nous évaluons cette égalité en a en tenant compte de $\mu_a(a) = 0$ dans $\mathbb{K}[a]$:

$$U(a)\mu_a(a) + V(a)Q(a) = 1 \tag{6.138}$$

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

$$\begin{aligned}\psi\colon \mathbb{K}[X]/(\mu_a) &\to \mathbb{K}[a]\\ \bar{R} &\mapsto R(a)\end{aligned} \tag{6.139}$$

et nous montrons qu'elle convient. Pour cela, nous nous souvenons que la proposition 6.83 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 3.41 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 est polynômes annulateurs de a. Donc $R \in (\mu_a)$ et nous avons $\bar{R} = 0$ dans $\mathbb{K}[X]/(\mu_a)$.

□

Exemple 6.86
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 6.85. Du point de vue de Bézout, $\mu_{\sqrt{2}}(X) = X^2 - 2$, et nous cherchons des polynômes U et V tels que

$$U(X^2 - 2) + VX = 1. \tag{6.140}$$

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 $\sqrt{2}$:

$$V(\sqrt{(2)}) = \frac{1}{2}\sqrt{2}. \tag{6.141}$$

△

Lemme 6.87 ([91]).
Un nombre complexe algébrique dont tous les conjugués sont de module 1 *est une racine de l'unité.*

Proposition 6.88 ([90]).
Soient un corps $\mathbb{K}$*, un 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 affirmation sont vraies, alors $[\mathbb{K}(\alpha) : \mathbb{K}]$ *est le degré du polynôme minimal de* α *sur* $\mathbb{K}$*.*

Problèmes et choses à faire

Il y a des redites avec la propriété 6.85 : une meilleure articulation est sans doute possible.

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 6.60). Nous savons par le lemme 6.64 (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 3.102 dit que (μ) est un idéal maximum ; la proposition 3.104 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 6.82(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 6.64 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 6.82. Or $\mathbb{K}[X]$ n'est pas de dimension finie sur $\mathbb{K}$, donc $\mathbb{K}[\alpha]$ non plus.

□

Lemme 6.89 ([92])**.**
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 6.90.
Soit $\mathbb{L}$ une extension de $\mathbb{K}$ et $A \subset \mathbb{L}$.

(1) Nous notons $\mathbb{K}(A)$ le plus petit sous corps de $\mathbb{L}$ contenant $\mathbb{K}$ et A. C'est l'intersection de tous les sous-corps de $\mathbb{L}$ contenant A.

(2) Nous notons $\mathbb{K}[A]$ le plus petit sous anneau de $\mathbb{L}$ contenant $\mathbb{K}$ et A. C'est l'intersection de tous les sous-anneaux de $\mathbb{L}$ contenant A.

*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 6.91.
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 a priori de parler de corps engendré par A sans dire dans quel corps plus grand nous nous plaçons.

Exemple 6.92
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. △

Exemple 6.93
Nous avons déjà vu à l'occasion de la définition 3.145 que $A[X]$ est l'anneau de tous les polynômes de degré fini en X. Cela rentre dans le cadre de la définition 6.90 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 dedans[31]. Par contre, $\mathbb{K}(X)$ est un corps parce qu'il contient également les fractions rationnelles. △

Exemple 6.94
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

31. Lorsqu'on multiplie, les degrés montent toujours.

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 $x \in \mathbb{F}_p$. △

Lemme 6.95.
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 corollaire 6.37. Nous identifions $\mathbb{K}$ avec $\phi(\mathbb{K})$ où

$$\phi\colon \mathbb{K}[X] \to \mathbb{L} \tag{6.142}$$

est la projection canonique. Nous considérons également $a = \phi(X)$.

Nous avons alors $P(a) = 0$ dans $\mathbb{L}$. En effet $P(a) = P\big(\phi(X)\big)$ 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 $\mathbb{L}$.

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 $Q = \sum_i Q_i a^i$. □

Proposition 6.96 ([33]).
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

$$I_a = \{Q \in \mathbb{K}[X] \text{ tel que } Q(a) = 0\}; \tag{6.143a}$$
$$I_b = \{Q \in \mathbb{K}[X] \text{ tel que } Q(b) = 0\}. \tag{6.143b}$$

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

$$P = \mu_a Q. \tag{6.144}$$

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 pourait 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 (6.144) 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. □

Exemple 6.97
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 $\mu_2 = X^2 + 2$. Nous avons effectivement $\mu_a\mu_b$ divise P dans $\mathbb{R}[X]$.

Si par contre nous considérions 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. △

6.4.5 Racines de polynômes

Corollaire 6.98 (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 6.83 : 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. □

Avant de lire l'énoncé suivant, allez relire la définition 3.154 pour savoir ce qu'est un polynôme nul.

Théorème 6.99 (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

$$\begin{cases} a\alpha + b = 0 & \text{(6.145a)} \\ a\beta + b = 0. & \text{(6.145b)} \end{cases}$$

La différence entre les deux donne $a(\alpha - \beta) = 0$. Vu que $\alpha \neq \beta$, la règle du produit nul (lemme 1.64) 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 corollaire 6.98 nous donne un polynôme Q de degré n tel que

$$P = (X - \alpha_1)Q. \tag{6.146}$$

Étant donne que pour tout $i \neq 1$ nous avons $\alpha_i \neq \alpha_1$,

$$0 = P(\alpha_i) = \underbrace{(\alpha_i - \alpha_1)}_{\neq 0} Q(\alpha_i), \tag{6.147}$$

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 (6.146) sont alors également nuls. □

Problèmes et choses à faire

On a déjà utilisé par ailleurs le fait qu'un polynôme ayant davantage de racines que son degré s'annule. Donc ce théorème doit être énoncé et prouvé plus haut.

Exemple 6.100
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 6.158 une condition pour qu'un polynôme à plusieurs variables s'annule du fait qu'il ait « trop » de racines. △

Remarque 6.101.
L'intérêt du théorème 6.99 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 14.24.

6.4.6 Corps de rupture

Définition 6.102.
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 $\mathbb{L} = \mathbb{K}(a)$.*

6.103.
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 6.4.10 et surtout dans la question (2) des questions difficiles d'algèbre.

Définition 6.104 (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 $\mathbb{L}[X]$.*

Exemple 6.105
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 $\mathbb{L}$:

$$P = (X - \sqrt{2})(X + \sqrt{2}). \tag{6.148}$$

Le corps $\mathbb{Q}(\sqrt{2})$ est donc un corps de rupture pour P. △

Exemple 6.106
Dans l'exemple 6.105, nous avions un corps de rupture dans lequel le polynôme P était scindé. Il n'en est pas toujours ainsi. Prenons

$$P = X^3 - 2 \tag{6.149}$$

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. △

Exemple 6.107
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. △

Vu que nous allons abondamment parler du quotient $\mathbb{K}[X]/(P)$, nous nous permettons un petit lemme.

Lemme 6.108.
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 44. D'abord $\mathbb{K}[X]$ est un anneau principal par le lemme 3.163. 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 3.102).

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. □

Proposition 6.109 (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 6.51). Le fait que ce soit un corps est le lemme 6.108. Le morphisme $j\colon \mathbb{K} \to \mathbb{K}[X]/(P)$ 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 1.66).

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 3.13.2.2, 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 $(0, 1, 0, 0, \ldots)$.

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 (3.183). 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 $P(\bar{X}) = \sum_k a_k \bar{X}^k = \sum_k a_k \overline{X^k}$, et

$$P(\bar{X}) = \overline{P(X)} = \bar{P} = 0. \tag{6.150}$$

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 3.152 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 6.110
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 :

$$(X + \bar{X})(X - \bar{X}) = X^2 - \bar{X}^2 = X^2 + 1, \tag{6.151}$$

c'est-à-dire que P est bien factorisé, et que nous avons retrouvé la multiplication $x^2 + 1 = (x + i)(x - i)$. △

6.111.
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

$$P = X^4 - X^2 - 2 \tag{6.152}$$

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 $\mathbb{Q}(i)$.

6.112.
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 6.113 ([84]).
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

$$\psi\colon \mathbb{K}[X]/(P)\to\mathbb{L} \tag{6.153}$$

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 6.60 s'applique donc et nous avons le polynôme minimal μ de α dans $\mathbb{K}[X]$. Il divise P qui est irréductible, donc

$$P=\lambda\mu \tag{6.154}$$

pour un certain $\lambda\in\mathbb{K}$.

Nous posons

$$\begin{aligned}\psi\colon \mathbb{K}[X]/(P)&\to\mathbb{L}\\ \bar{Q}&\mapsto Q(\alpha).\end{aligned} \tag{6.155}$$

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

$$\psi(\bar{X})=X(\alpha)=\alpha. \tag{6.156}$$

En ce qui concerne l'unicité, fixer $\psi(\bar{X})$ est suffisant pour fixer un morphisme. En effet si $\psi(\bar{X})=\alpha$, alors

$$\psi(\bar{Q})=\psi\Big(\sum_k a_k\bar{X}^k\Big)=\sum_k a_k\psi(\bar{X})^k=\sum_k a_k\alpha^k. \tag{6.157}$$

Pour le second point de l'énoncé, il faut remarquer que α est algébrique et non transcendant. Donc en utilisant les propositions 3.156 et 6.85(5) nous trouvons

$$\text{Image}(\psi)=\{Q(\alpha)\text{ tel que }Q\in\mathbb{K}[X]\}=\mathbb{K}[\alpha]=\mathbb{K}(\alpha). \tag{6.158}$$

Et finalement pour le dernier point, un morphisme de corps est toujours injectif. Si il est également surjectif, il sera bijectif. □

6.4.7 Pile d'extensions

Lemme 6.114 ([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

$$\mathbb{L}_1=\mathbb{K}(\alpha_1)_{\mathbb{L}_1} \tag{6.159}$$

et

$$\mathbb{L}_k = \mathbb{L}_{k-1}(\alpha_k)_{\mathbb{L}_k}. \tag{6.160}$$

Alors

$$\mathbb{L}_n = \mathbb{K}(\alpha_1, \dots, \alpha_n)_{\mathbb{L}_n}. \tag{6.161}$$

Démonstration. Nous démontrons par récurrence sur n. Le cas $n = 1$ est simplement l'hypothèse (6.159).

Supposons donc que le lemme soit correct pour n, et étudions le cas $n + 1$. Nous avons, par définition et par hypothèse de récurrence :

$$\mathbb{L}_{n+1} = \mathbb{L}_n(\alpha_{n+1})_{\mathbb{L}_{n+1}} = \Big(\mathbb{K}(\alpha_1, \dots, \alpha_n)_{\mathbb{L}_n}\Big)(\alpha_{n+1})_{\mathbb{L}_{n+1}}. \tag{6.162}$$

Notre tâche sera donc de montrer que

$$\Big(\mathbb{K}(\alpha_1, \dots, \alpha_n)_{\mathbb{L}_n}\Big)(\alpha_{n+1}) = \mathbb{K}(\alpha_1, \dots, \alpha_{n+1}) \tag{6.163}$$

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

$$\mathbb{K}(\alpha_1, \dots, \alpha_{n+1}) \subset \big(\mathbb{K}(\alpha_1, \dots, \alpha_n)_{\mathbb{L}_n}\big)(\alpha_{n+1})_{\mathbb{L}_{n+1}}. \tag{6.164}$$

Il faut donc prouver l'inclusion inverse ; c'est-à-dire montrer que tout élément x du corps $\big(\mathbb{K}(\alpha_1, \dots, \alpha_n)_{\mathbb{L}_n}\big)(\alpha_{n+1})$ 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 6.80(2), de la forme $r(\alpha_{n+1})$ avec $r \in \mathbb{K}(\alpha_1, \dots, \alpha_n)(X)$, c'est-à-dire

$$P(\alpha_{n+1})Q(\alpha_{n+1})^{-1} \tag{6.165}$$

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

$$P(\alpha_{n+1}) = \sum_i a_i \alpha_{n+1}^i. \tag{6.166}$$

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

$$r(\alpha_{n+1}) = P(\alpha_{n+1})Q(\alpha_{n+1})^{-1}. \tag{6.167}$$

On vient ainsi de montrer que tout élément $x \in \big(\mathbb{K}(\alpha_1, \dots, \alpha_n)_{\mathbb{L}_n}\big)(\alpha_{n+1})$ 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 :

$$\big(\mathbb{K}(\alpha_1, \dots, \alpha_n)_{\mathbb{L}_n}\big)(\alpha_{n+1})_{\mathbb{L}_{n+1}} \subset \mathbb{K}(\alpha_1, \dots, \alpha_{n+1}). \tag{6.168}$$

Les inclusions (6.164) et (6.168) prouvent l'égalité d'ensembles (6.163) que nous voulions montrer. □

6.4.8 Polynômes à plusieurs variables

Nous avons déjà vu $A[X, Y]$ lorsque A est un anneau en la définition 3.182.

Définition 6.115.
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 6.116.
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.

La proposition suivante est analogue à 6.80(2).

Lemme 6.117 ([1])**.**
Soient un corps $\mathbb{K}$, une extension $\mathbb{L}$ et des éléments $\alpha_1,\dots,\alpha_n$ dans $\mathbb{L}$. Alors

$$\mathbb{K}(\alpha_1,\dots,\alpha_n)=\{r(\alpha_1,\dots,\alpha_n)\text{ tel que }r\in\mathbb{K}(X_1,\dots,X_n)\}. \tag{6.169}$$

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

$$\mathbb{K}(\alpha_1,\dots,\alpha_n)\subset\big\{r(\alpha_1,\dots,\alpha_n)\text{ tel que }r\in\mathbb{K}(X_1,\dots,X_n)\big\}. \tag{6.170}$$

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 $r\in\mathbb{K}[X_1,\dots,X_n]$. □

6.4.9 Corps de décomposition

Définition 6.118.
*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 6.119 ([93])**.**
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 corollaire 6.98 nous permet de factoriser $X-\alpha$:

$$P=(X-\alpha)Q \tag{6.171}$$

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 6.109 qui donne l'existence d'un corps de rupture). Dans $\mathbb{L}_1$ nous avons

$$P=(X-\alpha)Q \tag{6.172}$$

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

$$\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_{n-1}). \tag{6.173}$$

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

$$\mathbb{D} = \mathbb{K}(\alpha_1, \dots, \alpha_{n-1}, \alpha) \tag{6.174}$$

est un corps de décomposition de P. Vu que $\mathbb{D}$ contient $\mathbb{K}(\alpha)$ (comme cas particulier du lemme 6.117), 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

$$Q = (X - \alpha_1) \dots (X - \alpha_{n-1}). \tag{6.175}$$

Donc nous avons dans $\mathbb{D}$ l'égalité

$$P = (X - \alpha)(X - \alpha_1) \dots (X - \alpha_{n-1}). \tag{6.176}$$

□

Lemme 6.120 ([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 6.28.

Le polynôme P est scindé dans $\mathbb{L}$, c'est-à-dire que, en notant n le degré de P,

$$P = \prod_{i=1}^{n} (X - \lambda_i) \tag{6.177}$$

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

$$P = \prod_{k=1}^{n} (X - \mu_k) \tag{6.178}$$

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 (6.177) et (6.178) 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 3.92), 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 6.121 ([84]).
Soient :

- *un isomorphisme de corps $\tau : \mathbb{K} \to \mathbb{K}'$;*
- *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 $\sigma : \mathbb{L} \to \mathbb{L}'$.

Démonstration. Soit m le nombre de racines de P dans $\mathbb{L}\backslash\mathbb{K}$. Nous faisons une récurrence sur m.

Si $m = 0$ alors $\mathbb{K}$ est un corps de rupture de P ; nous avons

$$P = (X - \lambda_1)\dots(X - \lambda_n) \tag{6.179}$$

avec $\lambda_i \in \mathbb{K}$. Dans ce cas nous avons aussi

$$\tau(P) = \big(X - \tau(\lambda_1)\big)\dots\big(X - \tau(\lambda_n)\big) \tag{6.180}$$

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 $\mathbb{L}\backslash\mathbb{K}$. Soit

$$P = P_1 \dots P_r \tag{6.181}$$

sa décomposition en irréductibles dans $\mathbb{K}[X]$ (notons que $r \leqslant n$ 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 6.28 que $\mathbb{K}[X]$ est un anneau factoriel. Le lemme 6.120 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 6.64 :

$$\begin{aligned}\psi\colon \mathbb{K}[X]/(P_1) &\to \mathbb{K}[\alpha]\\ \bar{Q} &\mapsto Q(\alpha).\end{aligned} \tag{6.182}$$

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

$$\tau(P) = \tau(P_1)\dots\tau(P_r), \tag{6.183}$$

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

$$\psi'\colon \mathbb{K}'[X]/\big(\tau(P_1)\big) \to \mathbb{K}'[\beta]. \tag{6.184}$$

De plus, par le lemme 6.39, nous savons que τ passe aux classes :

$$\phi_\tau\colon \mathbb{K}[X]/(P_1) \to \mathbb{K}'[X]/\big(\tau(P_1)\big) \tag{6.185}$$

est un isomorphisme d'anneaux. Et enfin, dernier résultat externe à invoquer, la proposition 6.85 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 corps [32] :

$$\tau_1 = \psi' \circ \phi_\tau \circ \psi^{-1}\colon \mathbb{K}_1 \to \mathbb{K}[X]/(P_1) \to \mathbb{K}'[X]/\big(\tau(P_1)\big) \to \mathbb{K}'_1. \tag{6.186}$$

Cet isomorphisme $\tau_1\colon \mathbb{K}_1 \to \mathbb{K}_2$ 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

$$\begin{array}{ccccc}\mathbb{K} & \xrightarrow{i} & \mathbb{K}_1 & \xrightarrow{i} & \mathbb{L}\\ \downarrow{\scriptstyle\tau} & & \downarrow{\scriptstyle\tau_1} & & \\ \mathbb{K}' & \xrightarrow[i]{} & \mathbb{K}'_1 & \xrightarrow{i} & \mathbb{L}'\end{array} \tag{6.187}$$

Le corps $\mathbb{L}$ est un corps de décomposition de P sur $\mathbb{K}_1$, et le nombre de racines de P dans $\mathbb{L}\backslash\mathbb{K}_1$ est strictement plus petit que m parce qu'il y en a exactement m dans $\mathbb{L}\backslash\mathbb{K}$ 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 :

32. 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.

— $\tau_1 : \mathbb{K}_1 \to \mathbb{K}'_1$ 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 $\mathbb{L}\backslash\mathbb{K}_1$ est strictement inférieur à m.

Donc, par hypothèse de récurrence sur m, il existe un isomorphisme $\sigma : \mathbb{L} \to \mathbb{L}'$ qui prolonge τ_1. Vu que τ_1 prolonge τ, nous avons également σ qui prolonge τ. □

L'énoncé le plus compact pour l'unicité du corps de décomposition (à isomorphisme près) est le suivant :

Proposition 6.122.
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 $f : \mathbb{L} \to \mathbb{F}$ tel que $f|_{\mathbb{K}} = \mathrm{Id}$.

Démonstration. C'est un cas particulier du théorème 6.121, où nous considérons $\mathbb{K} = \mathbb{K}'$ muni de l'isomorphisme identité. □

Cependant le passage par l'énoncé plus compliqué 6.121 est nécessaire pour les besoins de la récurrence.

6.123.
À propos de terminologie. Lorsque nous disons « *un* corps de décomposition » nous référons à la définition 6.118 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 6.119 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.

6.124.
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 6.125
Soit le polynôme $P = X^4 - 5X^2 + 6$. Sa factorisation en irréductibles est :

$$P = (X^2 - 2)(X^2 - 3). \tag{6.188}$$

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 $P = P_1P_2$ avec

$$P_1 = X^2 - 2 \tag{6.189a}$$
$$P_2 = X^2 - 3, \tag{6.189b}$$

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

$$P_1 = (X + \sqrt{2})(X - \sqrt{2}). \tag{6.190}$$

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

$$P_2 = (X - \sqrt{3})(X + \sqrt{3}). \tag{6.191}$$

Nous savons (par le lemme 6.114) que

$$\mathbb{L}_2 = \mathbb{L}_1(\sqrt{3}) = \big(\mathbb{Q}(\sqrt{2})\big)(\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3}). \tag{6.192}$$

Nous pouvons donc écrire en toute confiance, dans $\mathbb{Q}(\sqrt{2},\sqrt{3})$ la factorisation

$$P = (X+\sqrt{2})(X-\sqrt{2})(X+\sqrt{3})(X-\sqrt{3}). \tag{6.193}$$

Et nous notons que si nous avions commencé par P_2 au lieu de P_1, nous aurions eu le même résultat final. △

Corollaire 6.126 ([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 6.119.

Vu que le lemme 6.114 donne

$$\mathbb{K}(\alpha_1,\dots,\alpha_n) = \big(\mathbb{K}(\alpha_1,\dots,\alpha_{n-1})\big)(\alpha_n), \tag{6.194}$$

le corps $\mathbb{D}$ se construit comme une pile d'extensions finies. Les degrés se composant par le lemme 6.57, au final ce corps de décomposition est une extension finie.

Soit maintenant un corps de décomposition quelconque $\mathbb{L}$. La proposition 6.122 donne un isomorphisme de corps[33] $f\colon \mathbb{L} \to \mathbb{D}$ 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 $\mathbb{K}$[34] ? □

6.4.10 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 $P \in \mathrm{Frac}(A)[X]$ 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 6.127
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.

△

33. Un isomorphisme de corps est juste un isomorphisme d'anneaux.
34. Personnellement, je n'ai pas vérifié. Vérifiez vous-même et écrivez-moi pour dire si c'est bon ou non.

6.4.11 Clôture algébrique

Théorème 6.128.
Tout corps $\mathbb{K}$ possède une clôture algébrique[35] *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.*

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 6.129.
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. □

Exemple 6.130
Soit p un nombre premier. Montrons que le polynôme

$$Q(X) = X^p - X + 1 \tag{6.195}$$

est irréductible dans $\mathbb{F}_p$.

Nous supposons qu'il n'est pas irréductible, c'est-à-dire que

$$Q(X) = R(X)S(X) \tag{6.196}$$

avec R et S, des polynômes de degrés $\geqslant 1$ dans $\mathbb{F}_p[X]$

Soit $\bar{\mathbb{F}}_p$ une clôture algébrique[36] 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

$$\begin{aligned} Q(\alpha + a) &= (\alpha + a)^p - (\alpha + a) + 1 && \text{(6.197a)}\\ &= \alpha^p + a^p - \alpha - a + 1 && \text{(6.197b)}\\ &= \alpha^p - \alpha + 1 && \text{(6.197c)}\\ &= Q(\alpha) && \text{(6.197d)}\\ &= 0 && \text{(6.197e)} \end{aligned}$$

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

$$R(X) = \prod_{i=1}^{k} \big(X - (\alpha + a_i)\big) \tag{6.198}$$

où les a_i sont les éléments de $\mathbb{F}_p$. En développant un peu,

$$R(X) = X^k - \sum_{i=1}^{k} (\alpha + a_i^{k-1}) + \text{termes de degré plus bas en } X. \tag{6.199}$$

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 :

$$Q(\alpha) = \alpha^p - \alpha + 1 = 1 \neq 0. \tag{6.200}$$

35. Définition 6.70.
36. Définition 6.70. Pour l'existence c'est le théorème 6.128.

Le polynôme $X^p - X + 1$ est donc irréductible sur $\mathbb{F}_p$. △

6.4.12 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 6.143.

Définition 6.131.
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 6.132.
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 6.122 qui donne l'unicité du corps de décomposition à $\mathbb{K}$-isomorphisme près. Soit donc $\psi\colon \mathbb{L} \to \mathbb{L}'$ 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

$$P = a(X - \alpha_1) \dots (X - \alpha_n) \tag{6.201}$$

avec $a \in \mathbb{K}$ et $\alpha_i \in \mathbb{L}$. Nous avons donc

$$P = \psi(P) = a(X - \psi(\alpha_1)) \dots (X - \psi(\alpha_n)). \tag{6.202}$$

Donc les racines de P dans $\mathbb{L}'$ sont les éléments $\psi(\alpha_i)$ qui sont distincts. □

Exemple 6.133
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

$$P = X^p - T^p \tag{6.203}$$

dans $\mathbb{K}[X]$. Par le morphisme de Frobenius nous avons

$$P = (X - T)^p \tag{6.204}$$

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. △

Exemple 6.134
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 $\mathbb{Q}(i)$). △

Exemple 6.135
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. △

Proposition 6.136 ([94]).
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 $\operatorname{pgcd}(P,P')$ est $\geqslant 1$.

Démonstration. (1)⇒(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 une 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 $\psi\colon \mathbb{E}' \to \mathbb{E}$. 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

$$P\big(\psi(a)\big) = \psi\big(P(a)\big). \tag{6.205}$$

(2)⇒(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 $P = (X-a)^2Q$ avec $Q \in \mathbb{L}[X]$. En dérivant,

$$P' = 2(X-a)Q + (X-a)^2Q', \tag{6.206}$$

et donc a est également une racine de P'.

(3)⇒(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

$$AP + BP' = D. \tag{6.207}$$

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 $\deg(D) \geqslant 1$.

(4)⇒(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

$$P = (X-a)Q, \tag{6.208}$$

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 6.137.
Soit $P \in \mathbb{K}[X]$ irréductible. Le polynôme P est séparable si et seulement si $P' \neq 0$.

Démonstration. Soit $D = \operatorname{pgcd}(P,P')$ et nous voudrions prouver que $\deg(D) \geqslant 1$ si et seulement si $P' = 0$. Si $P' = 0$, alors $\operatorname{pgcd}(P,P') = P$ est donc $\deg(D) \geqslant 1$.

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 $\deg(P) \geqslant 1$. Dans les deux cas, P' est nécessairement non-nul. □

Corollaire 6.138.
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 6.136. □

Définition 6.139.
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 6.131).*

*(2) L'extension $\mathbb{L}$ est **séparable** si tous ses éléments sont séparables.*

Proposition 6.140.
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 corollaire 6.126. 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

$$P = \prod_{i=1}^{n}(X - a_i), \tag{6.209}$$

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 $k_a, k_n \in \mathbb{K}$ 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_n sont unitaires, $\mu_a = \mu_b$.

Nous avons :

$$P = k\mu = \prod_{i=1}^{n}(X - a_i). \tag{6.210}$$

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 corollaire 6.138. □

Corollaire 6.141.
Toute les extensions algébriques de $\mathbb{Q}$ sont séparables.

Démonstration. Le corps $\mathbb{Q}$ est de caractéristique nulle (définition 3.53). Le corollaire 6.138 dit alors que tout polynôme sur $\mathbb{Q}$ est séparable. La proposition 6.140 conclut en disant que toutes les extensions algébriques de $\mathbb{Q}$ sont séparables. □

Théorème 6.142 ([40]).
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

$$x^\omega = 1 \tag{6.211}$$

pour tout $x \in G$. Mais ce polynôme possède au plus ω racines dans $\mathbb{K}$. Du coup $|G| \leqslant \omega$. 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 3.33. □

Théorème 6.143 (Théorème de l'élément primitif[40]).
Toute extension de corps séparable finie admet un élément primitif[37].

Autrement dit, soient des éléments algébriques $\alpha_1, \dots, \alpha_n$ séparables[38] *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 6.142. 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

$$\mathbb{K}(\alpha_1, \dots, \alpha_n) = \mathbb{K}(\alpha_1, \dots, \alpha_{n-1})(\alpha_n), \tag{6.212}$$

et donc si $\mathbb{K}(\alpha_1, \dots, \alpha_{n-1}) = \mathbb{K}(\theta)$, nous avons

$$\mathbb{K}(\alpha_1, \dots, \alpha_n) = \mathbb{K}(\theta, \alpha_n) \tag{6.213}$$

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

$$\alpha_1 = \alpha, \alpha_2, \dots, \alpha_r \tag{6.214}$$

de P dans $\mathbb{E}$ et les racines

$$\beta_1 = \beta, \beta_2, \dots, \beta_s \tag{6.215}$$

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 $s \geqslant 2$.

Pour chaque $(i, j) \in [\![1, r]\!] \times [\![2, s]\!]$, l'équation $\alpha_i + x\beta_k = \alpha_1 + x\beta_1$ pour $x \in \mathbb{K}$ a au plus[39] une solution donnée le cas échéant par

$$x = (\alpha_i - \alpha_1)(\beta_1 - \beta_k)^{-1} \tag{6.216}$$

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 (6.216) :

$$\alpha_i + c\beta_k \neq \alpha_1 + c\beta_1. \tag{6.217}$$

Nous posons $\theta = \alpha_1 + c\beta_1$ et nous prétendons que $\mathbb{L} = \mathbb{K}(\theta)$.

37. Définition 6.90.
38. Définition 6.139(1).
39. La solution (6.216) peut être dans $\mathbb{L}$ et non dans $\mathbb{K}$. L'équation peut donc très bien ne pas avoir de solutions $x \in \mathbb{K}$.

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 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

$$S(\beta_1) = P(\theta - c\beta_1) = P(\alpha_1 + c\beta_1 - c\beta_1) = P(\alpha_1) = 0. \tag{6.218}$$

D'autre part, si $k \geqslant 2$, alors

$$S(\beta_k) = P(\alpha_1 + c\beta_1 - c\beta_k) = P\big(\alpha_1 + c(\beta_1 - \beta_k)\big) \neq 0 \tag{6.219}$$

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 (6.217)).

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,

$$R = X - \beta \in \mathbb{K}(\theta)[T], \tag{6.220}$$

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 6.144
Le théorème de l'élément primitif 6.143 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 6.145
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 6.146.
*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 6.147 ([95])**.**
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 6.148 ([95])**.**
Si $\mathbb{K}$ est un corps algébriquement clos, les idéaux maximaux de $\mathbb{K}[X_1, \dots, X_n]$ sont de la forme

$$(X_1 - a_1, \dots, X_n - a_n) \tag{6.221}$$

où les a_i sont des éléments de $\mathbb{K}$.

Démonstration. Nous commençons par montrer que

$$J = (X_1 - a_1, \dots, X_n - a_n) \tag{6.222}$$

est un idéal maximum. Pour cela nous considérons le morphisme surjectif d'anneaux

$$\begin{aligned}\phi\colon \mathbb{K}[X_1,\ldots,X_n] &\to \mathbb{K}\\ P &\mapsto P(a_1,\ldots,a_n).\end{aligned} \tag{6.223}$$

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 :

$$P=(X-a_1)Q_1+\cdots+(X_n-a_n)Q_n+R \tag{6.224}$$

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 (6.224) à $(a_1,\ldots,a_n)$ et en nous rappelant que $P\in\ker(\phi)$ nous obtenons

$$0=P(a_1,\ldots,a_n)=R, \tag{6.225}$$

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 $\mathbb{K}[X_1,\ldots,X_n]\to\mathbb{K}$, nous avons

$$\frac{\mathbb{K}[X_1,\ldots,X_n]}{J}=\mathbb{K}. \tag{6.226}$$

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 $\mathbb{K}[X_1,\ldots,X_n]/J$.

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 $a_1,\ldots,a_n$).

Le quotient

$$\frac{\mathbb{K}[X_1,\ldots,X_n]}{I} \tag{6.227}$$

est une $\mathbb{K}$-algèbre de type fini (définition 6.146). De plus c'est un corps par la proposition 3.50. C'est donc une extension algébrique finie de $\mathbb{K}$ par le théorème 6.147. Mais $\mathbb{K}$ étant algébriquement clos, il est sa propre et unique extension algébrique ; nous en déduisons que

$$\frac{\mathbb{K}[X_1,\ldots,X_n]}{I}=\mathbb{K}. \tag{6.228}$$

Donc pour tout $1\leqslant i\leqslant n$, 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 $I=J$. □

Corollaire 6.149.
Soit $\mathbb{K}$ un corps algébriquement clos et I, un idéal de $\mathbb{K}[X_1,\ldots,X_n]$. Si nous notons

$$V(I)=\{x\in\mathbb{K}^n \text{ tel que } P(x_1,\ldots,x_n)=0\} \tag{6.229}$$

l'ensemble des racines communes à tous les éléments de I, on a $V(I)=\varnothing$ si et seulement si $I=\mathbb{K}[X_1,\ldots,X_n]$.

Démonstration. Si $I=\mathbb{K}[X_1,\ldots,X_n]$ en particulier $1\in I$ et nous avons évidemment $V(I)=\varnothing$. Le sens difficile est l'autre sens.

Supposons que $I\neq\mathbb{K}[X_1,\ldots,X_n]$ et que K est un idéal maximum contenu dans I. Nous savons déjà par le théorème 6.148 que K est de la forme $K=(X_1-a_1,\ldots,X_n-a_n)$. Un élément de I est dans K, donc si $P\in I$ nous avons

$$P(a_1,\ldots,a_n)=0, \tag{6.230}$$

c'est-à-dire que $(a_1,\ldots,a_n)\in V(I)$ et donc que $V(I)\neq\varnothing$. □

6.6 Polynômes symétriques et alternés

6.6.1 Polynômes symétriques, alternés ou semi-symétriques

Lemme 6.150 ([57]).
Soit $\mathbb{K}$ un corps de caractéristique différente[40] *de 2. L'opération*

$$\begin{aligned} \cdot : S_n \times \mathbb{K}[T_1,\dots,T_n] &\to \mathbb{K}[T_1,\dots,T_n] \\ (\sigma \cdot f)(T_1,\dots,T_n) &= f\big(T_{\sigma(1)},\dots,T_{\sigma(n)}\big) \end{aligned} \tag{6.231}$$

est une action[41] *de S_n sur l'anneau $\mathbb{K}[T_1,\dots,T_n]$.*

Définition 6.151.
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 6.152.
Le k-ième ***polynôme symétrique élémentaire*** *à n inconnues est le polynôme*

$$\sigma_k(T_1,\dots,T_n) = \sum_{s\in F_k}\prod_{i=1}^{k} T_{s(i)} \tag{6.232}$$

où F_k est l'ensemble des fonctions strictement croissantes $\{1,2,\dots,k\} \to \{1,2,\dots,n\}$.

Une autre façon de décrire ces polynômes élémentaires est

$$\sigma_k = \sum_{1\leqslant i_1<\dots<i_k\leqslant n} X_{i_1}\dots X_{i_k}. \tag{6.233}$$

Par exemple

$$\sigma_1(T_1,\dots,T_n) = T_1 + T_2 + \dots + T_n \tag{6.234a}$$
$$\sigma_2(T_1,\dots,T_n) = T_1T_2 + \dots + T_1T_n + T_2T_3 + \dots + T_2T_n + \dots + T_{n-1}T_n \tag{6.234b}$$
$$\sigma_n(T_1,\dots,T_n) = T_1\dots T_n. \tag{6.234c}$$

En particulier, $\sigma_2(x,y,z) = xy + yz + xz$.

Théorème 6.153 ([96]).
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

$$Q(T_1,\dots,T_n) = P\big(\sigma_1(T_1,\dots,T_n),\dots,\sigma_n(T_1,\dots,T_n)\big). \tag{6.235}$$

Exemple 6.154
Nous voulons décomposer $P(x,y,z) = x^3 + y^3 + z^3$ en polynômes symétriques élémentaires, c'est-à-dire en

$$\begin{cases} \sigma_1 = x + y + z & \text{(6.236a)} \\ \sigma_2 = xy + xz + yz & \text{(6.236b)} \\ \sigma_3 = xyz. & \text{(6.236c)} \end{cases}$$

40. Le truc de la caractéristique deux est que $a = -a$ n'implique pas $a = 0$.
41. Définition 2.43.

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

$$P = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3. \tag{6.237}$$

△

Lemme 6.155 ([57]).
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 6.140 et du corollaire 6.141, $\mathbb{K}$ est une extension séparable de $\mathbb{Q}$, et donc vérifie le théorème de l'élément primitif (6.143). 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

$$\{1, \theta, \dots, \theta^{\delta-1}\}. \tag{6.238}$$

Mais par ailleurs la proposition 6.85(2) nous indique qu'une base de $\mathbb{Q}(\theta)$ sur $\mathbb{Q}$ est donnée par

$$\{1, \theta, \dots, \theta^{n-1}\} \tag{6.239}$$

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

$$\begin{aligned}\sigma_k\colon \mathbb{Q}(\theta) &\to \mathbb{Q}(\theta_k)\\ \sum_i q_i\theta^i &\mapsto \sum_i q_i\theta_k^i\end{aligned} \tag{6.240}$$

Nous avons $\sigma_1\colon \mathbb{K}\to\mathbb{K}$ 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

$$P=\sum_{l=0}^{N}\sum_{i=1}^{m}c_{il}T_i^l \tag{6.241}$$

avec $c_{il}\in\mathbb{K}$. Nous voyons $c_{i,.}$ comme un élément de $\mathbb{K}^m$ et donc nous écrivons [42]

$$P=\sum_{l=0}^{N}\sum_{i=1}^{m}c_l(\theta)_iT_i^l \tag{6.242}$$

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

$$P^{\sigma_k}=\sum_{l,i}c_l(\theta_k)_iT_i^l\in\mathbb{Q}(\theta_k)[T_1,\dots,T_m], \tag{6.243}$$

et $\bar{P}=PP^{\sigma_2}\dots P^{\sigma_k}$. Le coefficient de T_i^l dans $\bar{P}$ est

$$\bar{c}_l(\theta_1,\dots,\theta_\delta)_i=\sum_{l_1+\dots+l_\delta=l}c_{l_1}(\theta_1)_i\dots c_{l_\delta}(\theta_\delta)_i. \tag{6.244}$$

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 6.153 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

$$\deg(\bar{P})=\delta\deg(P) \tag{6.245}$$

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. □

6.6.3 Relations coefficients racines

Théorème 6.156 (Relations coeffitients-racines)**.**
Soit le polynôme $P=a_nX^n+\dots+a_1X+a_0$ et r_i ses n racines. Alors nous avons pour chaque $1\leqslant k\leqslant n$ la relation

$$\sigma_k(r_1,\dots,r_n)=(-1)^k\frac{a_{n-k}}{a_n} \tag{6.246}$$

où σ_k est le k^epolynôme symétrique défini en 6.152.

Exemple 6.157
Soit le polynôme

$$P(x)=x^3+2x^2+3x+4 \tag{6.247}$$

42. Il me semble qu'il manque la somme sur i dans [57].

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-racines [43] nous donnent $\sigma_1(a, b, c) = -2$ et $\sigma_2(a, b, c) = 3$, donc

$$a^2 + b^2 + c^2 = (-2)^2 - 2 \cdot 3 = -2. \tag{6.248}$$

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) :

```
sage: P(x)=x**3+2*x**2+3*x+4
sage: S=solve(  P(x)==0,x  )
sage: sols=[ s.rhs() for s in S  ]
sage: Q=[  s**2 for s in sols ]
sage: s=sum(Q)
sage: s.simplify_full()
-2
```

tex/frido/VAYVmNRpolynomeSym.py

Notez qu'il faut un peu chipoter pour isoler les solutions depuis la réponse de la fonction `solve`. △

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 6.158 (Annulation de fonctions polynomiales[97])**.**
Soit $\mathbb{K}$ un corps et P un polynôme à n indéterminées. Nous supposons que P s'annule sur un ensemble de la forme $A_1 \times \cdots \times A_n$ 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 nuls [44].

Démonstration. Nous prouvons le résultat par récurrence sur le nombre n d'indéterminées. Si $n = 1$, cela est le théorème 6.99. Nous classons les monômes du polynôme P par ordre de puissance de X_n et nous le factorisons :

$$P = \sum_{i=1}^{m} P_i X_n^i \tag{6.249}$$

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

$$Q(T) = P(a_1, \dots, a_{n-1}, T) = \sum_{i=1}^{m} P_i(a_1, \dots, a_{n-1}) T^i. \tag{6.250}$$

Le polynôme Q s'annule sur A_n avec $\deg(Q) = \deg_{X_n}(P) < \text{Card}(A_n)$ et le théorème 6.99 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

$$\deg_{X_j}(P_i) \leqslant \deg_{X_j} P < \text{Card}(A_j), \tag{6.251}$$

donc l'hypothèse de récurrence donne $P_i = 0$. Par suite, $P = 0$ également. □

43. Théorème 6.156

44. 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.

6.7 Minuscule morceau sur la théorie de Galois

Vous trouverez des détails et des preuves à propos de la théorie de Galois dans [98, 40].

Définition 6.159.
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 $\mathbb{K}$.

Définition 6.160.
*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*

$$\sum \alpha_{i_1 \dots i_n} b_1^{i_1} \dots b_n^{i_n} = 0 \tag{6.252}$$

avec $\alpha_{i_1 \dots i_n} \in \mathbb{K}$.

Nous disons que l'équation

$$x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 = 0 \tag{6.253}$$

est l'**équation générale** de degré n si les coefficients a_i sont algébriquement indépendants sur $\mathbb{K}$.

Théorème 6.161.
Le groupe de Galois d'un polynôme de degré n est isomorphe au groupe symétrique S_n.

Corollaire 6.162 ([99])**.**
L'équation générale de degré n est résoluble par radicaux si et seulement si $n \leqslant 5$.

Chapitre 7

Topologie générale

7.1 Éléments généraux de topologie

7.1.1 Définitions et propriétés de base

Définition 7.1.
Soit X, un ensemble et $\mathcal{T}$, une partie de l'ensemble de ses parties qui vérifie les propriétés suivantes.

(1) Les ensembles $\varnothing$ et X sont dans $\mathcal{T}$,

(2) Une union quelconque[1] *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****.*

Définition 7.2.
Si X est un espace topologique, un sous-ensemble F de X est dit ***fermé*** *si son complémentaire, F^c, est ouvert.*

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 $\mathcal{O} \subset V$.*

Lemme 7.3.
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

$$\left(\bigcap_{i\in I} F_i\right)^c = \bigcup_{i\in I} F_i^c. \tag{7.1}$$

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 ouvert[2]. □

Dans un espace topologique, nous avons une caractérisation très importante des ouverts.

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.
2. Un bon exercice est d'écrire ces unions et intersections, pour se convaincre que ça fonctionne.

Théorème 7.4.
Une partie d'un espace topologique est ouverte si et seulement si elle contient un voisinage[3] *ouvert 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,

$$A = \bigcup_{x \in A} \mathcal{O}_x \tag{7.2}$$

en effet, d'une part, $A \subset \bigcup_{x\in A} \mathcal{O}_x$ parce que chaque élément x de A est dans le $\mathcal{O}_x$ corrrespondant, 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. □

Le lemme 8.48 est une version particulière de celui-ci, pour l'espace topologique $\mathbb{R}$. Une autre application typique est la proposition 7.55 et le théorème 7.69.

7.1.2 Quelques exemples

7.1.2.1 Une première vague

Exemple 7.5
Pour un ensemble X quelconque, on considère l'ensemble $\mathcal{T} = \{\varnothing; X\}$. 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**. △

Exemple 7.6
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**. △

Exemple 7.7(Toutes les topologies d'un ensemble à 3 éléments)
On pose $X = \{1, 2, 3\}$. Alors on peut munir X de 29 topologies différentes[4] ; saurez-vous les retrouver toutes ? △

7.1.2.2 Topologie engendrée, topologie produit

Exemple 7.8
Soit X un ensemble, et $\mathcal{T}_0$ un sous-ensemble de parties de X. On construit alors l'ensemble $\mathcal{T}$ par

$$\mathcal{T} = \Big\{ \bigcup_{\alpha\in A} \bigcap_{i=1}^{n_a} \mathcal{O}_{\alpha,i} \text{ tel que } \mathcal{O}_{\alpha,i} \in \mathcal{T}_0 \forall \alpha, \forall i \Big\}. \tag{7.3}$$

Alors $\mathcal{T}$ est une topologie[5] sur X, qu'on appelle **topologie engendrée** par $\mathcal{T}_0$. △

3. Définition 7.2.
4. Remercions Erwann Aubry d'en avoir fourni la liste exhaustive ! https://math.unice.fr/~eaubry/Enseignement/L3/rappelstopo.pdf
5. Ce n'est pas un résultat évident : l'annoncer à un jury nécessite d'en avoir écrit la preuve.

Définition 7.9 (Produit d'espaces topologiques, thème 8)**.**
*Soient $X_1,\dots, X_n$ des espaces topologiques. Leur **produit** est l'ensemble*

$$X = \prod_{i=1}^{n} X_i \tag{7.4}$$

muni de la topologie engendrée par les produits $A_1 \times \cdots \times A_n$, avec $A_i \in X_i$ ouverts de chacun des ensembles.

7.1.2.3 Topologie induite

Définition 7.10 (Topologie induite)**.**
*Soit un espace topologique $(X, \mathcal{T})$, et soit $Y \subset X$. Alors on peut munir Y de la topologie constituée des $Y \cap \mathcal{O}$, pour $\mathcal{O} \in \mathcal{T}$: c'est ce qu'on appelle la **topologie induite**.*

Lemme 7.11 ([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 $S\backslash F = S \cap \Omega$. Si maintenant nous considérons le complémentaire de S dans X nous avons

$$F^c = (S\backslash F) \cup (X\backslash S) = (S \cap \Omega) \cup S^c = (S \cap \Omega) \cup (S^c \cap \Omega) \cup S^c = \Omega \cup S^c. \tag{7.5}$$

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. □

Lemme 7.12.
Si $B \subset A$ alors la fermeture de B pour la topologie de A (induite de X) que nous noterons $\tilde{B}$ est

$$\tilde{B} = \bar{B} \cap A \tag{7.6}$$

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 $(\mathcal{O} \cap A) \cap B \neq \varnothing$. 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 $a \in \bar{B}$. □

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 7.13
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 $\mathbb{R}$. △

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 7.14
Quid de la boule ouverte $B(1, \epsilon)$ dans le compact $[0, 1]$? Par définition c'est

$$B(1, \epsilon) = \{x \in [0, 1] \text{ tel que } |x - 1| < \epsilon\} =]1 - \epsilon, 1]. \tag{7.7}$$

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 $[0,1]$. △

7.1.3 Adhérence, fermeture, intérieur, point d'accumulation et isolé

7.1.3.1 Intérieur

Définition 7.15.
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. L'ensemble des points intérieurs de A est noté* $\mathrm{Int}(A)$.

*(2) L'**intérieur** de A, notée $\mathring{A}$, est l'union de tous les ouverts de X contenus dans A.*

Remarque 7.16.
Quelques remarques en vrac.

(1) Pour tout $A \subset X$, l'ensemble $\mathring{A}$ est un ouvert, comme union quelconque d'ouverts.

(2) Par ailleurs, on a $\mathring{A} = \mathrm{Int}\, A$: en effet, $x \in \mathrm{Int}\, A$ si et seulement s'il existe un ouvert contenant x et inclus dans A, si et seulement si x est dans l'union de tous les ouverts contenus dans A, si et seulement si $x \in \mathring{A}$.

(3) On a $\mathring{A} \subset A$, et $\mathring{A} = A$ si et seulement si A est un ouvert : en sens direct, c'est clair par égalité d'ensembles ; en sens inverse, c'est aussi clair puisque A est alors un ouvert contenu à A, donc $A \subset \mathring{A}$.

7.1.3.2 Adhérence et fermeture

Disons-le tout de suite : « adhérence » et « fermeture » sont synonymes. Dans le Frido, nous allons nous évertuer à utiliser le mot « adhérance » et la notation $\mathrm{Adh}(A)$ 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 7.17.
*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* $\mathrm{Adh}(A)$.

Lemme 7.18.
L'adhérence de A est l'intersection de tous les fermés de X contenant A.

Par ailleurs, nous avons le lien

$$(\mathrm{Int}(A))^c = \mathrm{Adh}(A^c). \tag{7.8}$$

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 $\mathring{A}$;

— 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 $\mathrm{Adh}(A) = \bar{A}$ en prouvant la double inclusion par contraposée.

Si $x \in \bar{A}$ alors $x \in \mathrm{Adh}(A)$ 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 $\mathrm{Adh}(A)$.

Si $x \in \bar{A}$ alors $x \in \mathrm{Adh}(A)$ Si x n'est pas dans $\mathrm{Adh}(A)$ 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 7.19.
Comme corollaire 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 7.18, si bien que A est fermé si et seulement si $(\bar{A})^c = A^c$, ou encore... ce qu'on affirmait au début.

Définition 7.20.
*Soit X un espace topologique. Un sous-ensemble A de X est **dense** dans X si $\bar{A} = X$.*

7.1.3.3 Frontière

Définition 7.21.
*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,*

$$\partial A = \bar{A} \backslash \mathring{A}. \tag{7.9}$$

7.1.3.4 Points d'accumulation et isolés

Définition 7.22.
*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 $A \backslash \{s\}$.*

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 8.64.

Notons qu'un point d'accumulation de A dans X n'est pas spécialement dans A.

Définition 7.23.
*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

7.24.
À propos de notations. La pire notation possible pour une suite est $(a_n)_n$. What on the f*** 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 $\lim_{n\to\infty} a_n$.

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.

Dès que nous avons une topologie nous avons une notion de convergence.

Définition 7.25 (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 $x_k \in \mathcal{O}$.*

7.2.1 Convergence dans un fermé

Proposition 7.26 ([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 7.4, 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. □

Corollaire 7.27.
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 7.26. □

Lemme 7.28.
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 $n \geqslant N$, alors $x_n \in A \cap \mathcal{O} \subset \mathcal{O}$. □

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 7.25 dit que toute suite convergeant vers y converge aussi vers x...

Exemple 7.29
Oui, il y a moyen de converger vers plusieurs points distincts si l'espace n'est pas super cool. Nous pouvons par exemple [100] 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 $0'$. △

Nous posons la définition suivante, qui nous permettra de donner une assez grande classe d'espaces topologiques dans lesquels nous avons unicité de la limite[6].

6. Voir la proposition 7.65.

Définition 7.30 (Espace topologique séparé)**.**
Si deux points distincts admettent toujours deux voisinages disjoints[7]*, nous disons que l'espace est* ***séparé*** *ou* ***Hausdorff****.*

Attention, cette notion est à ne pas confondre avec :

Définition 7.31 (Espace topologique séparable)**.**
Un espace topologique est ***séparable*** *s'il possède une partie dénombrable*[8] *dense*[9]*.*

Proposition 7.32.
Dans un espace séparé, si une suite converge, alors sa limite est unique.

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 $k \geqslant \max\{k_x, k_y\}$, 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. □

7.33.
Donc, on pourra parler, avec des espaces séparés, de « la limite d'une suite ». On notera $x_n \to a$, ou $\lim_{n\to\infty} x_n = a$, pour signifier que la suite (x_n) converge vers a.

Proposition 7.34 ([1])**.**
La convergence d'une suite pour la topologie de l'espace produit implique la convergence des suites « composante par composante ».

Démonstration. 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. □

Lemme 7.35 ([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 $x_n \to x$.

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 $n \geqslant N$ 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. □

7.2.3 Fonctions équivalentes

Proposition-définition 7.36 ([101])**.**
Soit un espace topologique X et $D \subset X$. Soient encore des fonctions $f, g\colon D \to \mathbb{C}$ et un point $a \in \mathrm{Adh}(D)$[10]*.*

Nous définissons sur $\mathrm{Fun}(D, \mathbb{C})$ *la relation $f \sim_a g$ lorsque qu'il existe un voisinage V de a dans X et une fonction $\alpha\colon V \to \mathbb{R}$ telles que*

(1) $\lim_{x\to a} \alpha(x) = 0$,

(2) pour tout $x \in (V \cap D)\backslash\{a\}$,

$$f(x) = \big(1 + \alpha(x)\big)g(x). \tag{7.10}$$

7. Définition 1.2.
8. Définition 1.28.
9. Définition 7.20.
10. Adhérence ou fermeture, c'est la même chose. Voir la définition 7.17 et le lemme 7.18.

Cette relation est une relation d'équivalence.

*Lorsque $f \sim_a g$, nous disons que f et g sont **équivalentes** en a.*

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 7.37.
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

$$\frac{f(x)}{g(x)} \in B(1, \epsilon) \tag{7.11}$$

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 (7.10) par $g(x)$ nous trouvons

$$\frac{f(x)}{g(x)} = 1 + \alpha(x). \tag{7.12}$$

Donc

$$|\frac{f(x)}{g(x)} - 1| = |\alpha(x)| \leqslant \epsilon, \tag{7.13}$$

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 7.38.
*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*

$$A = (A \cap O_1) \cup (A \cap O_2), \tag{7.14}$$

*et tels que $A \cap O_1 \neq \varnothing$, et $A \cap O_2 \neq \varnothing$. Si un sous-ensemble n'est pas non-connexe, alors on dit qu'il est **connexe**.*

Une autre façon d'exprimer la condition (7.14) 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 7.39.
Soit X un espace topologique. Les conditions suivantes sont équivalentes.

(1) L'espace X est connexe.

(2) Si $X = A \sqcup B$ avec A et B fermés disjoints dans X, alors $A = \varnothing$ ou $B = \varnothing$.

(3) Si $A \subset X$ avec A ouvert et fermé en même temps, alors $A = \varnothing$ ou $A = X$.

Nous verrons plus tard (proposition 7.83) une autre caractérisation de la connexité.

Proposition 7.40.
Si $A \subset X$ est connexe et si $A \subset B \subset \bar{A}$, alors B est connexe.

Proposition 7.41.
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 $A_i \cap A_{i+1} \neq \varnothing$, 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) $C_j \cap A \neq \varnothing$ parce que p est dans l'intersection,

(1c) $C_j \cap B \neq \varnothing$ 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 proche[11]. 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 11.

7.4.1 Définition et notions connexes

Soit E, un sous-ensemble de $\mathbb{R}$. Nous pouvons considérer les ouverts suivants :

$$\mathcal{O}_x = B(x, 1) \tag{7.15}$$

pour chaque $x \in E$. Évidemment,

$$E \subseteq \bigcup_{x\in E} \mathcal{O}_x. \tag{7.16}$$

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 7.42.
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 7.43.
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 7.44.
Certaines sources (dont wikipédia) disent que pour être compact il faut aussi être séparé[12]. Pour ces sources, un espace qui ne vérifie que la propriété de Borel-Lebesgue est alors dit **quasi-compact**.

11. Parce qu'on a la flemme de faire une preuve par récurrence !
12. Définition 7.30.

7.45.
La définition 7.43 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 7.46.
Si K est une partie compacte de l'espace topologie X, alors K est un espace topologique compact pour la topologie induite[13] *de X.*

Démonstration. Nous notons τ la topologie de X et τ_K la topologie induite de X vers K, c'est-à-dire

$$\tau_K = \{\mathcal{O} \cap K \text{ tel que } \mathcal{O} \in \tau\}. \tag{7.17}$$

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

$$K = \bigcup_{i\in I}(K \cap \mathcal{O}_i) \subset \bigcup_{i\in I} \mathcal{O}_i. \tag{7.18}$$

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

$$K \subset \bigcup_{j\in J} \mathcal{O}_i. \tag{7.19}$$

Nous avons donc aussi

$$K \subset \bigcup_{j\in J} K \cap \mathcal{O}_i = \bigcup_{j\in J} A_j. \tag{7.20}$$

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. □

Définition 7.47.
Une partie d'un espace topologique est ***relativement compact*** *si son adhérence est compacte.*

Définition 7.48.
Un espace topologique est ***localement compact*** *si tout élément possède un voisinage compact.*

Définition 7.49 (Séquentiellement compact)**.**
Nous disons qu'un espace topologique est ***séquentiellement compact*** *si toute suite admet une sous-suite convergente.*

Définition 7.50.
Un espace topologique est ***dénombrable à l'infini*** *s'il est réunion dénombrable de compacts.*

Définition 7.51.
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 7.52.
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 $\bigcap_{i\in I} F_i \cap K = \varnothing$, alors il existe une partie finie non vide A de I tel que $\bigcap_{i\in A} F_i \cap K = \varnothing$.

13. Définition 7.10.

(3) *Si $\{F_i\}_{i\in I}$ est une famille de fermés telle que pour tout choix de A fini dans I, $\bigcap_{i\in A} F_i \bigcap K \neq \varnothing$, alors l'intersection complète est non vide : $\bigcap_{i\in I} F_i \bigcap K \neq \varnothing$.*

(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 simple[14] reformulation en français de la propriété (3).

Prouvons (1) ⇒ (2). Soit $\{F_i\}_{i\in I}$ une famille de fermés tels que $K\bigcap_{i\in I} F_i = \varnothing$. Les complémentaires $\mathcal{O}_i$ de F_i dans X recouvrent K et donc on peut en extraire un sous-recouvrement fini :

$$K \subset \bigcup_{i\in A} \mathcal{O}_i \tag{7.21}$$

pour un certain sous-ensemble fini A de I. Pour ce même choix A, nous avons alors aussi

$$\bigcap_{i\in A} F_i \cap K = \varnothing. \tag{7.22}$$

L'implication (2) ⇒ (1) est la même histoire de passage aux complémentaires. □

Le théorème 9.51 est en général celui qu'on nomme « théorème des fermés emboîtés », mais le corollaire suivant en mériterait également le nom.

Corollaire 7.53 ([1]).
Soient un espace topologique compact X et une suite $(F_i)_{i\in\mathbb{N}}$ de fermés emboîtés[15] *dans X telle que*

$$\bigcap_{i\in\mathbb{N}} F_i = \varnothing. \tag{7.23}$$

Alors il existe $j_0 \in \mathbb{N}$ tel que $F_i = 0$ pour tout $i \geqslant j_0$.

Démonstration. La proposition 7.52 nous dit qu'il existe une partie finie non vide J de $\mathbb{N}$ telle que $\bigcup_{j\in J} F_j = \varnothing$. Si $j_0 = \min(J)$, alors $F_j \subset F_{j_0}$ pour tout $j \in J$ et nous avons

$$\varnothing = \bigcap_{j\in J} F_j = F_{j_0}. \tag{7.24}$$

Dès que $F_{j_0} = \varnothing$, tous les suivants sont également vides. □

7.4.2 Base de topologie

Définition 7.54 (Base de topologie[102]).
*Une famille $\mathcal{B}$ d'ouverts de X est une **base de la topologie** de X si pour tout $x \in X$ et pour tout voisinage V de x, il existe $A \in \mathcal{B}$ tel que $x \in A \subset V$.*

Proposition 7.55.
Si $\mathcal{B}$ est une base de la topologie de X alors tout ouvert de X est une union d'éléments de $\mathcal{B}$.

Démonstration. Soit $\mathcal{O}$ un ouvert de X ; pour chaque $x \in \mathcal{O}$ nous considérons un ouvert $U(x)$ tel que $x \in U(x) \subset \mathcal{O}$ (possible par le théorème 7.4). Nous prenons alors $B(x) \in \mathcal{B}$ tel que

$$x \in B(x) \subset U(x) \subset \mathcal{O}. \tag{7.25}$$

Alors nous avons $\mathcal{O} = \bigcup_{x\in\mathcal{O}} B(x)$. □

Notons toutefois que nous sommes loin d'avoir une union dénombrable en général.

14. 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.

15. C'est-à-dire que $F_{i+1} \subset F_i$.

7.4.3 Quelques propriétés

Lemme 7.56.
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 7.55 : disons $\mathcal{O}_i = \bigcup_{j\in J_i} A_{(i,j)}$. Soit $J = \{j = (i, j_i) | i \in I, j_i \in J_i\}$; 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 $K \subset \bigcup_{j\in J_0} A_j \subset \bigcup_{i\in I_0} \mathcal{O}_i$. □

Exemple 7.57(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 $\{\varnothing, X\}$. Toutes les parties de cet espace sont compactes, mais les seuls fermés sont $\{\varnothing, X\}$. Toutes les autres parties sont alors compactes et non fermées. △

Proposition 7.58 ([103]).
Tout compact d'un espace topologique séparé est fermé.

Démonstration. Soient X un espace séparé et K compact dans X. Nous considérons $y \in \complement K$ et, par hypothèse de séparation, pour chaque $x \in K$ nous considérons un voisinage ouvert V_x de x et un voisinage ouvert [16] W_x de y tels que $V_x \cap W_x = \varnothing$. Bien entendu les V_x forment un recouvrement ouvert de K dont nous pouvons extraire un sous-recouvrement fini : soit S fini dans K tel que

$$K \subset \bigcup_{x\in S} V_x. \tag{7.26}$$

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 $W \cap K = \varnothing$. 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 7.4), en d'autres termes, que K est fermé. □

Lemme 7.59 ([104]).
Une partie fermée d'une compact est elle-même compacte.

Démonstration. 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 $\{\mathcal{O}_i\}_{i\in I} \cup \{K\backslash F\}$ 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 $K\backslash F$, ça reste un sous-recouvrement fini de F tout en étant extrait de $\{\mathcal{O}_i\}_{i\in I}$. □

Proposition 7.60.
Si V est une partie de l'espace topologique X muni de la topologie induite [17] 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).

16. Oui, la notation du voisinage peut surprendre, mais elle est quand même pratique pour ce qu'on veut en faire.
17. Définition 7.10.

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. □

7.4.4 Compactifié d'Alexandrov

Proposition-définition 7.61 ([105])**.**
Soit un espace topologique localement compact[18] *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 $K^c\cup\{\omega\}$ où K est compact de X. Ici, le complémentaire de K est pris dans X, pas dans $\hat{X}$.*

Alors $\hat{X}$ est un espace topologique compact (cela justifie le nom « ouvert » donné aux parties susdéfinies).

Oh bien entendu les plus férus 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 ? Je vous laisse dormir sur ces questions ; sachez que X lui-même n'est certainement pas un élément de X.

En ce qui concerne $\mathbb{R}$ auquel nous pouvons attacher deux infinis ($+\infty$ et $-\infty$), ce sera la définition 13.24.

Pour $\mathbb{C}$, nous donnerons une caractérisation de la limite en ∞ dans le lemme 13.92.

7.5 Limites et continuité de fonctions

7.5.1 Limites

Définition 7.62 (Limite d'une fonction, thème 16)**.**
Soient X et Y des espaces topologiques, et un point d'accumulation a de X. Soit encore une fonction $f\colon X\to Y$. L'élément $y\in Y$ est une ***limite*** *de f en a si pour tout voisinage W de y (pour la topologie de Y), il existe un voisinage V de a dans X tel que*

$$f\big(V\backslash\{a\}\big)\subset W. \tag{7.27}$$

Si un tel élément est unique[19]*, alors nous disons que cet élément est la* ***limite*** *de f et nous notons*

$$\lim_{x\to a} f(x)=y. \tag{7.28}$$

7.63.
Souvent, nous considérons une fonction $f\colon D\to\mathbb{R}$ avec $D\subset\mathbb{R}$. Dans ce cas, le X de la définition de la limite est D muni de la topologie induite de $\mathbb{R}$ vers D. Dans ce cas, la condition (7.27) s'écrit sous la forme

$$f\big(V\cap D\backslash\{a\}\big)\subset W. \tag{7.29}$$

où V est un voisinage de a dans $\mathbb{R}$ et non un voisinage de D dans D.

Remarque 7.64.
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 pas nécessaire que f soit définie en a pour que l'on puisse parler de limite de f en a. Par exemple nous avons

$$\lim_{x\to 1}\frac{x^2-1}{x-1}=2, \tag{7.30}$$

18. Définition 7.48.
19. Rappelons que ce n'est pas toujours le cas, mais que ça l'est si l'espace topologique est séparé – définition 7.30.

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 faisans du semblant d'anticiper) la définition (13.104). Dans la formule

$$f'(a) = \lim_{x\to a} \frac{f(x) - f(a)}{x - a}, \tag{7.31}$$

la fonction sur laquelle nous prenons la limite n'est *jamais* définie en $x = a$.

Cela est intimement lié à ce qu'on raconte dans 8.1.13.

Proposition 7.65 (Unicité de la limite pour un espace séparé)**.**
Soient X un espace topologique, A une partie de X et Y un espace topologique séparé[20]*. Nous considérons une fonction $f : A \to Y$. 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 :

$$\begin{cases} f(W \cap A) \subset V & \text{(7.32a)} \\ f(W' \cap A) \subset V'. & \text{(7.32b)} \end{cases}$$

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

$$f(W \cap W' \cap A) \subset f(W \cap A) \subset V, \tag{7.33}$$

et

$$f(W \cap W' \cap A) \subset f(W' \cap A) \subset V', \tag{7.34}$$

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 $y = y'$. □

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 7.66 (Fonction continue[106])**.**
Deux définitions :

*(1) Soient une fonction $f : X \to Y$ 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 $f : X \to Y$ est **continue** sur X si pour tout ouvert $\mathcal{O}$ de Y, l'ensemble*

$$f^{-1}(\mathcal{O}) = \{x \in X \text{ tel que } f(x) \in \mathcal{O}\} \tag{7.35}$$

est ouvert dans X.

20. Définition 7.30.

7.67.
Lorsque nous écrivons $f\colon X \to Y$, 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 $\mathbb{R} \to \mathbb{R}$, l'espace X sera la partie de $\mathbb{R}$ sur laquelle f sera définie, et la topologie sera la topologie induite de $\mathbb{R}$.

Exemple 7.68([1])
Un truc bien avec la définition 7.66(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

$$\begin{aligned} f\colon \{a\} &\to \mathbb{R} \\ a &\mapsto 4. \end{aligned} \tag{7.36}$$

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 $\varnothing$ soit $\{a\}$. Dans les deux cas c'est un ouvert. △

La proposition 9.50 donnera des détails sur ce qu'il se passe lorsque l'espace est métrique.

Théorème 7.69.
Une fonction $f\colon X \to Y$ 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.

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 7.4 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 7.70.
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 7.29 et la proposition 7.65.

Lemme 7.71 ([1])**.**
Soient une fonction $f\colon X \to Y$, et un point d'accumulation $a \in X$[21]*. 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 forciori, $f\big(V\backslash a\big) \subset W$ comme le demande la définition de la limite.

21. 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.

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 $f\big(V\backslash a\big) \subset W$. Mais vu que $f(a) \in W$, nous avons $f(V) \subset W$.

□

7.5.2.2 Continuité séquentielle

Définition 7.72.
*Si X et Y sont deux espaces topologiques, une fonction $f\colon X \to \mathbb{R}$ est **séquentiellement continue** en un point a si pour toute suite convergente $x_n \to a$ dans X nous avons $f(x_n) \to f(x)$ dans Y.*

Proposition 7.73 (Caractérisation séquentielle de la limite[1])**.**
Soient deux espaces topologiques X et Y ainsi qu'une fonction $f\colon X \to Y$. Soit $a \in X$ et $\ell \in Y$. Si

$$\lim_{x\to a} f(x) = \ell, \tag{7.37}$$

alors, pour toute suite (x_k) telle que $x_k \to a$, on a

$$\lim f(x_k) = \ell. \tag{7.38}$$

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 7.62 de la continuité en un point). Par la convergence $a_k \to a$, 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. □

Corollaire 7.74 (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 $f\colon X \to Y$ 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 $f(x_k) \to f(a)$.

Soit un voisinage V de $f(a)$ dans Y. Le fait que f soit continue en a signifie[22] que $f(a)$ est une limite de f en a, c'est-à-dire[23] qu'il existe un voisinage W de a tel que $f(W\backslash\{a\}) \subset V$.

Vu que $x_k \to a$, il existe N tel que $x_k \in W$ pour tout $k \geqslant N$. 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 $k \geqslant N$. Cela signifie exactement que $f(x_k) \to f(a)$. □

7.5.2.3 Application réciproque

Définition 7.75 (injection, surjection, bijection)**.**
Soient des ensembles A et B ainsi qu'une application $f\colon A \to B$.

*(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.

22. C'est la définition 7.66 de la continuité en un point.
23. Définition 7.62 d'être une limite.

Définition 7.76.
*Soit $f\colon A \to B$ une bijection. L'**application réciproque** de f est la fonction*

$$\begin{aligned} f^{-1}\colon B &\to A \\ y &\mapsto \text{le } x \in A \text{ tel que } f(x) = y. \end{aligned} \tag{7.39}$$

Plus généralement si $f\colon X \to Y$ est une application quelconque et si $S \subset Y$ nous notons

$$f^{-1}(S) = \{x \in X \text{ tel que } f(x) \in S\}, \tag{7.40}$$

et dans le cas où S est réduit à un unique élément y, nous notons $f^{-1}(y)$ au lieu de $f^{-1}\big(\{y\}\big)$. 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 7.77.
Soit $f\colon A \subset \mathbb{R}^n \to B \subset \mathbb{R}^m$ une bijection continue. Si A est compact, alors $f^{-1}\colon B \to A$ est continue.

Proposition 7.78.
Soient I un intervalle dans $\mathbb{R}$ et $f\colon I \to \mathbb{R}$ une fonction continue strictement monotone. Alors la fonction réciproque $f^{-1}\colon f(I) \to \mathbb{R}$ est continue sur l'intervalle $f(I)$.

7.5.2.4 Homéomorphisme

Définition 7.79.
*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 7.80 ([1])**.**
Soit une fonction $f\colon X \to Y$, continue sur l'ouvert A de X au sens où elle est continue en chaque point de A. Alors la fonction restriction $\tilde{f}\colon A \to Y$ est également continue pour la topologie sur A, induite[24] 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

$$f\big(W \backslash \{a\}\big) \subset V. \tag{7.41}$$

La partie $W \cap A$ est un voisinage de a pour la topologie de A, et vérifie

$$f\big(W \cap A \backslash \{a\}\big) \subset V. \tag{7.42}$$

donc $f(a)$ est une limite de $\tilde{f}$ pour $x \to a$. La fonction $\tilde{f}\colon A \to Y$ est continue en chaque point de A. □

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 7.81
Que signifie d'être continue pour une fonction $f\colon \mathbb{Q} \to \mathbb{R}$? D'après le théorème 7.69, il s'agit

24. Exemple 7.10.

d'être continue en chaque point de $\mathbb{Q}$. Il s'agit donc, par la définition 7.66 que pour tout $q \in \mathbb{Q}$, le nombre $f(q)$ soit une limite de f pour $x \to q$.

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 7.10 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 $|f(q) - f(q')|$.

Bref, c'est exactement le mécanisme usuel de la continuité sur $\mathbb{R}$, sauf qu'il faut seulement considérer les rationnels. △

Lemme 7.82 (Application partielle[1])**.**
Soient trois espaces topologiques X_1, X_2 et Y. Nous considérons une fonction continue $f\colon X_1 \times X_2 \to Y$ ainsi que $x_1 \in X_1$. Alors l'application

$$\begin{aligned} g\colon X_2 &\to Y \\ x_2 &\mapsto f(x_1, x_2) \end{aligned} \tag{7.43}$$

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 :

$$g^{-1}(\mathcal{O}) = \{x_2 \in X_2 \text{ tel que } (x_1, x_2) \in f^{-1}(\mathcal{O})\}. \tag{7.44}$$

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 7.9 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

$$(x_1, x_2) \in A_1 \times A_2 \subset f^{-1}(\mathcal{O}). \tag{7.45}$$

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

$$g(y_2) = f(x_1, x_2) \in \mathcal{O}. \tag{7.46}$$

Cela termine la démonstration. □

7.5.4 Continuité et connexité

Proposition 7.83.
Un espace topologique X est connexe si et seulement si toute application continue $X \to \mathbb{Z}$ est constante.

Proposition 7.84.
L'image d'un ensemble connexe par une fonction continue est connexe.

Démonstration. Soit $f\colon X \to Y$ 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. □

Une application de ce théorème sera le théorème de valeurs intermédiaires 13.50.

Exemple 7.85
Les espaces topologiques $\mathbb{R}$ et $\mathbb{R}^2$ ne sont pas homéomorphes. △

Démonstration. Supposons par l'absurde que $f\colon \mathbb{R} \to \mathbb{R}^2$ soit un homéomorphisme. Nous posons $E = f\big(\mathbb{R}\backslash\{0\}\big)$ et $z_0 = f(0)$. Vu que f est bijective nous avons

$$E = \mathbb{R}^2\backslash\{z_0\}, \tag{7.47}$$

qui est connexe.

Vu que E est connexe et que f^{-1} est continue, la proposition 7.84 nous dit que $f^{-1}(E)$ est connexe. Mais par définition, $f^{-1}(E) = \mathbb{R}\backslash\{0\}$ qui n'est pas connexe. □

7.5.5 Continuité et compacité

Théorème 7.86.
L'image d'un compact[25] *par une fonction continue est un compact.*

Dans le cadre des espaces vectoriels normés, ce théorème est démontré en la proposition 9.44.

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

$$f(K) \subseteq \bigcup_{\mathcal{O}\in\Omega} \mathcal{O}. \tag{7.48}$$

Par construction, nous avons aussi

$$K \subseteq \bigcup_{\mathcal{O}\in\Omega} f^{-1}(\mathcal{O}), \tag{7.49}$$

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

$$K \subseteq \bigcup_{i=1}^{n} f^{-1}(\mathcal{O}_i). \tag{7.50}$$

Dans ce cas, nous avons que

$$f(K) \subseteq \bigcup_{i=1}^{n} \mathcal{O}_i, \tag{7.51}$$

ce qui prouve la compacité de $f(K)$. □

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 7.87.
Si E est un ensemble, une ***distance*** *sur E est une application $d\colon E \times E \to \mathbb{R}$ telle que pour tout $x, y \in E$,*

(1) $d(x, y) \geqslant 0$

25. Définition 7.43.

(2) $d(x,y)=0$ *si et seulement si* $x=y$,
(3) $d(x,y)=d(y,x)$
(4) $d(x,y)\leqslant d(x,z)+d(z,y)$.

*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 7.88.
Soit (E,d) *un espace métrique. Nous définissons les **boules ouvertes** par*

$$B(x,r)=\{y\in E \text{ tel que } d(x,y)<r\}. \tag{7.52}$$

pout tout $x\in E$ *et* $r>0$. *Alors en posant*

$$\mathcal{T}=\big\{\mathcal{O}\subset E \text{ tel que } \forall x\in\mathcal{O},\exists r>0 \text{ tel que } B(x,r)\subset\mathcal{O}\big\} \tag{7.53}$$

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 $\varnothing\in\mathcal{T}$ parce que tout élément de l'ensemble vide ... heu ... enfin parce que d'accord hein [26]. 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 $B(x,r)\subset\bigcap_{i=1}^{n}A_i$. □

Remarque 7.89.
Quatre remarques à propos de cette définition.

(1) Cette définition est faite exprès pour respecter le théorème 7.4. Même si, a priori, on aurait dû utiliser la topologie engendrée faite à l'exemple 7.8... mais on peut montrer que les deux topologies sont les mêmes.
(2) Par construction, les boules ouvertes sont une base de la topologie (définition 7.54) 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 7.32 et 7.65 !

7.90.
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 1.73, en posant $d(x,y)=|x-y|$ nous avons une distance sur $\mathbb{K}$.

De plus, les boules définies en 1.73 sont alors les mêmes que celles définies en (7.52), ce qui donne à tout corps totalement ordonné une structure d'espace topologique.

7.6.1.1 Les boules, une base de topologie

Proposition 7.91.
Un espace métrique séparable [27] accepte une base de topologie 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*

$$\mathcal{B}=\{B(a_i,r_j)\}_{i,j\in\mathbb{N}} \tag{7.54}$$

est une base de la topologie de E.

26. Pour qui ne seraient pas d'accord, allez ajouter $\varnothing$ dans la définition des ouverts et puis c'est tout.
27. Qui possède une partie dense dénombrable, définition 7.31.

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 1.109).

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

$$\|y-x\| \leqslant \|y-a\| + \|a-x\| < \frac{2}{3}r + \frac{1}{3}r = r. \tag{7.55}$$

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. □

Remarque 7.92.
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 12.6).

Voir aussi le corollaire 15.212 qui donnera tout ouvert comme union de pavés presque disjoints.

Définition 7.93.
*Soit (X,d) un espace métrique. Un sous-ensemble $A \subset X$ est **borné** s'il existe une boule de X contenant A.*

Proposition 7.94.
Toute réunion finie d'ensembles bornés est un ensemble borné. Toute partie d'un ensemble borné est un ensemble borné.

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 maxima et minima de fonctions. Le théorème exact est le suivant.

Lemme 7.95 (de Lebesgue[107])**.**
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 $x_n \to x$. 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. □

Lemme 7.96 ([107])**.**
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 finis 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. □

Théorème 7.97 (Bolzano-Weierstrass[107], thème 11)**.**
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

$$X_n = \overline{\{x_k \text{ tel que } k > n\}}. \tag{7.56}$$

Ce sont des fermés ayant la propriété d'intersection finie non vide, et donc la proposition 7.52 nous dit qu'ils ont une intersection non vide. Un élément de cette intersection est automatiquement un point d'accumulation de la suite [28].

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 7.95, 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 7.96, nous considérons un ensemble fini $\{y_i\}_{i\in A}$ tel que le 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. □

Exemple 7.98(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. △

Le théorème de Bolzano–Weierstrass 7.97 a l'importante conséquence suivante.

Théorème 7.99 (Weierstrass)**.**
Une fonction continue à valeurs réelles définie sur un compact est bornée et atteint ses bornes.

Démonstration. Soient K un compact et $f\colon K \to \mathbb{R}$ une fonction continue. Nous désignons par A l'ensemble des valeurs prises par f sur K :

$$A = f(K) = \{f(x) \text{ tel que } x \in K\}. \tag{7.57}$$

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 1.122).

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 7.97. Afin d'alléger la notation, nous allons noter (x_n) la sous-suite convergente. Nous avons donc

$$x_n \to x \in K. \tag{7.58}$$

Par la proposition 7.74, nous avons que f prend en x la valeur

$$f(x) = \lim_{n\to\infty} f(x_n). \tag{7.59}$$

28. Définition 7.22.

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 $\lim_{n\to\infty} f(x_n) < \infty$. 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

$$M - \frac{1}{n} < f(x_n) \leqslant M. \tag{7.60}$$

En passant à la limite $n \to \infty$, ces inégalités deviennent

$$M \leqslant f(x) \leqslant M, \tag{7.61}$$

et donc $f(x) = M$, ce qui prouve que f atteint sa borne M au point $x \in K$. □

7.6.2 Distance à un ensemble

Définition 7.100.
Si A est une partie de l'espace métrique (X, d), et si $b \in X$, nous définissons

$$d(b, A) = \inf_{y\in A} d(b, y). \tag{7.62}$$

Lemme 7.101 ([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 7.2). 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 $d(b, A) \geqslant r$ et donc $d(b, A) \geqslant r > 0$. 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 7.102(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 7.103 ([1]).
Soient un espace métrique (X, d) ainsi qu'une partie $A \subset X$. Soit $r > 0$. La partie

$$\mathcal{O} = \{x \in X \text{ tel que } d(x, A)\} \tag{7.63}$$

est ouverte.

Démonstration. Soit $y \in \mathcal{O}$; nous avons $d(y, A) < r$. Autrement dit,

$$\inf_{a\in A} d(y, a) < r \tag{7.64}$$

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

$$d(z, a) \leqslant d(z, y) + d(y, a) < r - \delta + \delta = r. \tag{7.65}$$

□

Lemme 7.104 ([1]).
Si F est un fermé dans (X, d) et si x n'est pas dans F, alors $d(x, F) > 0$.

Lemme 7.105 ([1]).
Si A est une partie de (X, d), alors la fonction

$$\begin{aligned} f\colon \Omega &\to [0, \infty[\\ x &\mapsto d(x, A) \end{aligned} \tag{7.66}$$

est continue.

7.6.3 Norme

Définition 7.106 ([108], 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 $N\colon E\to\mathbb{R}^+$ telle que*

(1) $N(x)=0$ si et seulement si $x=0$;

(2) $N(\lambda x)=|\lambda|N(x)$ pour tout $\lambda\in\mathbb{R}$ et $x\in E$;

(3) $N(x+y)\leqslant N(x)+N(y)$

pour tout $x,y\in E$ et pour tout $\lambda\in\mathbb{K}$.

*La propriété (3) est appelée **inégalité triangulaire**.*

*Un espace vectoriel muni d'une norme est un **espace vectoriel normé**.*

En prenant $\lambda=-1$ dans la propriété (2), nous trouvons immédiatement que $N(-x)=N(x)$.

Proposition 7.107.
Toute norme N sur l'espace vectoriel E vérifie l'inégalité

$$\big|N(x)-N(y)\big|\leqslant N(x-y) \tag{7.67}$$

pour tout $x,y\in E$.

Démonstration. Nous avons, en utilisant le point (3) de la définition 7.106,

$$N(x)=N(x-y+y)\leqslant N(x-y)+N(y), \tag{7.68a}$$
$$N(y)=N(y-x+x)\leqslant N(y-x)+N(x). \tag{7.68b}$$

Supposons d'abord que $N(x)\geqslant N(y)$. Dans ce cas, en utilisant (7.68a),

$$\big|N(x)-N(y)\big|=N(x)-N(y)\leqslant N(x-y)+N(y)-N(y)=N(x-y). \tag{7.69}$$

Si par contre $N(x)\leqslant N(y)$, alors nous utilisons (7.68b) et nous trouvons

$$\big|N(x)-N(y)\big|=N(y)-N(x)\leqslant N(y-x)+N(x)-N(x)=N(y-x). \tag{7.70}$$

Dans les deux cas, nous avons retrouvé l'inégalité annoncée. □

Cette proposition signifie aussi que

$$-N(x-y)\leqslant N(x)-N(y)\leqslant N(x-y). \tag{7.71}$$

7.108.
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 7.107 s'énoncera donc

$$\big|\|x\|-\|y\|\big|\leqslant\|x-y\|. \tag{7.72}$$

Un espace vectoriel E muni d'une norme est, on l'a déjà dit, un **espace vectoriel normé** ; on le notera $(E,\|.\|)$ pour distinguer la norme fixée.

Une autre inégalité utile de temps en temps.

Corollaire 7.109.
Si a et b sont dans un espace vectoriel normé, alors

$$\big|\|a-b\|-\|b\|\big|\leqslant\|a\|. \tag{7.73}$$

Démonstration. Il s'agit seulement de la proposition 7.107 avec $x=a-b$ et $y=-b$. □

Lemme-définition 7.110 (Distance induite par une norme)**.**
Soit un espace vectoriel normé $(E, \|.\|)$. Nous posons

$$d(x, y) = \|x - y\|. \tag{7.74}$$

Alors

(1) d est invariante par translations : $d(a, b) = d(a + u, b + u)$

(2) d est une distance[29] *sur E.*

C'est la ***distance induite*** *par la norme.*

Démonstration. Le fait que la formule (7.74) 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

$$d(x, y) = \|x - y\| = \|x - z + z - y\| \leqslant \|x - z\| + \|z - y\| = d(x, z) + d(z, y). \tag{7.75}$$

□

Corollaire 7.111.
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 9.28.

29. Définition 7.87.

Chapitre 8

Topologie sur les réels

8.1 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 1.93.

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 1.73(2) permet de définir une norme sur $\mathbb{R}$.

Lemme 8.1.
L'application

$$x \mapsto |x| \tag{8.1}$$

est une norme sur $\mathbb{R}$.

Démonstration. Grâce au lemme 1.76 et à la remarque 1.77, on a, pour tous $x,\ y,\ \lambda \in \mathbb{R}$:

(1) $|x| = 0$ implique $x = 0$,

(2) $|\lambda x| = |\lambda||x|$,

(3) $|x + y| \leqslant |x| + |y|$,

et donc, les conditions de la définition 7.106 sont immédiatement vérifiées. □

8.2.
Nous verrons plus tart que cette norme donne lieu à une structure d'espace topologique. Tant sur $\mathbb{Q}$ que sur $\mathbb{R}$, nous considérons la topologie métrique correspondant à cette norme (hors cas rarissimes qui seront signalés). De plus, nous utiliserons toujours les caractérisations de la proposition 9.26 pour parler de suites convergentes et de suites de Cauchy.

Proposition 8.3.
Les rationnels sont denses dans les réels.

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 1.109 dit qu'il existe un rationnel dans $]x-\epsilon/2, x+\epsilon/2[$ et donc dans $B(x, \epsilon)$. □

Proposition 8.4 ([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 1.109 donne un élément $x_\delta \in \mathbb{Q}$ tel que

$$x - \delta < x_\delta < x. \tag{8.2}$$

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 :

$$\begin{cases} \delta_i = x - x_i & \text{(8.3a)} \\ x_{i+1} = x_{\delta_i/2} \in \mathbb{Q}. & \text{(8.3b)} \end{cases}$$

Ainsi nous avons pour tout i les inégalités

$$x_i = x - \delta_i < x - \frac{\delta_i}{2} < x_{i+1} < x. \tag{8.4}$$

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

$$x_{k+1} \in B(x, \frac{\delta_k}{2}) \subset B(x, \epsilon). \tag{8.5}$$

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. □

8.1.1 Compacité pour les réels

Pour la définition générale d'un compact, c'est 7.43.

Proposition 8.5.
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 haut [1]. 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.

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},... 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 $\mathbb{R}\backslash K$ 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 $B(x, \epsilon_1)$, 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. □

Théorème 8.6 (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 1.123. Un compact est fermé et borné (proposition 8.5). 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.

1. Nous laissons à titre d'exercice le cas où K est borné par le haut et pas par le bas.

Soit Ω, un recouvrement du segment $[a,b]$ par des ouverts, c'est-à-dire que

$$[a,b] \subseteq \bigcup_{\mathcal{O}\in\Omega} \mathcal{O}. \tag{8.6}$$

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 c ; 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 7.39), ce qui prouve que $M=[a,b]$, et donc que $[a,b]$ est compact [2]. □

Lemme 8.7 ([109]).
Si $a<b\in\mathbb{R}$ alors le segment $[a,b]$ est compact [3].

Démonstration. Soit $\{\mathcal{O}_i\}_{i\in I}$ un recouvrement de $[a,b]$ par des ouverts. Nous posons

$$M=\{x\in[a,b] \text{ tel que } [a,x] \text{ admet un sous-recouvrement fini extrait de } \{\mathcal{O}_i\}_{i\in I}\}. \tag{8.7}$$

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 $c\in M$.

2. Si vous n'aimez pas le coup du fermé et ouvert, le lemme 8.7 donne une autre preuve.
3. Définition 7.43

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 $[a,b]$. □

Lemme 8.8 ([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 7.56 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 $B(x_i,m_{x_i})\times\{K_2\}$. □

8.1.2 Conséquence : les fermés bornés sont compacts

Théorème 8.9 (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.

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 $\mathcal{O}_0=\complement\bigcup_i\overline{B(x_i,\frac{1}{5})}$, qui est ouvert comme complément d'un fermé. Pour $i\geqslant 1$ nous posons $\mathcal{O}_i=B(x_i,\frac{1}{4})$. Nous avons

$$K\subset\bigcup_{i\in\mathbb{N}}\mathcal{O}_i \tag{8.8}$$

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 la proposition 7.58.

Sens réciproque.

Un intervalle fermé et borné est compact dans $\mathbb{R}$ C'est le lemme 8.7.

Un produit de segments est compact Le produit de deux compacts de $\mathbb{R}$ est un compact dans $\mathbb{R}^2$ par le lemme 8.8.

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 7.59.

□

Exemple 8.10(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

$$B(0,1)\backslash\bigcup_i\overline{B(e_i,\frac{1}{4})}. \tag{8.9}$$

Le tout recouvre $B(0,1)$ mais toutes les premières boules sont nécessaires. △

Le théorème de Bolzano-Weierstrass 8.19 nous permettra de prouver plus simplement la non compacité en dimension infinie. Voir l'exemple 7.98.

8.1.3 Suites et limites dans les réels

8.1.3.1 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 8.11 (Limite d'une suite numérique)**.**
La suite (x_n) est convergente si et seulement s'il existe un réel ℓ tel que

$$\forall \epsilon > 0,\ \exists N \in \mathbb{N} \text{ tel que } \forall n \geqslant N,\ |x_n - \ell| < \epsilon. \tag{8.10}$$

Dans ce cas, le nombre ℓ est la limite de la suite (x_n). Nous dirons aussi souvent que la suite ***converge*** *vers le nombre ℓ.*

Démonstration. La limite d'une suite dans un espace topologique est la définition 7.25.

Si $x_n \to \ell$ et si $\epsilon > 0$ il existe N_ϵ tel que pour tout $n \geqslant N$ nous avons $x_n \in B(\ell, \epsilon)$ (parce que cette boule est un ouvert contenant ℓ). Vu la définition d'une boule (définition 7.88) et de la norme sur $\mathbb{R}$ (par 8.2), cette condition est bien $|x_n - \ell| < \epsilon$.

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 (8.10) nous assure qu'il existe N_ϵ tel que pour tout $n \geqslant N_\epsilon$ nous ayons

$$x_n \in B(\ell, \epsilon) \subset \mathcal{O}, \tag{8.11}$$

ce qui assure que la suite (x_n) converge vers ℓ pour la topologie métrique de $\mathbb{R}$. □

Une façon équivalente d'exprimer le critère (8.10) 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.

Nous disons qu'une suite réelle (x_n) converge[4] vers ℓ lorsque pour tout ε, il existe un N tel que

$$n > N \Rightarrow |x_n - \ell| \leqslant \varepsilon. \tag{8.12}$$

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 7.106). Nous pouvons donc facilement définir le concept de convergence d'une suite dans un espace vectoriel normé.

D'ailleurs, voici la proposition 8.11 écrite dans le cadre d'un espace vectoriel normé.

Définition 8.12.
Soit une suite (x_n) dans un espace vectoriel normé V. Nous disons qu'elle est ***convergente*** *s'il existe un élément $\ell \in V$ tel que*

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N} \text{ tel que } n \geqslant N \Rightarrow \|x_n - l\| < \varepsilon. \tag{8.13}$$

Dans ce cas, ℓ est appelé la ***limite*** *de la suite (x_n).*

4. Voir la définition 8.11 pour plus de détail.

8.1.3.2 Opérations sur les limites

Lemme 8.13.
Si a et b sont des suites dans $\mathbb{R}$, et si elles sont convergentes, alors la suite somme $a+b$ est convergente et sa limite est la somme des limites.

Démonstration. La fonction

$$\begin{aligned} f\colon \mathbb{R}\times\mathbb{R} &\to \mathbb{R} \\ (x,y) &\mapsto x+y \end{aligned} \tag{8.14}$$

est continue. Donc elle commute avec la limite. Nous notons x et y les limites des suites (x_n) et (y_n). Le calcul est le suivant [5] :

$$\lim(x_n+y_n) = \lim f(x_n,y_n) = f\big(\lim_{n\to\infty}(x_n,y_n)\big) = f(x,y) = x+y. \tag{8.15}$$

□

Proposition 8.14 ([1])**.**
Soient des suites à valeurs réelles (a_i) et (b_j) si elles sont convergentes, alors la suite ab est convergente et

$$\big(\lim_i a_i\big)\big(\lim_j b_j\big) = \lim_i (a_ib_i). \tag{8.16}$$

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

$$|a_ib_i-ab| \leqslant |a_ib_i-a_ib|+|a_ib-ab| \tag{8.17a}$$
$$\leqslant |a_i||b_i-b|+b|a_i-a|. \tag{8.17b}$$

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

$$|a_ib_i-ab| \leqslant (R+b)\eta<\epsilon. \tag{8.18}$$

□

8.1.4 Exemples

Exemple 8.15
Quelques suites usuelles.

(1) La suite $x_n=\frac{1}{n}$ converge vers 0.

(2) La suite $x_n=(-1)^n$ ne converge pas.

△

Deux limites pour voir comment ça fonctionne.

Lemme 8.16.
Si $r>1$ nous avons :

(1) $\lim_{n\to\infty} r^n=\infty$.

(2) $\lim_{n\to\infty}\frac{r^n}{n}=\infty$.

5. Assurez vous d'être capable de justifier les étapes.

Démonstration. Vu que $r > 1$ nous pouvons écrire $r = 1 + \delta$ avec $\delta > 0$. La formule du binôme de Newton (3.73) nous donne

$$(1 + \delta)^n = \sum_{k=0}^{n} \binom{k}{n} \delta^k > \binom{1}{n} \delta = n\delta. \tag{8.19}$$

La proposition 1.108 ($\mathbb{R}$ 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

$$\frac{a_{n+1}}{a_n} = \frac{n}{n+1} r. \tag{8.20}$$

Vu que $\frac{n}{n+1} \to 1$, 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 $n > N$,

$$\frac{n}{n+1} r > 1 + \delta. \tag{8.21}$$

Soit maintenant $k \in \mathbb{N}$. En utilisant un produit télescopique,

$$a_{N+k} = a_N \frac{a_{N+1}}{a_N} \frac{a_{N+2}}{a_{N+1}} \cdots \frac{a_{N+k}}{a_{N+k-1}} > a_N (1 + \delta)^{k-1}. \tag{8.22}$$

Or $(1 + \delta)^{k-1}$ tend vers ∞ lorsque $k \to \infty$ par le premier point. Donc nous avons $\lim_{n\to\infty} r^n/n = \infty$. □

Définition 8.17.
*Nous disons que deux suites (u_n) et (v_n) sont **équivalentes** s'il existe une fonction $\alpha\colon \mathbb{N} \to \mathbb{R}$ telle que*

(1) pour tout n à partir d'un certain rang, $u_n = v_n \alpha(n)$

(2) $\alpha(n) \to 1$.

8.1.5 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 $x_n \leqslant M$ pour tout n. De la même manière, la suite est bornée inférieurement s'il existe un m tel que $x_n \geqslant m$ pour tout n.

Le lemme suivant est souvent utilisé pour prouver qu'une suite est convergente.

Lemme 8.18.
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.

Théorème 8.19 (Bolzano-Weierstrass, thème 11)**.**
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 7.43 de la compactié). Nous avons donc des points $a_1, \dots, a_n$ tels que

$$K \subset \bigcup_{i=1}^{n} \mathcal{O}_{a_i} \tag{8.23}$$

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 1.26 qui dit que $\mathbb{N}$ est infini. □

Proposition 8.20.
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

$$\lim x_n = \Big(\lim(x_n)_1, \lim(x_n)_2, \dots, \lim(x_n)_m \Big) \tag{8.24}$$

où $(x_n)_k$ dénote la k-ième composante de (x_n).

Exemple 8.21
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 8.20, nous devons calculer séparément les limites

$$\begin{aligned} \lim \frac{1}{n} &= 0 \\ \lim \left(1 - \frac{1}{n}\right) &= 1. \end{aligned} \tag{8.25}$$

△

Exemple 8.22
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 $\mathbb{R}^2$. △

8.1.6 Suites adjacentes

Définition 8.23 ([110]).
*Les suites (a_n) et (b_n) sont **adjacentes** si l'une est croissante, l'autre décroissante et si $a_n - b_n \to 0$.*

Théorème 8.24 (Théorème des suites adjaentes).
Nous considérons des suites adjacentes (a_n) et (b_n) avec (a_n) croissante et (b_n) décroissante. Alors

(1) $b_n \geqslant a_n$ pour tout n,

(2) $a_n \leqslant b_q$ 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 $a_n \leqslant \ell \leqslant b_n$ pour tout n.

Démonstration. La suite $n \mapsto b_n - a_n$ est décroissante parce que $b_n - a_n \geqslant b_{n+1} - a_{n+1}$. Comme en plus $b_a - a_n \to 0$ nous avons

$$b_n - a_n \geqslant 0 \tag{8.26}$$

pour tout $n \in \mathbb{N}$. De plus $a_n \leqslant b_0$ pour tout n parce que si $a_N > b_0$ alors, b étant décroissante, $a_N > b_0 \geqslant b_N$ qui est contraire à ce que nous venons de prouver. La suite a étant croissante et majorée, elle est convergente [6] ; notons ℓ sa limite.

La suite b peut maintenant être écrite par

$$b_n = (b_n - a_n) + a_n \tag{8.27}$$

6. Proposition 8.18.

qui est une somme de deux suites convergentes. Elle est donc convergente et sa limite est la somme des limites [7], donc

$$\lim_{n\to\infty} b_n = \lim_{n\to\infty}(b_n - a_n) + a_n = 0 + \ell = \ell. \tag{8.28}$$

Voila. Donc les suites a et b convergent et ont la même limite.

Pour tout $n, q \in \mathbb{N}$ nous avons l'inégalité $a_n \leqslant b_q$. En prenant la limite $n \to \infty$ nous trouvons

$$\ell \leqslant b_q \tag{8.29}$$

pour tout q. Et de la même façon, $b_n \geqslant a_q$ donne $\ell \geqslant a_q$. L'un avec l'autre donne

$$a_q \leqslant \ell \leqslant b_q \tag{8.30}$$

pour tout $q \in \mathbb{N}$. □

Proposition 8.25 ([111]).
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 $a_n \to \ell$.

Démonstration. Soit $\epsilon > 0$. Il existe N_1 tel que $|a_{2n} - \ell| \leqslant \epsilon$ dès que $n \geqslant N_1$. Il existe également N_2 dès que $|a_{2n+1} - \ell| \leqslant \epsilon$ dès que $n \geqslant N_2$.

Nous posons $N = \max\{2N_1, 2N_2 + 2\}$ et nous avons, pour tout $n \geqslant N$:

$$|a_n - \ell| \leqslant \epsilon, \tag{8.31}$$

c'est-à-dire que $a \to \ell$. □

8.1.7 Limite supérieure et inférieure

Lemme-définition 8.26.
Soit (a_n) une suite dans $\bar{\mathbb{R}}$. Les limites suivantes existent dans $\bar{\mathbb{R}}$

$$\limsup_{n\to\infty} a_n = \lim_{n\to\infty}\big(\sup_{k\geqslant n} a_k\big) \tag{8.32}$$

et

$$\liminf_{n\to\infty} a_n = \lim_{n\to\infty}\big(\inf_{k\geqslant n} a_k\big). \tag{8.33}$$

*Elles sont nommées **limite supérieure** et la **limite inférieure** de la suite (a_k).*

Démonstration. Pour la limite supérieure, l'ensemble des $k \geqslant n$ est de plus en plus petit lorsque n grandit. Donc les ensembles $A_n = \{a_k \text{ tel que } k \geqslant n\}$ sont emboîtés et la suite $n \to \sup A_n$ est une suite décroissante. Elle a donc une limite dans $\bar{\mathbb{R}}$. □

8.27.
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

$$\limsup_{n\to\infty} A_n = \bigcap_{n\geqslant 1}\bigcup_{k\geqslant n} A_k \tag{8.34}$$

et

$$\liminf_{n\to\infty} A_n = \bigcup_{n\geqslant 1}\bigcap_{k\geqslant n} A_k \tag{8.35}$$

Nous avons

$$\limsup A_n = \{\omega \in \Omega \text{ tel que } \omega \in A_n \text{pour une infinité de } n\}. \tag{8.36}$$

7. Lemme 8.13.

Lemme 8.28.
Nous avons les formules pratiques suivantes :

$$\limsup a_n = \inf_{n\geqslant 1}\left(\sup_{k\geqslant n} a_k\right) \tag{8.37a}$$

$$\liminf a_n = \sup_{n\geqslant 1}\left(\inf_{k\geqslant n} a_k\right). \tag{8.37b}$$

Démonstration. La suite $n \mapsto \sup_{k\geqslant n} a_k$ est une suite décroissante, donc la limite est l'infimum. Même argument pour l'autre. □

Lemme 8.29.
La suite (a_n) dans $\mathbb{R}$ converge si et seulement si

$$\limsup a_n = \liminf a_n. \tag{8.38}$$

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 $n \geqslant N$ nous avons

$$\left|\sup_{k\geqslant n} a_k - l\right| < \epsilon \tag{8.39}$$

et

$$\left|\inf_{k\geqslant n} a_k - l\right| < \epsilon. \tag{8.40}$$

Pour tout $k \geqslant N$ nous avons alors $a_k \leqslant l + \epsilon$ et $a_k \geqslant l - \epsilon$. Cela donne $a_n \in B(l, \epsilon)$, c'est-à-dire $a_k \to l$ par la proposition 8.11.

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 $n \geqslant N_\epsilon$. Si $n \geqslant N_\epsilon$ nous avons

$$\left|\sup_{k\geqslant n} a_k - l\right| \leqslant \epsilon \tag{8.41}$$

et donc la limite de $\sup_{k\geqslant n} a_k$ lorsque $n \to \infty$ est bien l. □

8.1.8 Ouverts, voisinage, topologie

Lorsque $x \in E$, nous rappelons qu'un voisinage[8] de x est n'importe quel sous-ensemble de E qui contient une boule ouverte centrée en x. La proposition 7.4 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 7.89(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 bornée[9] s'il existe une boule[10] qui contient A.

Mais revenons à $\mathbb{R}$...

Lemme 8.30.
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 $\mathcal{O}$. □

8. Définition 7.2.
9. Définition 7.93.
10. À titre d'exercice, convainquez-vous que l'on peut dire boule *ouverte* ou *fermée* au choix sans changer la définition.

Par le même genre de raisonnements, on montre que l'union et l'intersection de deux ouverts sont encore des ouverts.

Remarque 8.31.
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 $\bigcap_{i=1}^{\infty} \mathcal{O}_i$.

Proposition 8.32.
Quels que soient les ensembles A et B dans $\mathbb{R}$, nous avons

$$\sup(A \cap B) \leqslant \sup A \leqslant \sup(A \cup B).$$

Nous laissons le lecteur le prouver, même si ce n'est pas dans notre habitude.

8.1.9 Intervalles et connexité

Nous allons déterminer tous les sous-ensembles connexes[11] de $\mathbb{R}$. Pour cela nous relisons d'abord la notion d'intervalle donnée en 1.13 ainsi que la proposition 1.123 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 $\sup(I)$[12] sont les **extrémités** de I.

Définition 8.33.
*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 $s : [0, 1] \to \mathbb{R}^p$, $s(t) = (1 - t)a + tb$. 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 22.7.

Le segment $[b, a]$ est l'image de l'application $r\colon [0, 1] \to \mathbb{R}^p$ donnée par $r(t) = (1 - t)b + ta$.

Proposition 8.34.
Une partie de $\mathbb{R}$ est connexe si et seulement si c'est un intervalle.

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

$$\mathcal{O}_1 =]m, x_0[$$
$$\mathcal{O}_2 =]x_0, M[.$$

11. Définition 7.38.
12. Qui existent par la proposition 1.122, quitte à poser $\pm\infty$ comme infimum et supremum lorsque I n'est pas borné.

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 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 une 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 ouvert [13], le point x_0 n'est pas dans l'ensemble par le lemme 8.30. Nous avons donc

— soit x_0 n'est pas dans $\mathcal{O}_1$,

— soit $x_0 \leqslant b$,

— soit les deux en même temps.

Nous allons montrer qu'un tel x_0 ne peut pas être dans A. D'abord, remarquons que $\sup \mathcal{A} \leqslant \sup \mathcal{O}$ 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 $x_0 \leqslant b$, 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 $x_0 \geqslant a$. Mais par construction, on a aussi que $x_0 \leqslant b$ (ici, l'inégalité est même stricte, mais ce n'est pas important). Donc

$$a \leqslant x_0 \leqslant b$$

avec $a, b \in A$, et $x_0 \notin A$. Cela finit de prouver que A n'est pas un intervalle. □

Théorème 8.35 (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 $f\colon K \to \mathbb{R}$. Alors le théorème 7.86 indique que $f(K)$ est compact. Par conséquent $f(K)$ est un fermé borné de $\mathbb{R}$ par le théorème de Borel-Lebesgue 8.9. 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 $f(y) = \inf f(K)$. □

Le théorème suivant est essentiellement inutile pour les raisons suivantes :

13. C'est l'intersection entre l'ouvert $\mathcal{O}_1$ et l'ouvert $\{x \text{ tel que } x < b\}$.

— Il est un cas particulier du théorème 7.97 qui donne pour tout espace métrique, l'équivalence entre la compacité et la compacité séquentielle.

— Il est une cas particulier du théorème 8.19 qui le donne pour tous les espaces compacts.

— Il utilise le cas particulier de $\mathbb{R}$, qui n'est pas démontré directement dans le Frido.

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 8.36 (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 8.9.

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

$$|a_n| \leqslant \|x_n\| \leqslant M. \tag{8.42}$$

La suite (a_n) est donc une suite réelle bornée et donc contient une sous-suite convergente par le théorème correspondant dans $\mathbb{R}$: 7.97. 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.

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 8.20.

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 ».

$$\begin{array}{lcccccccccc}
x_{\mathbb{N}} & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \dots \\
x_{I_1} & \times & \bullet & \bullet & \times & \bullet & \times & \times & \bullet & \bullet & \bullet & \dots \\
x_{I_2} & \times & \bullet & \times & \times & \bullet & \times & \times & \bullet & \bullet & \times & \dots \\
\vdots & & & & & & & & & & & \\
x_{I_m} & \times & \times & \times & \times & \bullet & \times & \times & \times & \bullet & \times & \dots
\end{array} \tag{8.43}$$

La première ligne, $x_{\mathbb{N}}$, est la suite de départ. □

Corollaire 8.37.
Si un 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 8.19. Si ℓ est la limite de cette sous-suite alors nous avons $\ell \geqslant x_n$ 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

$$x_{\alpha(n)} + \epsilon > \ell. \tag{8.44}$$

Vu que la suite est croissante pour tout $m > \alpha(K)$ nous avons $x_m + \epsilon > l$, ce qui signifie $|x_m - \ell| < \epsilon$. □

Nous aurons une version pour les fonctions croissantes et bornées en la proposition 13.66.

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 8.38.
Une partie non dénombrable de $\mathbb{R}^n$ possède un point d'accumulation[14].

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 1.31) et donc une suite. Or une suite dans un compact possède un point d'accumulation par le théorème 8.19.

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. □

8.1.10 Recouvrement d'un compact 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.

Nous notons $\mathcal{A} = \{B_i\}_{i\in I}$ où I est un ensemble d'indices (un ensemble quelconque).

$$s_1(A) = \{i \in I \text{ tel que } B_i \cap A \neq \varnothing\} \tag{8.45a}$$

$$\sigma_1(A) = \bigcup_{B\in s_1(A)} B. \tag{8.45b}$$

Et ensuite :

$$s_{k+1}(A) = \{i \in I \text{ tel que } B_i \cap \sigma_k(A) \neq \varnothing\} \tag{8.46a}$$

$$\sigma_{k+1}(A) = \bigcup_{B\in s_{k+1}(A)} B \tag{8.46b}$$

Lemme 8.39.
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 $I_1 \cap A \neq \varnothing$ alors

(1) $\sigma_N = \sigma_{N+1}$

(2) $A \subset \sigma_N(I_1)$.

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 $\text{Card}(\sigma_k) \geqslant k$ et en particulier $N \leqslant \text{Card}(\sigma_N) \leqslant N$. 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

$$\sigma_N(I_1) = I_1 \cup \dots \cup I_n. \tag{8.47}$$

L'ensemble

$$\tau = \bigcup_{k=n+1}^{N} I_k \tag{8.48}$$

est ouvert et est disjoint de $\sigma_N(I_1)$ parce que si I_l ($I_l \geqslant n+1$) intersectait $\sigma_N(I_1)$, nous aurions $l \in s_{N+1}$ ou encore $I_l \subset \sigma_{N+1}\backslash\sigma_N$.

Donc τ et σ_N sont deux ouverts disjoints qui recouvrent A. Vu que A est un intervalle, il est connexe[15]. Donc soit $A \subset \tau$ soit $A \subset \sigma_N$. Comme $I_1 \cap A \neq \varnothing$ nous sommes dans le cas $A \subset \sigma_N$. □

14. Définition 7.22.
15. Définition 7.38 et proposition 8.34.

8.1.11 Connexité par arcs

Définition 8.40.
Le sous-ensemble $A \subset \mathbb{R}^n$ est ***connexe par arcs*** *si pour tout $x, y \in A$, il existe un chemin*[16] *contenu dans A les reliant, c'est-à-dire une application continue*

$$\gamma : [0,1] \to \mathbb{R}^n \text{ tel que } \gamma(0) = x \text{ et } \gamma(1) = y$$

avec $\gamma(t) \in A$ pour tout $t \in [0,1]$.

8.41.
La connexité d'un ensemble n'implique pas sa connexité par arc. Il suffit pour cela de prendre un ensemble constitué de deux connexes reliés par un chemin de longueur infinie (le graphe d'une fonction de type $\sin(1/x)$ par exemple).

8.1.12 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 $f\colon \mathbb{R} \to \mathbb{R}$, que signifie $\lim_{x\to\infty} f(x)$? Il s'agit de considérer la fonction élargie

$$\begin{aligned} \tilde{f}\colon \bar{\mathbb{R}} &\to \bar{\mathbb{R}} \\ x &\mapsto \begin{cases} f(x) & \text{si } x \in \mathbb{R} \\ 0 & \text{si } x = \pm\infty. \end{cases} \end{aligned} \tag{8.49}$$

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 $\lim_{x\to a} f(x) = \pm\infty$.

8.1.13 Limite pointée ou épointée ?

Si vous êtes dans l'enseignement en France[17], vous devriez lire ceci à propos de limite pointée. Dans tous les autres cas, la limite pointée est une notion qui ne vous intéresse a priori pas.

Définition 8.42 ([112])**.**
Soient X et Y deux espaces topologiques, A une partie de X, f une application de A dans Y, a un point de X adhérent à A et ℓ un point de Y. On dit que ℓ est une ***limite pointée*** *de f au point a si pour tout voisinage V de ℓ, il existe un voisinage W de a tel que pour tout point x de $W \cap A$, l'image $f(x)$ appartient à V.*

La notion de limite pointée ne diffère de la limite que du fait que pour calculer la limite pointée en a, nous tenons compte des valeurs de f sur *tout* le voisinage de a, y compris le point a lui-même.

16. Attention : ici quand on dit *chemin*, on demande que l'application soit continue. Dans de nombreux cours de géométrie différentielle, on demande C^∞. Il faut s'adapter au contexte.
17. En particulier si vous voulez passer l'agrégation.

(1) Dans la majorité des cas, la limite pointée donne le même résultat que la limite parce que, fondamentalement, si nous voulons calculer une limite de f au point a, c'est que f n'est pas définie en a. C'est en particulier toujours le cas pour les limites en l'infini ou les limites définissant les dérivées.

(2) La fonction f donnée par
$$f(x) = \begin{cases} 0 & \text{si } x \neq 0 \\ 4 & \text{si } x = 0 \end{cases} \tag{8.50}$$
a une limite pour $x \to 0$ et c'est $\lim_{x\to 0} f(x) = 0$. Elle n'a par contre pas de limite pointée en 0.

Cette fonction est l'exemple-type de différence entre limite usuelle et limite pointée.

(3) Les quelques théorèmes liant limite et continuité sont un peu différents si on veut les écrire pour lier limite pointée et continuité.

(4) La limite pointée capte un peu moins bien la notion intuitive de « ce que fais la fonction lorsque x s'approche de a », parce que le plus souvent nous voulons savoir ce que fait la fonction précisément lorsque x s'*approche* de a, pas quand x *est* en a.

(5) Dans la suite, nous n'utiliserons jamais la limite pointée parce qu'elle n'ajoute rien et n'est pratiquement utilisée nulle part à part dans l'enseignement en France.

Si vous voulez un cas dans lequel la différence se voit de façon macroscopique, aller lire le lemme 13.152, sa démonstration et l'exemple 13.153.

Que devez-vous faire ?

Enseignement en France La notion de limite pointée est celle nommée « limite » dans les programmes, et ce que nous nommons ici « limite » est nommé « limite épointée ». Peut-être pour induire en erreur tout le reste de la planète ?

Recherche Si vous faites de la recherche où que ce soit y compris en France, la seule définition de limite est la limite dite « épointée », celle qui sera toujours utilisée dans le Frido.

Doctorat Vous commencez un doctorat en math, et vous avez vu la limite pointée comme seule définition de limite durant vos études ? Oubliez-la. Ou alors attendez-vous à vous à de sérieux quiproquos lorsque vous discuterez de mathématique avec des étrangers.

8.1.14 Quelques mots à propos de la droite réelle complétée

Définition 8.43.
*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 8.44 (Topologie sur $\bar{\mathbb{R}}$)**.**
La topologie sur $\bar{\mathbb{R}}$ est celle sur $\mathbb{R}$ à laquelle nous ajoutons les voisinages de $\pm\infty$ de la façon suivante. Une partie V de $\bar{\mathbb{R}}$ 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 complétée [18].

Lemme 8.45.
L'adhérence de $\mathbb{R}$ dans $\overline{\mathbb{R}}$ est $\overline{\mathbb{R}}$.

Pour la suite nous utilisons la notation (pratique en probabilité)
$$\{f < a\} = \{x \in S \text{ tel que } f(x) < a\}. \tag{8.51}$$

18. Mais ne justifie pas le qualificatif « complété » parce que l'espace métrique $\mathbb{R}$ était déjà complet.

8.2 Topologie réelle en dimension n

Dans cette section, nous travaillons dans l'espace $\mathbb{R}^n$ pour un certain naturel n. Nous y définissons la notion d'ouvert et de fermé, qui sont la base de la topologie générale. Notons que ces définitions n'ont de sens que relativement à l'espace ambiant, aussi un ouvert de $\mathbb{R}$ ne sera en général pas un ouvert de $\mathbb{R}^2$: d'une part, il n'y a pas d'inclusion canonique de $\mathbb{R}$ dans $\mathbb{R}^2$ (les ouverts du second ne sont même pas des sous-ensembles du premier) et, d'autre part, les définitions se basent sur la notion de boule de $\mathbb{R}^n$ qui dépend évidemment de la valeur de n (une boule dans $\mathbb{R}$ est un intervalle, dans $\mathbb{R}^2$ c'est un disque, etc.)

8.2.1 Ouverts et fermés

Définition 8.46.
*La **boule ouverte** de centre $x_0 \in \mathbb{R}^n$ et de rayon $r \in \mathbb{R}^+$ est définie par*

$$B(x_0, r) = \{x \in \mathbb{R}^n \text{ tel que } \|x - x_0\| < r\}, \tag{8.52}$$

*tandis que la **boule fermée** de centre x_0 et de rayon r est*

$$\bar{B}(x_0, r) = \{x \in \mathbb{R}^n \text{ tel que } \|x - x_0\| \leqslant r\}; \tag{8.53}$$

la différence est que l'inégalité dans la première est stricte.

Définition 8.47.
*Une partie A de $\mathbb{R}^n$ est **ouverte** si pour tout $a \in A$ il existe $r > 0$ tel que $B(a, r) \subset A$. Une partie est donc ouverte lorsqu'elle contient une boule autour de chacun de ses éléments.*

Cette définition est évidemment à mettre en rapport avec le théorème 7.4.
Le lemme suivant justifie le vocabulaire des définitions 8.46.

Lemme 8.48.
Pour tout $x \in \mathbb{R}^n$ et tout $r > 0$ la boule $B(x, r)$ 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 $B\big(p, r - d(p, x)\big)$ est contenue dans $B(x, r)$. Pour cela, nous prenons $p' \in B\big(p, r - d(p, x)\big)$, et nous essayons de prouver que $p' \in B(x, r)$. En effet, en utilisant l'inégalité triangulaire,

$$d(x, p') \leqslant d(x, p) + d(p, p') \leqslant d(x, p) + r - d(p, x) = r. \tag{8.54}$$

□

8.2.2 Intérieur, adhérence et frontière

Définition 8.49.
*Soient $A \subset \mathbb{R}^n$ et $x \in \mathbb{R}^n$. Le point x est **intérieur** à A s'il existe une boule autour de x complètement contenue dans A. L'ensemble des points intérieurs à A est noté* $\operatorname{Int} A$ *ou $\mathring{A}$, de sorte qu'on a précisément*

$$x \in \operatorname{Int} A \overset{def}{\iff} \exists \epsilon > 0 \text{ tel que } B(x, \epsilon) \subset A.$$

8.50.
La notion d'adhérence a déjà été définie en 7.17, et précisé par le lemme 7.18. 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 :

$$x \in \operatorname{Adh} A \overset{\text{def}}{\iff} \forall \epsilon > 0, B(x, \epsilon) \cap A \neq \varnothing \tag{8.55}$$

Proposition 8.51.
Pour $A \subset \mathbb{R}^n$, nous avons

$$\text{Int}\, A \subseteq A \subseteq \text{Adh}\, A$$

Définition 8.52.
*La **frontière** ou le **bord** de A est défini par $\partial A = \text{Adh}\, A \backslash \text{Int}\, A$. L'ensemble A est un **ouvert** si $A = \text{Int}\, A$, et c'est un **fermé** si $A = \text{Adh}\, A$.*

Lemme 8.53 (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 $x \in Adh(S)$ (définition 7.17), 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. □

Corollaire 8.54.
Un ensemble et son complémentaire ont même frontière.

Démonstration. Conséquence du lemme 8.53. 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 8.55
Soit $X = [0, 1]$ muni de la topologie de la distance $|x - y|$ (définition 7.88). 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

$$B(1, r) = \{x \in X \text{ tel que } |x - 1| < r\} =]1 - r, 1] \tag{8.56}$$

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 $\mathbb{R}$. △

Lemme 8.56 (Passage de douane[113, 114])**.**
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 $X\backslash\bar{A}$ ne peuvent pas recouvrir γ parce que ce sont deux ouverts disjoints alors que γ est connexe (voir la définition 7.38 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. □

On vérifiera que les notations et les dénominations sont cohérentes en prouvant la proposition suivante.

Proposition 8.57.
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 8.58.
Si $A \subset \mathbb{R}^n$ et $A^c = \mathbb{R}^n \backslash A$, 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 8.59
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, $A \cap B = \varnothing$ alors que $\bar{A} \cap \bar{B} = \{1\}$. △

8.2.3 Point d'accumulation, point isolé

Les définitions de point d'accumulation et de point isolé sont 7.22 et 7.23. Nous voyons maintenant ce que ces définitions donnent dans le cas de l'espace topologique $\mathbb{R}$.

Lemme 8.60.
Soit $D \subset \mathbb{R}$. Un point $a \in D$ est isolé dans D si et seulement si il existe $\varepsilon > 0$ tel que

$$[a - \varepsilon, a + \varepsilon] \cap D = \{a\}. \tag{8.57}$$

Autrement dit, il existe un intervalle autour de a dans lequel a est le seul élément de D.

Lemme 8.61.
Un point $a \in \mathbb{R}$ est un point d'accumulation de D si pour tout $\varepsilon > 0$,

$$\Big([a - \varepsilon, a + \varepsilon]\backslash\{a\}\Big) \cap D \neq \varnothing. \tag{8.58}$$

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 8.62
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. △

Exemple 8.63
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. △

Exemple 8.64
Soit $D =]1, 2[\cup \{12\}$. Le point 12 est adhérence, mais pas d'accumulation parce que le voisinage $]9, 14[$ n'intersectionne pas $D\backslash\{12\}$. △

8.2.4 Limite de suite

Définition 8.65 (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*

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N} \text{ tel que } \forall n \geqslant N,\ \|x_n - \ell\| < \varepsilon. \tag{8.59}$$

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 $x_n \to \ell$.*

Notez aussi la similarité avec la définition 8.11.

Remarque 8.66.
Nous n'écrivons pas « $\lim_{n\to\infty} x_n$ » 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 $\lim_{n\to 4} x_n$ parce que cela vaudrait x_4 et rien d'autre.

Ceci est une différence importante avec les limites de fonctions.

Lemme 8.67 (Unicité de la limite)**.**
Il ne peut pas y avoir deux nombres différents qui satisfont à la condition (8.59)*. 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

$$\|x_n - \ell\| < \varepsilon \tag{8.60}$$

pour tout $n \geqslant N$, et $N' > 0$ tel que

$$\|x_n - \ell'\| < \epsilon \tag{8.61}$$

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

$$\|\ell - \ell'\| = \|\ell - x_n + x_n - \ell'\| \leqslant \|\ell - x_n\| + \|x_n - \ell'\| < 2\varepsilon. \tag{8.62}$$

Cela prouve que $\|\ell - \ell'\| = 0$. □

Le théorème de Bolzano-Weierstrass 7.97 dit que dans le cas métrique, la compacité séquentielle est équivalente à la compacité.

Chapitre 9

Topologie générale, le retour

9.1 Topologie et distance

Lemme 9.1.
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

$$\big\{B(y_1, r_1) \times B(y_2, r_2)\big\}_{\substack{y_i \in A_i \\ r_i \in \mathbb{Q}^+}} \tag{9.1}$$

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 produit [1], 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

$$(x_1, x_2) \in B(y_1, \frac{r_1}{2}) \times B(y_2, \frac{r_2}{2}). \tag{9.2}$$

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

$$d_i(z_i, x_i) \leqslant d(z_i, y_i) + d(y_i, x_i) \leqslant \frac{r_i}{2} + \frac{r_i}{2} = r_i. \tag{9.3}$$

Au final,

$$(x_1, x_2) \in B(y_1, \frac{r_1}{2}) \times B(y_2, \frac{r_2}{2}) \subset \mathcal{O}. \tag{9.4}$$

□

Définition 9.2.
*Si (X, d_X) et (Y, d_Y) sont des espaces métriques, une **isométrie** est une application bijective $f : X \to Y$ telle que pour tout $x, y \in X$ nous ayons*

$$d_Y\big(f(x), f(y)\big) = d_X(x, y). \tag{9.5}$$

Remarque 9.3.
Une application vérifiant (9.5) est automatiquement injective. En pratique, il ne faut donc vérifier que la surjectivité.

Exemple 9.4(Manque de surjectivité)
Si $X = [0, \infty[$ et $f(x) = x + 1$ alors f vérifie (9.5) pour la distance $d(x, y) = |x - y|$, mais n'est pas surjective. △

1. Définition 7.9.

Proposition-définition 9.5 (Groupe des isométries)**.**
Si (X, d) est un espace métrique,

(1) l'ensemble des isométries de X, noté $\mathrm{Isom}(X)$ *est un groupe pour la composition.*

(2) Ce groupe agit fidèlement[2] *sur X.*

Proposition 9.6.
Une isométrie entre deux espaces métriques est continue.

Démonstration. Soient $f\colon X \to Y$ une application isométrique et $\mathcal{O}$ un ouvert de Y. Soit $a \in f^{-1}(\mathcal{O})$; si $d(a,b) < r$, alors $d\big(f(a), f(b)\big) < r$ et donc $b \in f^{-1}\big(B(f(a), r)\big)$. 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. □

Exemple 9.7
Si X est un ensemble, nous pouvons écrire la **distance discrète** :

$$d(x,y) = \begin{cases} 0 & \text{si } x = y \\ 1 & \text{si } x \neq y. \end{cases} \tag{9.6}$$

La topologie résultante est la topologie discrète, côtoyée dans l'exemple 7.6 [3].

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. △

9.1.0.1 Distance point-ensemble

Définition 9.8.
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*

$$d(x, A) = \inf_{a \in A} d(x, a). \tag{9.7}$$

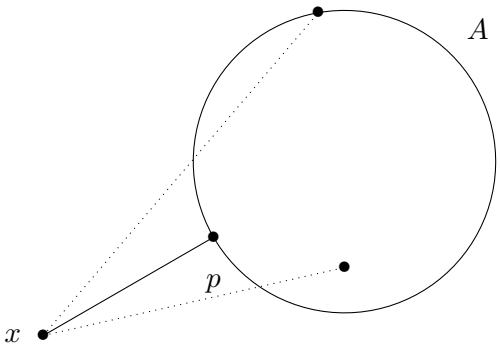


FIGURE 9.1 – La distance entre x et A est donnée par la distance entre x et p. Les distances entre x et les autres points de A sont plus grandes que $d(x,p)$.

9.1.1 Suites et espaces métriques

Proposition 9.9 (Caractérisation séquentielle de la limite[1])**.**
Soient deux espaces métriques X et Y ainsi qu'une fonction $f\colon X \to Y$. Soit $a \in X$ et $\ell \in Y$. On a

$$\lim_{x \to a} f(x) = \ell, \tag{9.8}$$

2. Si vous ne savez pas ce que c'est, alors vous avez zappé la définition 2.46.
3. Vérifiez-le tout de même !

si et seulement si, pour toute suite (x_k) telle que $x_k \to a$, on a

$$\lim f(x_k) = \ell. \tag{9.9}$$

Par ailleurs, l'une des deux limites existe si et seulement si l'autre existe.

Démonstration. Le sens direct est la proposition 7.73. 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 $x \to a$. 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 $B(\ell,\epsilon)$. □

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.

Corollaire 9.10 (Caractérisation séquentielle de la continuité en un point[1])**.**
Si X et Y sont des espaces métriques, alors une fonction $f\colon X \to Y$ 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 $\|x - a\| \leqslant \delta$ et $\|f(x) - f(a)\| > \epsilon$. Nous considérons un tel ϵ et pour chaque $n \geqslant 1 \in \mathbb{N}$ nous considérons un x_n correspondant à $\delta = \frac{1}{n}$. Cela nous donne une suite $x_n \to a$ dans X mais $\|f(x_n) - f(a)\|$ reste plus grand que ϵ. Cela montre que f n'est pas non plus séquentiellement continue. □

Les espaces métriques ont une propriété importante que la fermeture séquentielle est équivalente à la fermeture.

Proposition 9.11 (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 7.26. 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 $X\backslash F$ ne soit pas ouvert. Alors il existe $x \in X\backslash F$ 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. □

Lemme 9.12.
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 corollaire 7.27 ; 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[4] $B(\ell, r) \cap A = \varnothing$. 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 $x_n \to \ell$. □

Corollaire 9.13.
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.

4. Une autre manière de dire la même chose : si $\ell \notin \bar{A}$, alors $d(\ell, A) > 0$.

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 ou de la lectrice). □

En termes savants, ce corollaire signifie que la fermeture $\bar{A}$ est composé de A plus de toutes les limites de toutes les suites contenues dans A.

Proposition 9.14 (Caractérisation séquentielle de la continuité[1])**.**
Soient X et Y deux espaces métriques. Soit $f\colon X \to Y$ une application séquentiellement continue (en tout $a \in X$). Alors f est continue.

Démonstration. 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 $x_k \in \complement f^{-1}(\mathcal{O})$ pour tout k. Nous allons montrer que $x \in \complement f^{-1}(\mathcal{O})$ et la caractérisation séquentielle[5] de la fermeture conclura que $\complement f^{-1}(\mathcal{O})$ est fermé.

Pour tout k, nous avons $f(x_k) \in \complement\mathcal{O}$, mais $\mathcal{O}$ est ouvert et $f(x_k) \xrightarrow{Y} f(x)$ parce que f est séquentiellement continue. Par conséquent $f(x) \in \complement\mathcal{O}$ et $x \in \complement f^{-1}(\mathcal{O})$. □

Proposition 9.15.
Si X et Y sont deux espaces métriques et $f, g\colon X \to Y$ sont deux fonctions continues égales sur une partie dense de X alors $f = g$.

Démonstration. Les fonctions f et g sont séquentiellement continues (proposition 7.74, ou proposition 9.10). 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 $a_n \to x$. La séquentielle continuité de f et g donnent

$$f(a_n) \to f(x) \tag{9.10a}$$
$$g(a_n) \to g(x), \tag{9.10b}$$

mais pour tout n, $f(a_n) = g(a_n)$. Par unicité de la limite[6] dans Y, $f(x) = g(x)$. □

9.1.2 Espace métrisable

Définition 9.16 (Espace vectoriel topologique métrisable[115])**.**
*Un espace topologique est **métrisable** si il existe une distance compatible avec la topologie.*

Proposition 9.17 ([116])**.**
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

$$V_n = \{x \in X \text{ tel que } d(x, A) < \frac{1}{n}\}. \tag{9.11}$$

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 7.4. 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).

5. Proposition 9.11.
6. Proposition 7.65.

Soient $\epsilon > 0$ que nous fixerons plus bas, et $y \in B(x,\epsilon)$. L'inégalité triangulaire donne

$$d(y,a) \leqslant d(y,x) + d(x,a) < \epsilon + \frac{1}{n}. \tag{9.12}$$

Nous pouvons donc choisir ϵ de telle sorte que $d(y,a) < 1/n$. Avec ce ϵ, nous avons, pour tout $y \in B(x,\epsilon)$:

$$d(y,A) \leqslant d(y,a) < \frac{1}{n} \tag{9.13}$$

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 7.101.

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

$$\mathcal{O}^c = \bigcap_{n\in\mathbb{N}} V_n, \tag{9.14}$$

ce qui donne immédiatement

$$\mathcal{O} = \bigcup_{n\in\mathbb{N}} V_n^c \tag{9.15}$$

où les V_n^c sont fermés. □

Corollaire 9.18.
Si X est un espace topologique métrisable, alors X accepte une base dénombrable de topologie autour de chaque point.

Démonstration. Il s'agit seulement de remarquer que les singletons sont fermés et d'appliquer la proposition 9.17. □

9.2 Suites de Cauchy, métrique et espaces complets

9.2.1 Généralités

Définition 9.19 (Suite de τ-Cauchy, espace vectoriel topologique[117, 118])**.**
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 $k,l \geqslant N$.*

Définition 9.20 (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 converge*[7] *vers un élément de A.*

Définition 9.21 (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 $n,m \geqslant N$ 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 1.73). Dans ce contexte, le ϵ était pris dans le corps lui-même.

Définition 9.22 (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. Définition 7.25.

9.23.
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 9.25 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 coincident.

Définition 9.24.
*Un **espace de Banach** est un espace vectoriel normé complet*[8] *pour la topologie de la norme.*

Exemple 9.25(La complétude n'est pas une propriété topologique[119])
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 $\mathbb{N}$:

$$d_1(x,y) = \left|\frac{1}{x} - \frac{1}{y}\right|. \tag{9.16}$$

Pour vérifier que cette formule définit bien une distance (définition 7.87), le seul point non immédiat est l'inégalité triangulaire :

$$d_1(x,y) = \left|\frac{1}{x} - \frac{1}{y}\right| \leqslant \left|\frac{1}{x} - \frac{1}{z}\right| + \left|\frac{1}{z} - \frac{1}{y}\right| = d_1(x,z) + d_1(z,y). \tag{9.17}$$

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

$$\left|\frac{1}{x} - \frac{1}{y}\right| < \epsilon \tag{9.18}$$

pour $y \in \mathbb{N}$. Nous trouvons que $\frac{1}{y} > \frac{1}{x} - \epsilon$ et $\frac{1}{y} < \frac{1}{x} + \epsilon$, soit

$$\begin{cases} y > \dfrac{1}{\frac{1}{x} + \epsilon} & \text{(9.19a)} \\ y < \dfrac{1}{\frac{1}{x} - \epsilon}. & \text{(9.19b)} \end{cases}$$

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 discrète[9].

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

$$(\mathbb{N}, d) \simeq (\mathbb{N}, d_1). \tag{9.20}$$

8. Définition 9.22.
9. Celle dont toutes les parties sont des ouverts.

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 1.109) nous avons, pour $n, m > N$:

$$\left|\frac{1}{n} - \frac{1}{m}\right| < \frac{1}{n} < \frac{1}{N} < \epsilon. \tag{9.21}$$

Or cette suite ne converge pas. Soit en effet un candidat limite k. Calculons

$$d_1(x_n, k) = \left|\frac{1}{n} - \frac{1}{k}\right| \to \frac{1}{k} \neq 0. \tag{9.22}$$

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.

△

9.2.2 Espace topologique métrique

Dans les espaces vectoriels topologiques métriques, il n'y a pas d'ambiguïté.

Proposition 9.26 (Caractérisations avec la distance d)**.**
Soit (E, d) un espace vectoriel topologique métrique.

(1) Une suite (x_n) dans E est convergente[10] *vers x si et seulement si pour tout $\epsilon \in \mathbb{R}$ il existe N_ϵ tel que pour tout $n \geqslant N_\epsilon$ nous avons $d(x_n, x) \leqslant \epsilon$.*

(2) Une suite (x_n) dans E est de Cauchy[11] *si pour tout $\epsilon \in \mathbb{R}$, il existe un N_ϵ tel que si $p, q \geqslant N_\epsilon$, nous avons $d(x_p, x_q) \leqslant \epsilon$.*

Démonstration. En ce qui concerne la convergence :

Sens direct Nous supposons que $x_k \to x$ 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 $d(x, x_k) \leqslant \epsilon$.

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 7.88 et en particulier la liste des ouverts est donnée par (7.53). 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 :

10. Définition 7.25.
11. Définition 9.19.

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 $p, q \geqslant N_\epsilon$ alors $x_p - x_q \in B(0,\epsilon)$. Posons $u = x_p - x_q$; en utilisant l'invariance par translation (lemme 7.110(1)) nous avons

$$d(u,0) = d(x_p - x_q, 0) = d(x_p, x_q). \tag{9.23}$$

Par conséquent $d(x_p, x_q) \leqslant \epsilon$.

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 $d(x_p, x_q) \leqslant \epsilon$ dès que $p, q \geqslant N_\epsilon$. En utilisant encore l'invariance par translation nous avons

$$d(x_p, x_q) = d(x_p - x_q, 0), \tag{9.24}$$

et comme cela est plus petit que ϵ, nous avons $x_p - x_q \in B(0,\epsilon) \subset \mathcal{O}$.

□

Proposition 9.27 ([120]).
Toute suite convergente dans un espace métrique est de Cauchy.

Démonstration. Nous utilisons les caractérisations de la proposition 9.26 des suites convergentes et de Cauchy.

Soit un espace métrique (X,d) et $x_n \to \ell$ une suite convergente. Si $\epsilon > 0$, la proposition 9.26(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

$$d(x_n, x_m) \leqslant d(x_m, \ell) + d(l, x_m) \leqslant 2\epsilon. \tag{9.25}$$

Cela prouve que (x_n) est une suite de Cauchy. □

9.3 Topologie et espace vectoriel

9.3.1 Espace vectoriel topologique

Définition 9.28.
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[12] $V \times V \to V$ *; et*

(2) la multiplication par un scalaire est une application continue[13] $\mathbb{K} \times V \to V$.

On le redit quand même : le corps[14] 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 9.29 ([118]).
Pour $x \in V$ et $\lambda \in \mathbb{K}$, $\lambda \neq 0$ fixés, les fonctions T_x et M_λ définies par :

$$\begin{aligned} T_x : V &\to V \\ y &\mapsto x + y \end{aligned} \qquad \text{et} \qquad \begin{aligned} M_\lambda : V &\to V \\ y &\mapsto \lambda y \end{aligned} \tag{9.26, 9.27}$$

sont des homéomorphismes de V dans V.

Démonstration. Ce sont des bijections continues, dont les inverses sont respectivement T_{-x} et $M_{1/\lambda}$. □

12. Naturellement, l'espace $V \times V$ est muni de la topologie produit.
13. Naturellement, l'espace $\mathbb{K} \times V$ est muni (lui aussi) de la topologie produit.
14. Définition 1.61

Corollaire 9.30 (Invariance de la topologie [118]).
Toute base de voisinage de 0 *se transporte en tout point de l'espace vectoriel topologique.*

Lemme 9.31 ([118]).
Soit V un espace vectoriel topologique, et W un voisinage de 0*. Il existe U un voisinage de* 0*, symétrique*[15]*, tel que $U + U = W$.*

Démonstration. Par continuité de l'addition et par la définition de la topologie produit, il existe U_1 et U_2 tels que $U_1 + U_2 \subset W$. 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, si bien que $U + U = W$. □

Définition 9.32.
Une distance d sur un espace vectoriel topologique V est dite ***compatible*** *avec la topologie si la topologie induite*[16] *de d est celle de V.*

Une distance d sur un espace vectoriel V est dite ***invariante*** *si pour tout $x, y, u \in V$ nous avons*

$$d(x + u, y + u) = d(x, y). \tag{9.28}$$

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.

Théorème 9.33 ([118]).
Si V est un espace vectoriel topologique possédant en tout point une base de topologie dénombrable, 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. Grâce à la proposition 9.30, on peut tout ramener en 0 puis faire les transports en tous les points de l'espace. Mieux : grâce à la proposition 9.31 (appliquée deux fois de suite), on peut créer une base de voisinage (U_n) de 0 telle que pour tout $n \in \mathbb{N}$,

$$U_{n+1} + U_{n+1} + U_{n+1} + U_{n+1} \subset U_n. \tag{9.29}$$

Pour tous entiers naturels n et k, on obtient alors

$$U_{n+1} + U_{n+2} + \cdots + U_{n+(k-1)} + U_{n+k} \subset U_{n+1} + U_{n+1} \subset U_n. \tag{9.30}$$

On construit à présent, pour tout $n \in \mathbb{N}$, l'ensemble

$$D_n = \left\{ \sum_{i=1}^{n} \frac{c_i}{2^i} \text{ tel que } \forall i = 1, \cdots, n, c_i \in \{0, 1\} \right\}, \tag{9.31}$$

et $D = \cup_{n>0} D_n$. Ensuite, définissons ϕ sur $D \cup [1, +\infty[$ et à valeurs dans les parties de V :

$$\phi(r) = \begin{cases} V & \text{si } r \geqslant 1; \\ c_1 U_1 + \cdots + c_n U_n & \text{si } r \in D_n. \end{cases} \tag{9.32}$$

Quelques remarques sur cette fonction.

(1) $\phi(r) + \phi(s) \subset \phi(r + s)$: Si déjà $r + s \geqslant 1$, c'est clair. Sinon, on se place dans D_n avec le n qui va bien – de telle sorte que r, s et $r + s$ soient dedans. Notons :

$$r = \sum_{i=1}^{n} \frac{r_i}{2^i}; \tag{9.33}$$

$$s = \sum_{i=1}^{n} \frac{s_i}{2^i}; \tag{9.34}$$

$$r + s = \sum_{i=1}^{n} \frac{t_i}{2^i}. \tag{9.35}$$

15. C'est-à-dire que, pour tout $x \in V$, on a $x \in U$ si et seulement si $-x \in U$.
16. Définition 7.88.

Deux cas se produisent. Si pour tout i, $t_i = r_i + s_i$, alors

$$\phi(r+s) = \sum_i t_i U_i = \sum_i r_i U_i + \sum_i s_i U_i = \phi(r) + \phi(s); \tag{9.36}$$

l'égalité a lieu car r_i et s_i ne peuvent jamais valoir 1 en même temps.
Sinon, posons k le plus petit entier tel que $t_k \neq r_k + s_k$. Alors, nécessairement, $r_k = 0$, $s_k = 0$ et $t_k = 1$. Il s'ensuit, grâce à (9.29) et (9.30), que

$$\phi(r) = \sum_{i=1}^{k-1} r_i V_i + \sum_{i=k+1}^{n} r_i V_i \subset \sum_{i=1}^{k-1} r_i V_i + V_{k+1} + V_{k+1}; \tag{9.37}$$

$$\phi(s) = \sum_{i=1}^{k-1} s_i V_i + \sum_{i=k+1}^{n} s_i V_i \subset \sum_{i=1}^{k-1} s_i V_i + V_{k+1} + V_{k+1}; \text{ d'où} \tag{9.38}$$

$$\phi(r) + \phi(s) = \sum_{i=1}^{k-1} r_i V_i + \sum_{i=1}^{k-1} s_i V_i + V_{k+1} + V_{k+1} + V_{k+1} + V_{k+1} = \sum_{i=1}^{k-1} t_i V_i + V_k \subset \phi(r+s). \tag{9.39}$$

(2) $0 \in \phi(r)$ *pour tout* r *:* en effet, $\phi(r)$ n'est jamais vide, c'est toujours un voisinage de 0.

(3) *si* $r < s$ *alors* $\phi(r) \subset \phi(s)$ *:* il suffit d'écrire

$$\phi(r) \subset \phi(r) + \phi(s-r) \subset \phi(s). \tag{9.40}$$

Enfin, on définit

$$d(x,y) = \inf\{r \in [0;1] \text{ tel que } y - x \in \phi(r)\}. \tag{9.41}$$

Il suffit alors de voir que d convient. De par sa définition, il est clair qu'elle est invariante par translation ; reste à voir que c'est bien une distance, et qu'elle est compatible avec la topologie.

$d(x,x) = 0$ Oui, car 0 est dans $\phi(r)$, pour tout r, puisque les U_i sont des voisinages de 0.

$d(x,y) = d(y,x)$ Oui, car tous les voisinages considérés sont symétriques : pour tout i et tout $x \in V$, on a $x \in U_i$ si et seulement si $-x \in U_i$.

$d(x,z) \leqslant d(x,y) + d(y,z)$ Soit $\epsilon > 0$. Par définition des distances comme infimums, et grâce au corollaire 1.113, il existe r et s dans D tels que :

$$d(x,y) < r < d(x,y) + \frac{\epsilon}{2} \quad \text{et} \quad d(y,z) < s < d(y,z) + \frac{\epsilon}{2}. \tag{9.42}$$

Comme $d(x,y) + d(y,z) < r + s$, et par la remarque (3) sur ϕ, on a $y - x \in \phi(r)$ et $z - y \in \phi(s)$; donc

$$(y-x) + (z-y) = z - x \in \phi(r) + \phi(s) \subset \phi(r+s) \tag{9.43}$$

Ainsi, pour tout $\epsilon > 0$, on a

$$d(x,z) \leqslant r + s < d(x,y) + d(y,z) + \epsilon. \tag{9.44}$$

Compatibilité avec la topologie Si $d(0,y) < r$, alors $y \in \phi(r)$; en particulier pour $r = 1/2^k$, on a $y \in \phi(r) = V_k$. D'où, pour tout $n \in \mathbb{N}$, $B(0, 1/2^n) \subset V_n$.

□

Proposition 9.34.
Un espace vectoriel topologique[17] *est métrisable si et seulement si il possède en tout point une base dénombrable de topologie.*

Démonstration. Il s'agit seulement de mettre bout à bout les corollaires 9.18 et théorème 9.33. □

17. Définition 9.28.

9.3.2 Équivalence entre Cauchy et $\tau-$Cauchy

Lemme 9.35.
Soit un espace vectoriel topologique[18] V *et une distance* $d\colon V\times V\to\mathbb{R}^+$ *compatible*[19] *avec la topologie de* V*. Si* d *est invariante*[20]*, 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

$$d(0,x_m-x_n)<\epsilon, \tag{9.45}$$

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 9.36.
Soit V *un espace vectoriel topologique métrisable*[21]*, 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 9.33. Vu qu'elle est invariante par translation, les suites d-Cauchy sont exactement les suites τ-Cauchy par le lemme 9.35. □

Remarque 9.37.
Même si V est métrisable, si on choisit la métrique n'importe comment, on ne peut rien espérer.

9.38.
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.

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 1.118 qui en est un lemme indispensable mais qui parle de notions différentes, bien que très liées.

Théorème 9.39 (Complétude de $\mathbb{R}$, critère de Cauchy[9])**.**
Nous avons :

(1) L'espace métrique $(\mathbb{R},d)$ *est complet (définition 9.22).*

18. Définition 9.28.
19. Définition 9.32.
20. Définition 9.32.
21. i.e. admet une base dénombrable de topologie, voir la proposition 9.34

(2) *Une suite dans $\mathbb{R}$ est convergente (définition 7.25) si et seulement si elle est de Cauchy (définition 9.36).*

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 1.73).

Donc si (x_n) est de Cauchy dans $(\mathbb{R}, d)$, elle est de Cauchy dans le corps ordonné $(\mathbb{R}, \leqslant)$. Donc le théorème 1.118 nous dit que (x_n) est convergente dans $(\mathbb{R}, \leqslant)$. Et donc convergente dans $(\mathbb{R}, d)$.

Toutes les autres affirmations se prouvent de la même manière. □

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 1.118 en remplaçant partout $\mathbb{Q}$ par $\mathbb{R}$, et aussi en remplaçant les $|x - y|$ par $d(x, y)$.

9.40.
Nous pouvons également mettre une structure d'espace métrique sur $\mathbb{C}$ en posant

$$d(z, z') = |z - z'|. \tag{9.46}$$

Proposition 9.41.
L'espace métrique $(\mathbb{C}, d)$ est complet.

Démonstration. Commençons par nous rendre compte que pour tout $z \in \mathbb{C}$ nous avons $|\operatorname{Re}(z)| \leqslant |z|$. 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 $x_k = \operatorname{Re}(z_j)$, nous avons

$$|x_k - x_l| = |\operatorname{Re}(z_k - z_l)| \leqslant |z_k - z_l|. \tag{9.47}$$

Vu que (z_k) est de Cauchy, il existe un N tel que si $k, l \geqslant N$,

$$|x_k - x_l| \leqslant |z_k - z_l| \leqslant \epsilon. \tag{9.48}$$

Donc la suite des parties réelles converge par la complétude de $(\mathbb{R}, d)$ du théorème 9.39. 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 suffisament grand,

$$|z_k - (x + iy)| = \big|\operatorname{Re}(z_k) - x + i(\operatorname{Im}(z_k) - y)\big| \leqslant |x_k - x| + |y_k - y| \leqslant \epsilon. \tag{9.49}$$

□

9.4 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 13.42 que la fonction $f : \mathbb{R} \to \mathbb{R}$ est continue en a si et seulement si pour tout $\varepsilon > 0$, il existe un $\delta > 0$ tel que

$$|x - a| \leqslant \delta \Rightarrow |f(x) - f(a)| \leqslant \varepsilon. \tag{9.50}$$

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) $|x + y| \leqslant |x| + |y|$

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 :

$$\text{taille de } (a, b) = \sqrt{a^2 + b^2}. \tag{9.51}$$

Nous pouvons introduire une notion de distance entre les éléments de $\mathbb{R}^2$ de façon similaire :

$$d\big((a_x, a_y), (b_x, b_y)\big) = \sqrt{(a_x - b_x)^2 + (a_y - b_y)^2}. \tag{9.52}$$

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.

9.4.0.1 Critère de Cauchy

Lemme 9.42.
Une suite de Cauchy[22] *dans un espace vectoriel normé admettant une sous-suite convergente est elle-même convergente vers la même limite.*

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 $m, p \geqslant N$. Nous allons montrer que si $k > N$ alors $\|a_k - \ell\| < 2\epsilon$. Pour cela nous considérons un $n > N$ tel que $\|a_n - \ell\| \leqslant \epsilon$ et nous calculons

$$\|a_k - \ell\| \leqslant \|a_k - a_n\| + \|a_n - \ell\| \leqslant 2\epsilon. \tag{9.53}$$

□

Dans le cas des espaces de dimension finie, le fait d'être complet est automatique, comme le montre la proposition suivante.

Proposition 9.43.
Soit $\big(E, \|.\|\big)$ *un espace vectoriel normé de dimension finie sur un corps* $\mathbb{K}$ *qui est complet*[23]. *Alors* E *est complet*[24].

Pour rappel, la complétude de l'espace métrique $\mathbb{R}$ est la proposition 1.79.

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

$$\|f_n - f_m\| = \|\sum_\alpha (a_{n\alpha} - a_{m\alpha}) e_\alpha\| = \sum_\alpha |a_{n\alpha} - a_{m\alpha}|^2. \tag{9.54}$$

22. Définition 9.21.
23. La définition est 1.73, 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 $\mathbb{C}$.
24. Définition 9.22.

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 $(a_{n\alpha})_{\alpha\in\mathbb{N}}$ 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

$$\|f_n - f\| = \|\sum_\alpha (a_{n\alpha} - a_\alpha)e_\alpha\|, \tag{9.55}$$

dont la limite $n \to \infty$ est bien zéro. Donc la suite (f_n) converge vers $f \in E$. L'espace E est alors complet. □

Proposition 9.44.
Soient V et W deux espaces vectoriels normés. Soient K une partie compacte de V et $f\colon K \to W$ une fonction continue. Alors l'image $f(K)$ est compacte dans W.

Ce résultat est démontré dans un cadre plus général par le théorème 7.86.

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 8.19). 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

$$f(a) = \lim f(x'_n) = \lim y_n. \tag{9.56}$$

Cela prouve que la limite de (y_n) est dans $f(K)$ et par conséquent que $f(K)$ est fermé.

$f(K)$ **est borné** Si $f(K)$ n'est pas borné, nous pouvons trouver une suite (x_n) dans K telle que

$$\|f(x_n)\|_W > n \tag{9.57}$$

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

$$|f(a)| = \lim |f(x'_n)|. \tag{9.58}$$

La suite $f(x'_n)$ est alors une suite bornée, ce qui n'est pas possible au vu de la condition (9.57) imposée à la suite de départ (x_n).

□

Corollaire 9.45.
Si $f\colon K \to \mathbb{R}$ 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 9.44 montre que $f(K)$ est compact et donc borné. □

9.4.1 Quelques exemples de normes sur $\mathbb{R}^n$

Il est possible de définir de nombreuses normes sur $\mathbb{R}^n$. Citons-en quelques-unes.

Proposition-définition 9.46.
Les formules suivantes définissent des normes sur $\mathbb{R}^n$.

(1) Les normes $\|.\|_{L^p}$ *(*$p \in \mathbb{N}$*) sont définies de la façon suivante :*

$$\|x\|_{L^p} = \Big(\sum_{i=1}^{n} |x_i|^p \Big)^{1/p}, \tag{9.59}$$

pour tout $x = (x_1, \dots, x_n) \in \mathbb{R}^n$.

(2) La norme L^2 *est la* ***norme euclidienne****.*

(3) Nous définissons également la ***norme supremum*** *par*

$$\|x\|_\infty = \max_i |x_i|. \tag{9.60}$$

Démonstration. Point par point [25].

(1)

(2) Le fait que $x \mapsto \|x\|_{L^2}$ soit une norme provient de la propriété suivante :

$$\sqrt{(a+b)^2} \leqslant \sqrt{a^2} + \sqrt{b^2}, \tag{9.61}$$

laquelle se démontre en passant au carré :

$$(a+b)^2 = a^2 + b^2 + 2ab \leqslant a^2 + b^2 + 2|ab| = \big(\sqrt{a^2} + \sqrt{b^2}\big)^2. \tag{9.62}$$

(3)

□

Parmi ces normes, celles qui seront le plus souvent utilisées dans ces notes sont

$$\begin{aligned} \|x\|_{L^1} &= \sum_{i=1}^{n} |x_i|, \\ \|x\|_{L^2} &= \Big(\sum_{i=1}^{n} |x_i|^2 \Big)^{1/2}. \end{aligned} \tag{9.63}$$

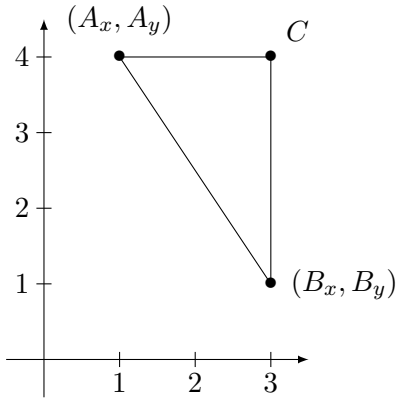


FIGURE 9.2 – La *norme* euclidienne induit la *distance* euclidienne. D'où son nom. Le point C est construit aux coordonnées (A_x, B_y).

Soient $A = (A_x, A_y)$ et $B = (B_x, B_y)$ deux éléments de $\mathbb{R}^2$. La distance [26] euclidienne entre A et B est donnée par $\|A - B\|_2$. En effet, sur la figure 9.2, la distance entre les points A et B est donnée par

$$|AB|^2 = |AC|^2 + |CB|^2 = |A_x - B_x|^2 + |A_y - B_y|^2, \tag{9.64}$$

par conséquent,

$$|AB| = \sqrt{|A_x - B_x|^2 + |A_y - B_y|^2} = \|A - B\|_2. \tag{9.65}$$

25. Preuve non terminée

26. Ne pas confondre « distance » et « norme ».

Remarque 9.47.
Si A, B et C sont trois points dans le plan $\mathbb{R}^2$, alors l'inégalité triangulaire $|AB| \leqslant |AC| + |CB|$ est précisément la propriété (3) de la norme (définition 7.106). En effet l'inégalité triangulaire s'exprime de la façon suivante en terme de la norme $\|.\|_2$:

$$\|A - B\|_2 \leqslant \|A - C\|_2 + \|C - B\|_2. \tag{9.66}$$

En notant $u = A - C$ et $v = C - B$, l'équation (9.66) devient exactement la propriété de définition de la norme :

$$\|u + v\|_2 \leqslant \|u\|_2 + \|v\|_2. \tag{9.67}$$

Ceci explique pourquoi cette propriété des normes est appelée « inégalité triangulaire ».

9.5 Espaces métriques

9.5.1 Espaces métrisables

Définition 9.48.
Un espace topologique est ***métrisable*** *s'il est homéomorphe à un espace métrique.*

Proposition 9.49.
Une fonction séquentiellement continue sur un espace métrisable et à valeurs dans un espace métrique est continue.

Démonstration. Soient E un espace métrique et $\phi\colon X \to (E, d)$ un homéomorphisme. Nous supposons que $f\colon X \to Y$ est séquentiellement continue. Nous considérons l'application $\tilde{f} = f \circ \phi^{-1}$, c'est-à-dire

$$\begin{aligned} \tilde{f}\colon E &\to Y \\ a &\mapsto f\big(\phi^{-1}(a)\big). \end{aligned} \tag{9.68}$$

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

$$\tilde{f}(a_k) = f\big(\phi^{-1}(a_k)\big), \tag{9.69}$$

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

$$\lim_{k\to\infty} \tilde{f}(a_k) = \lim_{k\to\infty} f\big(\phi^{-1}(a_k)\big) = f\big(\phi^{-1}(a)\big) = \tilde{f}(a). \tag{9.70}$$

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 9.14. L'application $f = \tilde{f} \circ \phi$ est donc continue en tant que composée d'applications continues. □

9.5.2 Fonctions continues

La propriété suivante donne des caractérisations importantes de la continuité dans le cas des espaces métriques.

Proposition 9.50 (Continuité, ouverts et voisinages et limite[121])**.**
Soient $f\colon E \to F$ 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 $W' = B\big(f(a), \epsilon\big)$, il existe une boule $V' = B(a, \delta)$ telle que $f(V) \subset W$.

(4) $\forall \epsilon > 0$, $\exists \delta > 0$ tel que $f\big(B(a, \delta)\big) \subset B\big(f(a), \epsilon\big)$.

(5) $\lim_{x\to a} f(x) = f(a)$ *où la limite est donnée par la définition 7.62,*

(6) Pour tout $\epsilon > 0$*, il existe* $\delta > 0$ *tel que* $\|x - a\| < \delta$ *implique* $\|f(x) - f(a)\| < \epsilon$*.*

La proposition 9.78 nous montrera que ces équivalences tiennent encore lorsque l'espace a une topologie de semi-normes.

Démonstration. L'équivalence (1) ⇔ (2) est la définition 7.66. L'équivalence (3) ⇔ (4) est une simple paraphrase.

Montrons (2) ⇒ (3). Si $W' = B\big(f(a), \delta\big)$, nous avons un voisinage V de a tel que $f(V) \subset W$. L'ensemble V contenant une boule autour de chacun de ses points [27], il en contient un autour de a : $V' = B(a, \delta) \subset V$. A fortiori nous avons $f(V') \subset W$.

Montrons (3) ⇒ (2). Si W est un ouvert autour de $f(a)$, il contient une boule autour de $f(a)$: $B\big(f(a), \epsilon\big) \subset W$. Il existe donc une boule $V' = B(a, \delta)$ telle que $f(V') \subset B\big(f(a), \epsilon\big) \subset W$.

L'équivalence (1) ⇔ (5) est la définition 7.66 de la continuité en un point couplée à l'unicité de la limite due à la proposition 7.65 parce qu'un espace métrique est séparé.

Prouvons (5) ⇒ (6). Soient $\epsilon > 0$ et $V = B\big(f(a), \epsilon\big)$. Étant donné que $f(a)$ est une limite de f pour $x \to a$, 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 $x \in B(x, \delta) \subset W$ et donc $f(x) \in B\big(f(a), \epsilon\big)$, c'est-à-dire $\|f(a)-f(x)\| < \epsilon$.

Enfin l'implication (2) ⇒ (5) est une réécriture de la définition de la limite en un point. □

Voici un théorème qui parle de fermés emboîtés dans un espace métrique. Le corollaire 7.53 parle du cas $\cap_i A_i = \varnothing$ dans un compact.

Théorème 9.51 (Théorème des fermés emboîtés[122])**.**
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 emboités. 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 $N \geqslant n$, la queue de suite $(x_n)_{n\geqslant N}$ 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 a un point.

Condition nécessaire Soit (x_n) un suite de Cauchy. Nous considérons les ensembles

$$F_n = \overline{\{x_i \text{ tel que } i \geqslant n\}}. \tag{9.71}$$

Le fait que la suite soit de Cauchy implique que $\operatorname{diam}(F_n) \to 0$. Par hypothèse, nous avons alors

$$\bigcap_{n\in\mathbb{N}} F_n = \{a\}. \tag{9.72}$$

Pour s'assurer que a est bien la limite de (x_n), il suffit de remarquer que

$$d(x_n, a) \leqslant \operatorname{diam} F_n \to 0. \tag{9.73}$$

□

Proposition 9.52.
Soient (X, d) *un espace topologique métrique et* F *un fermé de* X*. Nous avons* $d(x, F) = 0$ *si et seulement si* $x \in F$*.*

27. Cela est le théorème-définition 7.88 des ouverts dans un espace métrique, à ne pas confondre avec le théorème 7.4.

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 $d(x_\epsilon, x) \leqslant \psi$. 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 $\lim_{k\to\infty} x_k = x$ par la proposition 9.26(1).

Par la caractérisation séquentielle des fermés (un fermé contient les limites de toutes ses suites, proposition 9.11), la suite (x_k) étant dans F, la limite est dans F. Donc $x \in F$. □

Lemme 9.53.
Soit A_n une suite décroissante de fermés dans un espace métrique[28] *compact K. Alors*

$$C = \bigcap_{n\in\mathbb{N}} A_n \tag{9.74}$$

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 7.59), 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 7.97. Une queue de la suite y_n est dans A_2 et nous considérons donc une sous-suite convergente dans A_2 donnée par

$$z_n = y_{\sigma_2(n)} = x_{\sigma_1\sigma_2(n)}. \tag{9.75}$$

En continuant ainsi nous construisons une suite convergente dans A_k. Nous considérons enfin la suite

$$y_n = x_{\sigma_1\ldots\sigma_n(n)}. \tag{9.76}$$

Pour tout k, une queue de cette suite est une sous-suite de $x_{\sigma_1\ldots\sigma_k(n)}$ et par conséquent cette suite converge dans A_k. La limite de cette suite est donc dans l'intersection demandée. □

Remarque 9.54.
Cette propriété est fausse pour les ouverts. Par exemple

$$\bigcap_{n>1}]0, \frac{1}{n}[= \varnothing. \tag{9.77}$$

Lemme 9.55.
Si K est un compact dans un espace métrique et F un fermé disjoint de K, alors $d(K,F) > 0$.

Démonstration. Le fonction

$$\begin{aligned} K &\to \mathbb{R} \\ x &\mapsto d(x,F) \end{aligned} \tag{9.78}$$

est une fonction continue sur K, et donc atteint son minimum par le théorème de Weierstrass 7.99. 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. □

Proposition 9.56 ([107])**.**
Une isométrie d'un espace métrique compact sur lui-même est une bijection.

Démonstration. Soient X un espace métrique compact et $f\colon X \to X$ 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 9.55 appliqué au fermé $\{x\}$ et au compact $f(K)$ donne un $r > 0$ tel que

$$d\big(x, f(K)\big) > r. \tag{9.79}$$

28. L'hypothèse métrique provient de l'utilisation de Bolzano-Weierstrass, lequel est vrai pour les espaces séquentiellement compacts, dont les espaces métriques.

Soit la suite $u_n = f^n(x)$; c'est une suite dans K et possède donc une sous-suite convergente (Bolzano-Weierstrass7.97) que l'on nomme (y_n). Vu que f est une isométrie,

$$d(y_n, y_{n+1}) = d(x, y_m) > r \tag{9.80}$$

pour un certain $m \leqslant n+1$. 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. □

Proposition 9.57.
Soient (X, d) un espace métrique compact et (u_n) une suite de X telle que

$$\lim_{n\to\infty} d(u_n, u_{n+1}) = 0. \tag{9.81}$$

Alors l'ensemble des points d'accumulation[29] *de (u_n) est connexe.*

Démonstration. Nous notons Γ l'ensemble des points d'accumulation de la suite.

Γ est compact Nous notons $A_p = \{u_n \text{ tel que } n \geqslant p\}$ et nous avons

$$\Gamma = \bigcap_{p\in\mathbb{N}} \overline{A_p} \tag{9.82}$$

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 7.3). En tant que fermé dans un compact, Γ est compact (lemme 7.59).

Recouvrement par deux compacts Supposons que Γ ne soit[30] pas connexe. Nous pouvons alors considérer S et O, deux ouverts disjoints recouvrant Γ et intersectant tout deux Γ. Nous posons alors

$$A = S \cap \Gamma \tag{9.83a}$$
$$B = O \cap \Gamma, \tag{9.83b}$$

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[31].

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 9.55. Nous notons

$$A' = \{x \in X \text{ tel que } d(x, A) < \frac{\alpha}{3}\} \tag{9.84a}$$
$$B' = \{x \in X \text{ tel que } d(x, B) < \frac{\alpha}{3}\} \tag{9.84b}$$

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

$$K = X \backslash (A' \cup B') \tag{9.85}$$

qui est fermé en tant que complémentaire d'ouvert, et donc compact. Étant donné que $A \subset A'$ et $B \subset B'$, nous avons $K \cap \Gamma = \varnothing$.

L'idée est maintenant de montrer que K contient un point d'accumulation de (u_n).

29. Définition 7.22.
30. est-ce qu'il faut vraiment un subjonctif ici ?
31. Lemme 7.59.

Sous-suites de (u_n) L'hypothèse sur la suite (u_n) nous indique qu'il existe un N_0 tel que $\forall n \geqslant N_0$,

$$d(u_n, u_{n+1}) < \frac{\alpha}{3}. \tag{9.86}$$

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 $B' \cap A' = \varnothing$, mais n_0 n'est pas n_2 lui-même parce que $d(A', B') \geqslant \frac{\alpha}{3}$ 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 (9.86) 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

$$\begin{aligned} d(u_{n_0}, B) &\geqslant d(u_{n_0-1}, B) - d(u_{n_0-1}, u_{n0}) \\ &\geqslant d(A, B) - d(u_{n_0-1}, A) - d(u_{n_0-1}, u_{n_0}) \\ &\geqslant \alpha - \frac{\alpha}{3} - \frac{\alpha}{3} \\ &= \frac{\alpha}{3}. \end{aligned} \tag{9.87}$$

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 $N \geqslant N_0$, il existe un $n_0 \geqslant N$ 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 9.58.
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. □

Lemme-définition 9.59.
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

$$V_n = \{z \in E \text{ tel que } |z|\} \cup \bigcup_{a\notin\Omega} B(a, \frac{1}{n}), \tag{9.88}$$

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 $d(z, \complement\Omega) \geqslant \frac{1}{n}$. Du coup si nous prenons δ tel que

$$\frac{1}{n+1} < \delta < \frac{1}{n} \tag{9.89}$$

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 $K_n \to \mathbb{R}$ 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

$$\Omega = \bigcup_{n=0}^{\infty} K_n \subset \bigcup_{n=0}^{\infty} \text{Int}(K_{n+1}) \subset \bigcup_{n=0}^{\infty} \text{Int}(K_n). \tag{9.90}$$

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

$$K \subset \bigcup_{n=0}^{\infty} \text{Int}(K_n). \tag{9.91}$$

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

$$\frac{1}{n+1} < \delta_n < \frac{1}{n}. \tag{9.92}$$

Théorème 9.60 (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 9.66.

9.5.3 Ensembles enchaînés

Soit (x, d) un espace métrique.

Définition 9.61.
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 $0 \leqslant i \leqslant n-1$ nous avons $d(u_n, u_{n+1}) \leqslant \epsilon$.*

Une partie A de X est ***bien enchaînée*** *si pour tout $\epsilon > 0$ et pour tout $a, b \in A$, il existe une ϵ-chaîne joignant a et b dans A.*

Les rationnels dans $\mathbb{R}$ sont bien enchaînés.

Proposition 9.62.
Un espace connexe est bien enchaîné.

Proposition 9.63.
La fermeture d'un ensemble bien enchaîné dans un espace métrique compact (X, d) est connexe.

Démonstration. Soit $A \subset X$ un ensemble bien enchaîné, 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 $\lim_{k\to\infty} d(u_k, u_{k+1}) = 0$. Par conséquent la proposition 9.57 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

$$\bigcup_{x \in \bar{A}} C_{a,x} = \bar{A}. \tag{9.93}$$

Vu que le membre de gauche est une union de connexes, c'est un connexe par la proposition 7.41. □

Corollaire 9.64.
Un espace métrique compact est connexe si et seulement s'il est bien enchaîné.

9.5.4 Produit fini d'espaces métriques

Définition 9.65.
Si $(E_1, d_1), \dots, (E_n, d_n)$ sont des espaces métriques nous mettons la distance suivante sur le produit cartésien $E = E_1 \times \dots \times E_n$:

$$d(x, y) = \max_{i=1,\dots,n} d_i(x_i, y_i). \tag{9.94}$$

Théorème 9.66 ([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 (9.65) (attention : chacun des K_i peut être de dimension infinie) :

$$d(\alpha, \beta) = \max\{d_i(\alpha_i, \beta_i)\} \tag{9.95}$$

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 7.97). 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 $k = 1, \ldots, n$, il existe $N_k > 0$ tel que si $p > N_k$ alors

$$d\big((\alpha_p)_k - \ell_p\big) \leqslant \epsilon. \tag{9.96}$$

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

$$d\big(\alpha_n, (\ell_1, \ldots, \ell_n)\big) \leqslant \epsilon. \tag{9.97}$$

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

$$\mathcal{P}_i = \mathcal{O}_i \times K_2 \times \ldots \times K_n, \tag{9.98}$$

qui est un recouvrement de K par des ouverts (de K) d'où aucun sous-recouvrement fini ne peut être extrait. □

Pour la culture générale, il y a bien entendu moyen de faire des produits dénombrables et pire d'espaces métriques.

Définition 9.67 ([123]).
Soient (E_n, d_n) des espaces métriques. Sur l'ensemble produit $E = \prod_{i=1}^{\infty} E_i$ nous définissons la métrique

$$d(x, y) = \sum_{k=1}^{\infty} \frac{1}{2^k} d'_k(x_i, y_i) \tag{9.99}$$

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 9.68 (Tykhonov dénombrable[123]).
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 9.60.

9.5.5 Équicontinuité

Définition 9.69 ([124]).
*Soit une famille de fonctions $f_i \colon X \to E$ 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*

$$\|f_i(x) - f_i(y)\| < \epsilon \tag{9.100}$$

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 pout.

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 13.335.

Proposition 9.70 ([1, 124]).
Soit une suite équicontinue (f_i) de fonctions qui converge simplement vers f, alors f est continue.

Démonstration. Soit une suite équicontinue $f_i\colon X \to E$ 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

$$|f(x) - f(a)| \leqslant |f(x) - f_i(x)| + |f_i(x) - f_i(a)| + |f_i(a) - f(a)|. \tag{9.101a}$$

Plusieurs majorations.

— Vu que $f_i \to f$, 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 $|f_i(x) - f_i(a)| \leqslant \epsilon$.

— Vu que $f_i \to f$, 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

$$|f(x) - f(a)| \leqslant 3\epsilon. \tag{9.102}$$

□

9.5.6 Continuité uniforme

Définition 9.71 ([125])**.**
Soient deux espaces métriques (E, d) et (E', d'). Une application $f\colon E \to E'$ est ***uniformément continue*** *si pour tout $\epsilon > 0$, il existe $\delta > 0$ tel que $d(x, y) \leqslant \delta$ implique $d'\big(f(x), f(y)\big) \leqslant \epsilon$.*

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.

9.6 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 9.8 sur les espaces de Baire.

Définition 9.72.
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 9.73 (Baire[126])**.**
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

$$B(x_1, r_1) \cap A_1 = \varnothing. \tag{9.103}$$

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 $B(x_2, r_2) \cap A_2 = \varnothing$. Notons que $B(x_2, r_2) \cap A_1 = \varnothing$ aussi, par construction.

Par récurrence nous construisons une suite d'éléments x_n et de rayons $r_n < \epsilon/2^n$ tels que

(1) $B(x_n, r_n) \cap A_j = \varnothing$ pour tout $j \leqslant n$,

(2) $\overline{B(x_n, r_n)} \subset B(x_{n-1}, r_{r-1})$.

Cette suite étant de Cauchy (parce que contenue dans des intervalles emboîtés de rayon décroissant vers zéro), elle converge[32] 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. □

32. Par la proposition 1.79

9.7 Topologie des semi-normes

Les principaux espaces topologiques construit avec des semi-normes seront les espaces de fonctions de la définition 31.10. Nous verrons également la topologie $*$-faible sur $\mathscr{D}'(\Omega)$ en la définition 31.17.

Définition 9.74.
*Si E est un espace vectoriel, une **semi-norme** sur E est une application $p\colon E \to \mathbb{R}$ telle que*

(1) $p(x) \geqslant 0$,

(2) $p(\lambda x) = |\lambda| p(x)$

(3) $p(x+y) \leqslant p(x) + p(y)$.

La seule différence avec une norme est simplement qu'une semi-norme peut s'annuler en des éléments non-nuls de l'espace.

Lemme 9.75 ([127])**.**
Si p est une semi-norme nous avons

$$|p(x) - p(y)| \leqslant p(x-y). \tag{9.104}$$

Démonstration. Nous avons d'une part $p(x+h) \leqslant p(x) + p(h)$ et d'autre part $p(x) \leqslant p(x+h) + p(-h) = p(x+h) + p(h)$. En isolant $p(x+h) - p(x)$ dans chacune ce des deux inégalités,

$$-p(h) \leqslant p(x+h) - p(x) \leqslant p(h) \tag{9.105}$$

ou encore

$$|p(x+h) - p(x)| \leqslant p(h) \tag{9.106}$$

qui donne le résultat demandé en posant $h = y - x$. □

Soit $(p_i)_{i\in I}$ une famille de semi-normes sur E. Nous construisons alors une topologie sur E de la façon suivante.

Définition 9.76 (Topologie et semi-normes[128, 129])**.**
*Pour tout J fini dans I nous définissons les **boules ouvertes***

$$B_J(x,r) = \{y \in E \text{ tel que } p_j(y-x) < r \; \forall j \in J\}. \tag{9.107}$$

*La **topologie** sur E donnée par la famille de semi-norme 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 9.77.
Une suite (x_n) dans E converge vers x au sens de la topologie des semi-normes si et seulement si pour tout $i \in I$,

$$p_i(x - x_n) \to 0. \tag{9.108}$$

Démonstration. Si la suite (x_n) converge[33] vers x, alors pour tout ouvert $\mathcal{O}$ autour de x, il existe un N tel que si $n \geqslant N$, alors $x_n \in \mathcal{O}$. En particulier pour tout j et pour tout $\epsilon > 0$, il doit exister un $n \geqslant N_j$ 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 $n \geqslant N_i$ implique $p_i(x - x_n) \leqslant \epsilon$. 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 $p_j(x - x_n) \leqslant \epsilon$ pour tout j et donc $x_n \in B_J(x,r)$. □

La proposition suivante est un vulgaire plagiat de la proposition 9.50.

33. Définition 7.25.

Proposition 9.78.
Soit $f\colon \mathbb{R} \to (E, p_i)_{i\in I}$ 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 $f(V) \subset W$,

(3) pour tout $i \in I$ et $\epsilon > 0$ il existe $\delta > 0$ tel que

$$f\big(B(t_0, \delta)\big) \subset B_i\big(f(t_0), \epsilon\big). \tag{9.109}$$

Démonstration. L'équivalence (1) ⇔ (2) est la définition 7.66.

Prouvons (2) ⇒ (3). Soient $i \in I$ et $\epsilon > 0$. Considérons la boule $B_i\big(f(t_0), \epsilon\big)$, qui est un ouvert de E contenant $f(t_0)$. Il existe donc un ouvert V autour de t_0 tel que $f(V) \subset B_i\big(f(t_0), \epsilon\big)$. En particulier V contient une boule $B(t_0, \delta)$ et nous avons

$$f\big(B(t_0, \delta)\big) \subset f(V) \subset B_i\big(f(t_0), \epsilon\big). \tag{9.110}$$

Prouvons (3) ⇒ (2). Soit W un ouvert autour de $f(t_0)$. Il existe un $i \in I$ et $\epsilon > 0$ tel que $B_i\big(f(t_0), \epsilon\big) \subset W$. Nous avons alors un $\delta > 0$ tel que

$$f\big(B(t_0, \delta)\big) \subset B_i\big(f(t_0), \epsilon\big) \subset W. \tag{9.111}$$

□

Lorsqu'on a un espace E muni d'une quantité dénombrable de semi-normes $\{p_k\}_{k\in I}$ nous définissons l'écart [34]

$$d(x, y) = \sup_{k\geqslant 1} \min\big\{\frac{1}{k}, p_k(x - y)\big\}. \tag{9.112}$$

Notons que cette écart est invariant par translation au sens où pour tout x, y, h dans E nous avons

$$d(x + h, y + h) = \sup_{k\geqslant 1} \min\big\{\frac{1}{k}, p_k(x - y)\big\} = d(x, y). \tag{9.113}$$

Proposition 9.79.
Si X est un espace topologique dont la topologie est donnée par une famille dénombrable de semi-normes, alors il est métrisable.

Proposition 9.80 ([127])**.**
La topologie donnée par les boules

$$B_k(a, r) = \{x \in E \text{ tel que } \forall\, k \leqslant \frac{1}{r}, p_k(x - a) < r\} \tag{9.114}$$

est la même que celle « usuelle » donnée par les semi-normes. 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 (9.114) et par P celle des semi-normes : P-continue, d-ouvert, etc.

D'abord nous avons

$$B(a, r) = \bigcap_{k\leqslant \frac{1}{k}} B_k(a, r). \tag{9.115}$$

Si $\mathcal{O}$ est un d-ouvert, il contient une d-boule autour de chacun de ses points. Or d'après la formule (9.115), 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.

34. Dans le cas de $E = \mathscr{D}(K)$, la première semi-norme est numérotée à zéro, donc il faudra poser $d(\varphi_1, \varphi_2)$ avec p_{k-1} au lieu de p_k.

Inversement nous supposons que $\mathcal{O}$ est un P-ouvert. Commençons par prouver que les semi-normes p_k sont d-continues. En effet soient $k \in \mathbb{N}$, $\epsilon \leqslant \frac{1}{k}$ et $x, y \in E$ tels que $d(x,y) \leqslant \epsilon$; nous avons

$$\begin{aligned} |p_k(y) - p_k(x)| &\leqslant p_k(x-y) && \text{(9.116a)}\\ &= \min\{\frac{1}{k}, p_k(x-y)\} && \text{(9.116b)}\\ &\leqslant d(x,y) && \text{(9.116c)}\\ &\leqslant \epsilon. && \text{(9.116d)} \end{aligned}$$

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 inclue à $B_k(a,r)$. Pour cela prenons $y \in B(x,\epsilon)$; nous avons

$$\big|p_k(a-x) - p_k(a-y)\big| \leqslant d(x,y) \leqslant \epsilon. \tag{9.117}$$

Par conséquent le nombre $p_k(a-y)$ est dans l'intervalle

$$p_k(a-x) \pm \epsilon \tag{9.118}$$

et il suffit de prendre $\epsilon < \frac{r - p_k(a-x)}{2}$. □

9.7.1 Espace dual

Nous parlerons plus en détail d'espace dual d'un espace normé en la section 12.11.

Définition 9.81.
Soient F un espace métrique et E un espace topologique vectoriel. Une topologie possible[35] *sur l'espace des applications linéaires $\mathcal{L}(E,F)$ est la* ***topologie $*$-faible*** *qui est la topologie des semi-normes*

$$p_v(T) = \|T(v)\|_F. \tag{9.119}$$

C'est une famille de semi-normes 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 $E \to \mathbb{R}$.

La proposition suivante indique qu'elle est un peu la topologie de la convergence ponctuelle.

Proposition 9.82.
Soient E un espace muni de la topologie des semi-normes $\{p_i\}_{i\in I}$ 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 :

$$\begin{aligned} T_n &\xrightarrow{*} T && && \text{(9.120a)}\\ p_v(T_n - T) &\to 0 \ \forall v \in E && \text{proposition 9.77} && \text{(9.120b)}\\ \|T_n(v) - T(v)\|_E &\to 0 \ \forall v \in E && && \text{(9.120c)}\\ T_n(v) &\xrightarrow{E} T(v). && && \text{(9.120d)} \end{aligned}$$

□

35. C'est, dans l'idée, celle qui sera choisie pour les espaces de distributions, voir la définition 31.17.

9.7.2 Espace $C^k(\mathbb{R}, E')$

Nous revenons à nos histoires de limites de la définition 7.25.

Proposition 9.83 (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 9.81. Il y a unicité de l'élément de E' vers lequel une fonction $u\colon \mathbb{R} \to E'$ peut converger.

Démonstration. Soit T un élément vers lequel u_t converge lorsque $t \to t_0$. 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 $|t - t_0| \leqslant \delta$. Nous avons donc, pour tout $x \in E$, la limite (dans $\mathbb{R}$) :

$$\lim_{t \to t_0} u_t(x) = T(x). \tag{9.121}$$

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

$$\lim_{t \to t_0} u_t(x) = T'(x). \tag{9.122}$$

Par unicité de la limite dans $\mathbb{R}$ nous devons alors avoir $T(x) = T'(x)$ pour tout x, c'est-à-dire $T = T'$. □

Proposition 9.84.
Soit $u\colon \mathbb{R} \to E'$ 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 $\mathbb{R}$

$$\lim_{t \to t_0} u_t(x) = u_{t_0}(x), \tag{9.123}$$

(3) nous avons la limite dans E'

$$\lim_{t \to t_0} u_t = u_{t_0}. \tag{9.124}$$

Démonstration. Soient $x \in E$ et $\epsilon > 0$. Par la proposition 9.78 la continuité de u donne un $\delta > 0$ tel que

$$u_{B(t_0,\delta)} \subset B_x(u_{t_0}, \epsilon). \tag{9.125}$$

C'est-à-dire que si $|t - t_0| \leqslant \delta$ nous avons

$$\big|u_{t_0}(x) - u_t(x)\big| < \epsilon, \tag{9.126}$$

ce qui signifie bien que la fonction $t \mapsto u_t(x)$ est continue en tant que fonction $\mathbb{R} \to \mathbb{R}$. Cela est le point (1). Le théorème de limite et continuité dans $\mathbb{R}$ nous donne immédiatement la limite (9.123).

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

$$u_{B(t_0,\delta)} \subset B_i(u_{t_0}, \epsilon) \subset \mathcal{O}. \tag{9.127}$$

Cela signifie bien que

$$|t - t_0| \leqslant \delta \Rightarrow u_t \in \mathcal{O}, \tag{9.128}$$

c'est-à-dire que nous avons la limite $\lim_{t \to t_0} u_t = u_{t_0}$ dans E'. Pour dire cela nous avons utilisé la définition 7.62 de la limite et le résultat d'unicité 9.83. □

Définition 9.85.
*Si nous avons une application $u\colon \mathbb{R} \to E'$ nous considérons sa **dérivée** donnée par la limite*

$$u'_{t_0} = \lim_{t \to t_0} \frac{u_t - u_{t_0}}{t - t_0}. \tag{9.129}$$

Cela est un nouvel élément de E' (pour peu que la limite existe). La fonction $u'\colon \mathbb{R} \to E'$ 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 31.5.

9.8 Espaces de Baire

Définition 9.86.
*Un **espace de Baire** est un espace topologique dans lequel toute intersection dénombrable d'ouverts denses est dense.*

Théorème 9.87 (Théorème de Baire[130])**.**
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 emboités B_n telle que

$$\bigcap_{n\in\mathbb{N}} U_n \cap V \tag{9.130}$$

contient l'intersection des B_n. Par le théorème 9.51 des fermés emboîtés (que nous utilisons parce que E est métrique et complet), cette intersection est non vide.

Ouvert d'un espace de Baire

□

Une des applications du théorème de Baire est le théorème de Banach-Steinhaus 12.92.

Chapitre 10

Espaces affines

Définition 10.1.
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 librement*[1]*.*

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.

10.2.
Lorsque nous écrivons « $M + x$ », le symbole plus n'est pas une loi de composition interne de $\mathcal{E}$, mais une action.

Soient $N, M \in \mathcal{E}$. Par liberté et transitivité de l'action, il existe un unique $x \in E$ tel que $M + x = N$. Ce vecteur x sera noté $\overrightarrow{MN}$.

Proposition 10.3.
Si $A, B, C \in \mathcal{E}$ nous avons les égalités suivantes dans E :

(1) $\overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$ *(relations de Chasles),*

(2) $\overrightarrow{AA} = 0$,

(3) $\overrightarrow{BA} = -\overrightarrow{AB}$.

10.4.
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 $\mathbb{K}^n$.

10.1 Repères cartésiens affines

Soit E un $\mathbb{K}$-espace vectoriel de dimension n et $\mathcal{E}$ un espace affine construit sur E.

Définition 10.5.
Un multiplet $(A, e_1, \ldots, e_n)$ 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.*

1. Définition 2.59.

Proposition 10.6.
Si $\mathcal{E}$ est un espace affine modelé sur l'espace vectoriel E de dimension n sur le corps $\mathbb{K}$, et si $\big(A, \{e_i\}_{i=1,\dots,n}\big)$ est un repère cartésien, alors

$$\begin{aligned} \phi\colon \mathbb{K}^n &\to \mathcal{E} \\ (x_1, \dots, x_n) &\mapsto A + \sum_i x_i e_i. \end{aligned} \tag{10.1}$$

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. □

10.2 Classification affine des conique

Soit une conique $f(x, y) = 0$ avec

$$f(x, y) = ax^2 + 2bxy + cy^2 + 2dx + 2ey + f \tag{10.2}$$

dans le repère $R = (A, e_i)$. La signature de la quadratique

$$q(x, y) = ax^2 + 2bx + cy^2 \tag{10.3}$$

ne dépend pas de la base choisie et un changement de variables

$$\begin{cases} \tilde{x} = \alpha x + \beta y & \text{(10.4a)} \\ \tilde{y} = \gamma x + \delta y & \text{(10.4b)} \end{cases}$$

peut nous amener dans trois cas :

$$q(x, y) = \begin{cases} \tilde{x}^2 + \tilde{y}^2 & \text{genre ellipse} \\ \tilde{x}^2 - \tilde{y}^2 & \text{genre hyperbole} \\ \tilde{x}^2 & \text{genre parabole.} \end{cases} \tag{10.5}$$

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

$$\begin{cases} x = x_0 + \tilde{x} & \text{(10.6a)} \\ y = y_0 + \tilde{y}. & \text{(10.6b)} \end{cases}$$

Un peu de calcul montre qu'alors la conique s'écrit

$$f(x_0, y_0) + q(\tilde{x}, \tilde{y}) + (2ax_0 + 2by_0 + 2d)\tilde{x} + (2bx_0 + 2cy_0 + 2e)\tilde{y} = 0. \tag{10.7}$$

Le point I sera un centre de symétrique si les termes linéaires en $\tilde{x}$ et $\tilde{y}$ s'annulent, c'est-à-dire si

$$\begin{cases} ax_0 + by_0 + d = 0 & \text{(10.8a)} \\ bx_0 + cy_0 + e = 0. & \text{(10.8b)} \end{cases}$$

Nous supposons que $(d, e) \neq (0, 0)$, sinon la conique de départ serait déjà centrée. Le déterminant du système (10.8) est

$$\delta = ac - b^2. \tag{10.9}$$

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 10.7
Soit

$$f(x,y) = x^2 + 2xy - y^2 - 6x + 2y - 1 = 0 \tag{10.10}$$

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

$$Q = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{10.11}$$

Son polynôme caractéristique est $\lambda^2 - 2$ sont 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

$$\begin{cases} x_0 + y_0 - 3 = 0 & \text{(10.12a)} \\ x_0 - y_0 + 1 = 0, & \text{(10.12b)} \end{cases}$$

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

$$R' = (I, \{e_i\}) \tag{10.13}$$

avec $I = A + x_0 e_1 + y_0 e_2$ où A est l'origine du repère dans lequel l'équation (10.10) était donnée.

Par construction dans ce repère nous avons la conique

$$f(x_0, y_0) + q(\tilde{x}, \tilde{y}) = 0, \tag{10.14}$$

c'est-à-dire

$$\tilde{x}^2 + 2\tilde{x}\tilde{y} - \tilde{y}^2 = 0. \tag{10.15}$$

Maintenant la nous avons une quadrique centrée nous voulons la mettre sous une forme plus canonique :

$$\left(\frac{1}{\sqrt{2}}(\tilde{x} + \tilde{y})\right)^2 - \tilde{y}^2 - 1 = 0. \tag{10.16}$$

Nous posons donc

$$\begin{cases} X = \frac{1}{\sqrt{2}}(\tilde{x} + \tilde{y}) & \text{(10.17a)} \\ Y = \tilde{y}, & \text{(10.17b)} \end{cases}$$

et nous trouvons l'hyperbole

$$X^2 - Y^2 - 1 = 0. \tag{10.18}$$

Cela revient à faire le changement de base

$$\begin{cases} e'_1 = \sqrt{2}e_1 & \text{(10.19a)} \\ e'_2 = -e_1 + e_2. & \text{(10.19b)} \end{cases}$$

Pour rappel, les vecteurs de bases se transforment avec la matrice inverse des coefficients. Étant donné que

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \tilde{x} \\ \tilde{y} \end{pmatrix}, \tag{10.20}$$

nous avons

$$\begin{pmatrix} e'_1 \\ e'_2 \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} e_1 \\ e_2 \end{pmatrix}. \tag{10.21}$$

C'est de là que provient le changement (10.19). △

10.3 Applications affines

Définition 10.8.
Soient $\mathcal{E}$ et $\mathcal{E}'$ deux espaces affines sur les espaces vectoriels E et E' (sur le même corps $\mathbb{K}$). Une application $f\colon \mathcal{E} \to \mathcal{E}'$ est dite ***affine*** *si pour tout $M \in \mathcal{E}$, il existe une application linéaire $u_M\colon E \to E'$ telle que*

$$f(M+x) = f(M) + u_M(x) \tag{10.22}$$

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 10.56 nous donnera une structure de groupe sur $\mathrm{Aff}(\mathbb{R}^n)$.

Lemme-définition 10.9 ([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 $f\colon \mathcal{E} \to \mathcal{E}'$.

Il existe une unique application linéaire $u\colon E \to E'$ telle que

$$f(M+x) = f(M) + u(x) \tag{10.23}$$

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 $u_1 = u_2$.

$u_M = u_N$ Avant de prouver l'unicité, nous considérons $M, N \in \mathcal{E}$ et les applications linéaires u_M et u_N vérifiant l'équation (10.22) pour M et N respectivement. Prouvons que $u_M = u_N$.
Posons

$$f(M+x) = f(M) + u_M(x) \tag{10.24a}$$
$$f(N+y) = f(N) + u_N(y). \tag{10.24b}$$

Définissons $a \in E$ par $N = M + a$; nous avons d'une part que

$$f(N+y) = f(M+y+a) = f(M) + u_M(y+a), \tag{10.25}$$

et d'autre part

$$f(N+y) = f(M+a) + u_N(y) = f(M) + u_M(a) + u_N(y). \tag{10.26}$$

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

$$f(N+x) = f(M) + u_N(x) = f(M) + u_M(x). \tag{10.27}$$

Donc effectivement u_M peut être utilisé en tout point de $\mathcal{E}$.

□

Ce lemme est important car il permet de démonter qu'une application est affine en prouvant la linéarité des u_M séparément sans devoir prouver qu'elles sont égales.

10.3.1 Autre propriétés

Lemme 10.10 ([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

$$\overrightarrow{AB} = u_f(x_b - x_a). \tag{10.28}$$

Démonstration. En appliquant f à $A = M + x_a$ et $B = M + x_b$,

$$f(A) = f(M) + u_f(x_a) \tag{10.29a}$$
$$f(B) = f(M) + u_f(x_b). \tag{10.29b}$$

Donc $f(B) = f(A) - u_f(x_a) + u_f(x_b)$ ou encore

$$f(B) = f(A) + u_f(x_b - x_a). \tag{10.30}$$

□

Remarque 10.11.
La condition (10.22) pour tout $M \in \mathcal{E}$ est équivalente à demander

$$f \circ t_x = t_{u(x)} \circ f \tag{10.31}$$

pour tout $x \in E$.

Proposition 10.12.
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 10.9. □

Exemple 10.13
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 (10.22), 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 10.14.
Si $f : \mathcal{E} \to \mathcal{E}'$ et $g : \mathcal{E} \to \mathcal{E}''$ sont des applications affines, alors $g \circ f : \mathcal{E} \to \mathcal{E}''$ est affine et $u_{g\circ f} = u_g \circ u_f$.

Démonstration. Si $M \in \mathcal{E}$ et $x \in E$ nous avons

$$\begin{aligned}(g \circ f)(M + x) &= g\big(f(M) + u_f(x)\big) \\ &= f\big(f(M)\big) + u_g\big(u_f(x)\big) \\ &= (g \circ f)(M) + (u_g \circ u_f)(x).\end{aligned} \tag{10.32}$$

□

Théorème 10.15.
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 $f : \mathcal{E} \to \mathcal{E}'$ 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

$$f(x) = b + ax. \tag{10.33}$$

Remarque 10.16.
L'équation (10.33) 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 $(A, \{e_i\})$.

10.4 Isomorphismes

Définition 10.17.
*Un **isomorphisme** entre les espaces affines $\mathcal{E}$ $\mathcal{E}'$ est une application affine $f : \mathcal{E} \to \mathcal{E}'$ inversible dont l'inverse est affine.*

Proposition 10.18.
Une application affine bijective est un isomorphisme. Si f est un isomorphisme d'espaces affines, alors $u_{f^{-1}} = (u_f)^{-1}$.

Proposition 10.19.
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

$$\begin{aligned} \varphi : \mathbb{K}^n &\to \mathcal{E} \\ (x_1, \dots, x_n) &\mapsto A + \sum_i x_i e_i \end{aligned} \tag{10.34}$$

est un isomorphisme. □

10.5 Sous espaces affines

Définition 10.20.
*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

$$F = \{AB \text{ tel que } A, B \in \mathcal{F}\} \tag{10.35}$$

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 10.21.
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 $f : \mathcal{E} \to \mathbb{K}^{n-k}$ 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

$$\begin{aligned} f\colon \mathcal{E} &\to \mathbb{K}^{n-k} \\ A + \sum_{i=1}^{n} x_i e_i &\mapsto \begin{pmatrix} x_{k+1} \\ \vdots \\ x_n \end{pmatrix}. \end{aligned} \tag{10.36}$$

Par construction nous avons $f(M) = 0$ si et seulement si $M \in \mathcal{F}$. □

Proposition 10.22 ([27])**.**
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

$$F = \operatorname{Span}\{\overrightarrow{AM} \text{ tel que } M \in \sigma\}. \tag{10.37}$$

Le sous-espace affine donné par la proposition 10.22 est le sous-espace affine **engendré** par la partie σ, et il est noté $\operatorname{eae}(\sigma)$.

Proposition 10.23.
Soit $\mathcal{E}$ un espace affine de dimension n sur $\mathbb{K}$, soit $f\colon \mathcal{E} \to \mathbb{K}^r$ 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

$$f\big(A + \sum_i x_i e_i\big) = f(A) + u_f\big(\sum_i x_i e_i\big). \tag{10.38}$$

Nous avons donc $f\big(A + \sum_i x_i e_i\big) = a$ lorsque

$$u_f(\sum_i x_i e_i) = a - f(A). \tag{10.39}$$

Nous avons donc

$$f^{-1}(a) = A + (u_f)^{-1}\big(a - f(A)\big), \tag{10.40}$$

dont la dimension est le rang de $(u_f)^{-1} = u_{f^{-1}}$ (proposition 10.18). Le rang de $(u_f)^{-1}$ est le dimension du noyau de u_f. □

Définition 10.24 (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.

Exemple 10.25
Soit un espace vectoriel normé[2] $(V, \|.\|)$. Pour tout $a \in V$ et $r > 0$, la boule $B(a, r)$ est convexe. La boule fermée $\overline{B(a, r)}$ également.

La boule centrée en zéro Soient $x, y \in B(0, r)$ et $\lambda \in]0, 1[$. Alors

$$\|\lambda x + (1-\lambda)y\| \leqslant |\lambda|\|x\| + |1-\lambda|\|y\| < (|\lambda| + |1-\lambda|)r \leqslant r \tag{10.41}$$

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.

2. Définition 7.106.

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

$$\lambda(x-a)+(1-\lambda)(y-a) \in B(0,r) \tag{10.42}$$

par la première partie. En développant et simplifiant,

$$\lambda x+(1-\lambda)y-a \in B(0,r), \tag{10.43}$$

ce qui signifie que $\lambda x+(1-\lambda)y \in B(a,r)$.

△

Proposition 10.26.
Soit A un ensemble convexe[3] *dans un espace vectoriel et $v_1,\dots,v_n$ des éléments de A. Alors toute combinaison*

$$a_1v_1+\cdots+a_nv_n \tag{10.44}$$

telle que $a_1+\cdots+a_n=1$ 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

$$t_2\big(t_1v_1+(1-t_1)v_2\big)+(1-t_2)v_3=av_1+bv_2+cv_3. \tag{10.45}$$

La réponse est immédiatement donnée par

$$t_2a=1-c \tag{10.46a}$$
$$t_1=a/t_2. \tag{10.46b}$$

Étant donné que $c \in [0,1]$ nous avons $t_2 \in [0,1]$. En ce qui concerne t_1 nous avons

$$t_1=\frac{a}{t_2} \leqslant \frac{1-c}{1-c}=1. \tag{10.47}$$

□

10.6 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 10.27 ([131])**.**
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

$$\sum_{i=1}^{r} \lambda_i \overrightarrow{GA_i}=0. \tag{10.48}$$

*Le point G donné par le lemme 10.27 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 10.28 (Combinaison convexe)**.**
*Des nombres $\lambda_1,\dots,\lambda_n$ vérifiant $\sum_i \lambda_i=1$ forment une **combinaison convexe**.*

Le théorème suivant donné quelques caractérisations équivalentes du barycentre.

3. Définition 10.24.

Théorème 10.29 ([131]).
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 $\left(\sum_i \lambda_i\right)\overrightarrow{AG} = \sum_i \lambda_i \overrightarrow{AA_i}$.

(4) Pour tout $B \in \mathcal{E}$, nous avons $\left(\sum_i \lambda_i\right)\overrightarrow{BG} = \sum_i \lambda_i \overrightarrow{BA_i}$.

Définition 10.30.
*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 $(A_i, 1)$.

10.6.1 Sous-espaces affines

Proposition 10.31.
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 10.29 : pour tout $B \in \mathcal{F}$,

$$\overrightarrow{BG} = \sum_i \lambda_i \overrightarrow{BA_i}. \tag{10.49}$$

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

$$F = \{\overrightarrow{AB} \text{ tel que } A, B \in \mathcal{F}\} \tag{10.50}$$

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

$$\overrightarrow{AV} = \overrightarrow{AX} + \overrightarrow{AY}. \tag{10.51}$$

Par les relations de Chasles,

$$\overrightarrow{AV} = \overrightarrow{AV} + \overrightarrow{VX} + \overrightarrow{AV} + \overrightarrow{VY}, \tag{10.52}$$

donc

$$0 = \overrightarrow{VX} - \overrightarrow{VA} + \overrightarrow{VY}, \tag{10.53}$$

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

$$\overrightarrow{AW} = \mu\overrightarrow{AX} = \mu(\overrightarrow{AW} + \overrightarrow{WX}), \tag{10.54}$$

ce qui signifie que

$$(1 - \mu)\overrightarrow{AW} + \mu\overrightarrow{XW} = 0 \tag{10.55}$$

et que W est un barycentre.

Afin de montrer que (10.50) 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

$$\begin{aligned}
\overrightarrow{AX} + \overrightarrow{BY} &= \overrightarrow{AX} + \overrightarrow{BA} + \overrightarrow{AY} && (10.56a)\\
&= \overrightarrow{AV} + \overrightarrow{BA} && V \text{ est celui donné plus haut} \quad (10.56b)\\
&= \overrightarrow{AV} - \overrightarrow{AB} && (10.56c)\\
&= \overrightarrow{AV} + \overrightarrow{AW} && W \text{ est donné par } \mu = -1. \quad (10.56d)\\
&= \overrightarrow{AV'}. && (10.56e)
\end{aligned}$$

□

Proposition 10.32 ([131]).
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

$$G = A_0 + \overrightarrow{A_0G} = A_0 + \sum_{i=1}^{r} \lambda_i \overrightarrow{A_0A_i}. \tag{10.57}$$

Notons que les vecteurs $\overrightarrow{A_0A_i}$ sont dans la direction du sous-espace affine engendré par les A_i par (10.37). Donc G est bien dans $\mathcal{F}$.

Inversement si X est dans $\mathcal{F}$, on a

$$X = A_0 + \sum_i \lambda_i \overrightarrow{A_0A_i} \tag{10.58}$$

parce que $\sum_i \lambda_i \overrightarrow{A_0A_i}$ est un élément général de la direction de $\mathcal{F}$. Du coup

$$\overrightarrow{A_0X} = \sum_i \lambda_i \overrightarrow{A_0A_i}, \tag{10.59}$$

et en utilisant la relation de Chasles sur chacun des $\overrightarrow{A_0A_i}$,

$$\overrightarrow{A_0X} = \sum_i \lambda_i \big(\overrightarrow{A_0X} + \overrightarrow{XA_i}\big). \tag{10.60}$$

De là nous concluons que

$$\big(1 - \sum_i \lambda_i\big)\overrightarrow{A_0X} + \sum_i \lambda_i \overrightarrow{A_iX} = 0, \tag{10.61}$$

ce qui signifie précisément que X est un barycentre des A_i. □

Proposition 10.33.
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 $\mathrm{Aff}\{A_i\}$ est l'espace

$$\mathrm{Span}\{\overrightarrow{A_0A_i}_{i=1,\dots,r}\} \tag{10.62}$$

qui est engendré par r vecteurs et donc est au plus de dimension r. □

En deux mots, la proposition suivante signifie que le barycentre des barycentres est le barycentre.

Proposition 10.34 (Associativité des barycentres[132]).
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 $\lambda_0, \dots, \lambda_m$ 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 $\{(b_k, \mu_k)\}_{k=1,\dots,n}$ 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

$$0 = \sum_{k=0}^{r} \mu_k \overrightarrow{bb_k} \tag{10.63a}$$

$$= \sum_{k} \sum_{i\in J_k} \lambda_i \overrightarrow{bb_k} \tag{10.63b}$$

$$= \sum_{k=0}^{r} \sum_{i\in J_k} \lambda_i (\overrightarrow{ba_i} + \overrightarrow{a_ib_k}) \tag{10.63c}$$

$$= \sum_{k=0}^{r} \sum_{i\in J_k} \lambda_i \overrightarrow{ba_i} + \sum_{k=0}^{r} \underbrace{\sum_{i\in J_k} \lambda_i \overrightarrow{a_ib_k}}_{=0} \tag{10.63d}$$

$$= \sum_{i\in I} \lambda_i \overrightarrow{ba_i}. \tag{10.63e}$$

Donc b est bien barycentre des a_i avec les poids λ_i. □

10.6.2 Enveloppe convexe

Définition 10.35.
*Soit A une partie d'un espace vectoriel E. L'**enveloppe convexe** de A, notée $\mathcal{C}\mathrm{onv}(A)$ est l'intersection de tous les convexes contenant A.*

L'enveloppe convexe est un convexe. En effet soit C un convexe contenant A et $x, y \in \mathcal{C}\mathrm{onv}(A)$; 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 $\mathcal{C}\mathrm{onv}(A)$.

Proposition 10.36 ([133])**.**
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'autre termes, un convexe est stable par barycentrage à poids positifs[4]*.*

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

$$\lambda_1 \overrightarrow{ba_1} + \lambda_2 \overrightarrow{ba_2} = 0. \tag{10.64}$$

Par définition, ce qui est noté $\overrightarrow{ab}$ n'est rien d'autre que $b - a$; en déballant (10.64), nous trouvons

$$\lambda_1(a_1 - b) + \lambda_2(a_2 - b) = 0 \tag{10.65}$$

et donc

$$b = \frac{\lambda_1}{\lambda_1 + \lambda_2} a_1 + \frac{\lambda_2}{\lambda_1 + \lambda_2} a_2, \tag{10.66}$$

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

$$A_r = \{(a_1, \lambda_1), \dots, (a_r, \lambda_r)\} \tag{10.67}$$

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 10.34 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. □

4. Sauf si on prend tous les poids nuls ; mais contre ce genre d'idées, on ne peut rien faire.

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

$$\sum_i \lambda_i x_i = \sum_i \lambda_i g. \tag{10.68}$$

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 $\sum_i \lambda_i = 0$ et avoir le barycentre

$$g = \sum_i \lambda_i x_i. \tag{10.69}$$

Proposition 10.37.
Soit E, un espace vectoriel et $A \subset E$. L'enveloppe convexe $\mathcal{C}\text{onv}(A)$ 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 10.36, ces barycentres sont dans l'enveloppe convexe et donc $\mathcal{B} \subset \mathcal{C}\text{onv}(A)$. A contrario, si nous prouvons que $\mathcal{B}$ était convexe, alors nous aurions $\mathcal{C}\text{onv}(A) \subset \mathcal{B}$ 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

$$a = \sum_i \lambda_i a_i \qquad \sum_{i=1}^{n} \lambda_i = 1 \tag{10.70a}$$

$$b = \sum_j \mu_j b_j \qquad \sum_{j=1}^{n} \mu_j = 1 \tag{10.70b}$$

Un point du segment $[a, b]$ est de la forme $p = ta + (1-t)b$ avec $t \in [0, 1]$. En développant,

$$p = \sum_{i=0}^{n} (t\lambda_i) a_i + \sum_{j=0}^{m} (1-t)\mu_j b_j. \tag{10.71}$$

Cela est le barycentre de la famille $\{(a_i, \lambda_i), (b_j, \mu_j)\}$, parce que la somme des coefficients est bien 1 :

$$\sum_i (t\lambda_i) + \sum_j (1-t)\mu_j = t + (1-t) = 1. \tag{10.72}$$

□

Théorème 10.38 (Carathéodory[43])**.**
Dans un espace affine de dimension n, l'enveloppe convexe[5] *de A est l'ensemble des barycentres à coefficients positifs ou nuls de familles de $n+1$ points.*

Démonstration. Soit $x \in \mathcal{C}\text{onv}(A)$; on sait par la proposition 10.37 que x est barycentre de points de A avec des coefficients positifs :

$$x = \sum_{k=1}^{p} \lambda_k x_k \tag{10.73}$$

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.

5. Définition 10.35.

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

$$\sum_{i=2}^p\alpha_ix_i=\sum_{i=2}^p\alpha_ix_1. \tag{10.74}$$

Nous posons $\alpha_1=-\sum_{i=2}^p\alpha_1$. Remarquons qu'alors $\sum_{i=1}^p\alpha_ix_i=0$ parce que

$$\sum_{i=1}^p\alpha_ix_i=\alpha_1x_1+\sum_{i=2}^p\alpha_ix_i=\alpha_1x_1+\sum_{i=2}^p\alpha_ix_1=\sum_{i=1}^p\alpha_ix_1=0. \tag{10.75}$$

Par conséquent ça ne coûte rien de récrire (10.73) sous la forme

$$x=\sum_{i=1}^p(\lambda_i+t\alpha_i)x_i. \tag{10.76}$$

Les α_i ne sont pas tous nuls, mais leur somme est nulle, donc il y en a au moins un négatif. Nous notons

$$\tau=\min\{-\frac{\lambda_i}{\alpha_i}\text{ tel que }\alpha_i<0\}, \tag{10.77}$$

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 $\mu_i\geqslant 0$, mais si $\alpha_i<0$ alors

$$\lambda_i+\tau\alpha_i\geqslant\lambda_i+(-\frac{\lambda_i}{\alpha_i})\alpha_i=0m \tag{10.78}$$

donc $\mu_i\geqslant 0$ 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

$$\sum_{i\notin J}\mu_ix_i=\sum_{i=1}^p\mu_ix_i=x. \tag{10.79}$$

Et voilà, nous avons écrit x comme un barycentre à coefficients positifs de moins de p éléments parce que J n'est pas vide. □

Corollaire 10.39.
Dans un espace affine de dimension finie, l'enveloppe convexe d'un compact est compacte.

Démonstration. Soit A une partie compacte de l'espace vectoriel E, et $\mathcal{C}\text{onv}(A)$ son enveloppe convexe. Nous allons montrer que toute suite dans $\mathcal{C}\text{onv}(A)$ admet une sous-suite convergente en écrivant un point de $\mathcal{C}\text{onv}(A)$ comme le théorème de Carathéodory 10.38 nous le suggère. Pour cela nous considérons le simplexe

$$\Lambda=\left\{\lambda\in\mathbb{R}^{n+1}\text{ tel que }\sum_{k=1}^{n+1}\lambda_k=1\text{ et }\lambda_k\geqslant 0\forall k\right\}. \tag{10.80}$$

Montrons en passant que Λ est compact. Si $\lambda_k\in\Lambda$ est une suite, alors chacun des λ_k est un $(n+1)$-uple de nombres dans $[0,1]$:

$$k\mapsto(\lambda_k)_i \tag{10.81}$$

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

$$\begin{aligned} f\colon \Lambda \times A^{n+1} &\to \mathcal{C}\text{onv}(A) \\ (\lambda, x) &\mapsto \sum_{k=1}^{n+1} \lambda_k x_k. \end{aligned} \tag{10.82}$$

C'est une application continue parce qu'elle est bilinéaire en dimension finie ; son image est contenue dans $\mathcal{C}\text{onv}(A)$ par la proposition 10.36, et elle est surjective par le théorème de Carathéodory 10.38. Bref, $\mathcal{C}\text{onv}(A) = f(\Lambda \times A^{n+1})$ est donc l'image d'un compact par une application continue ; elle est donc compacte par le théorème 7.86. □

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 du prendre une infinité de sous-suites et rien n'aurait été sûr.

10.6.3 Applications affines et barycentre

Proposition 10.40 ([134]).
Une application $f\colon \mathcal{E} \to \mathcal{E}'$ 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 $\{\big(f(A_i), \lambda_i\big)\}$.

Démonstration. En deux parties.

Si f est affine Par définition d'un barycentre,

$$\sum_i \lambda_i \overrightarrow{GA_i} = 0. \tag{10.83}$$

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 10.10 pour le calcul suivant :

$$\begin{aligned} \sum_i \lambda_i \overrightarrow{g(G)f(A_i)} &= \sum_i \lambda_i u_f(x_i - x_g) && \text{(10.84a)} \\ &= u_f\Big(\sum_i \lambda_i (x_i - x_g)\Big) && \text{(10.84b)} \\ &= u_f\Big(\sum_i \lambda_i \overrightarrow{GA_i}\Big) && \text{(10.84c)} \\ &= u_f(0) = 0. && \text{(10.84d)} \end{aligned}$$

Donc $f(G)$ est bien le barycentre du nouveau système.

Si f conserve les barycentres Nous définissons u par $f(O + x) = f(O) + u(x)$. A 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

$$\overrightarrow{OP} = \alpha \overrightarrow{OM} + \beta \overrightarrow{ON}, \tag{10.85}$$

et $P = O + x_p$. En décomposant $\overrightarrow{MO}$ et $\overrightarrow{NO}$ par les relations de Chasles de la proposition 10.3(1) nous avons

$$(\alpha + \beta - 1)\overrightarrow{PO} - \alpha \overrightarrow{PM} - \beta \overrightarrow{PN} \tag{10.86}$$

et donc P est barycentre du système

$$\big\{(\alpha + \beta - 1, O), (\alpha, M), (\beta, N)\big\}. \tag{10.87}$$

Le point $f(P)$ sera barycentre du système

$$\Big\{\big(\alpha + \beta - A, f(O)\big), \big(\alpha, f(M)\big), \big(\beta, f(N)\big)\Big\}. \tag{10.88}$$

Cela signifie que

$$(\alpha+\beta-1)\overrightarrow{f(P)f(O)}-\alpha\overrightarrow{f(P)f(M)}-\beta\overrightarrow{f(P)f(N)}=0. \tag{10.89}$$

En y substituant $\overrightarrow{f(P)f(O)}=u(-x_p)$, $\overrightarrow{f(P)f(M)}=u(x_m-x_p)$ et $\overrightarrow{f(P)f(N)}=u(x_mm-x_p)$ ainsi que $x_p=\alpha x_m+\beta x_b$ nous trouvons

$$u(\alpha x_m+\beta x_n)=\alpha u(x_m)+\beta u(x_n). \tag{10.90}$$

Donc u est linéaire.

u **ne dépend pas du point** O Il n'est pas besoin de démonter cela parce que la définition 10.8 ne le demande pas. Note : c'est le lemme 10.9 qui dit que c'est par ailleurs vrai.

□

10.7 Repères, coordonnées cartésiennes et barycentriques

Définition 10.41.
*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 10.42 ([131])**.**
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 $\mathrm{Aff}\{A_0,\dots,\hat{A}_i,\dots,A_r\}$.

(3) Les points $A_0,\dots,A_{r-1}$ sont affinement indépendants et $A_r\notin\mathrm{Aff}\{A_0,\dots,A_{r+1}\}$.

(4) Il existe i tel que les vecteurs $\overrightarrow{A_kA_i}$ $(k\in i)$ sont linéairement indépendants.

(5) Pour tout $i\in\{1,\dots,r\}$, les vecteurs $\overrightarrow{A_kA_i}$ $(k\neq i)$ sont linéairement indépendants.

Notons à propos de la condition (3) que l'existence d'un i tel que $A_i\notin\mathrm{Aff}\{A_0,\dots,\hat{A}_i,\dots,A_r\}$ 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 10.43.
*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

$$M=A_0+\overrightarrow{A_0M}. \tag{10.91}$$

Mais nous savons que les vecteurs $\overrightarrow{A_0A_i}$ forment une base de E, nous avons donc des nombres λ_i tels que

$$\overrightarrow{A_0M}=\sum_{i=1}^{n}\lambda_i\overrightarrow{A_0A_i}. \tag{10.92}$$

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

$$M=A_0+\sum_{i=1}^{n}\lambda_i\overrightarrow{A_0A_i}. \tag{10.93}$$

Proposition 10.44 ([1]).
La paire $\big(O, \{e_1, \dots, e_n\}\big)$ 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 10.42, 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 10.42 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

$$A + \sum_i x_i e_i = A' + \sum_i x'_i e'_i. \tag{10.94}$$

Nous considérons les coordonnées (a_i) de A' dans le repère (A, e_i), c'est-à-dire

$$A' = A + \sum_i a_i e_i. \tag{10.95}$$

En substituant $e'_i = \sum_k a_{jk} e_k$ et (10.95) dans (10.94) nous trouvons

$$\sum_k x_k e_k = \sum_k a_k e_k + \sum_{jk} a_{jk} x'_j e_k, \tag{10.96}$$

et par conséquent

$$x_k = a_k + \sum_j a_{jk} x'_j. \tag{10.97}$$

Les coordonnées barycentriques sont données par la proposition suivante.

Proposition 10.45 ([131]).
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 barycentre[6] des A_i affectés de poids λ_i tels que $\sum_{i=0}^r \lambda_i = 1$.

Démonstration. Nous avons vu plus haut (définition 10.43) que l'affine 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 10.32), 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 10.29 avec $B = A_0$:

$$\overrightarrow{A_0M} = \sum_{i=1}^r \lambda_i \overrightarrow{A_0A_i} \tag{10.98}$$

où la somme à droite s'étend a priori de 0 à r, mais comme $\overrightarrow{A_0A_0} = 0$, nous l'avons limitée à 1. Si M s'écrit comme barycentre de deux façons différentes, nous aurions

$$\overrightarrow{A_0M} = \sum_{i=1}^r \lambda_i \overrightarrow{A_0A_i} = \sum_{i=1}^r \mu_i \overrightarrow{A_0A_i} \tag{10.99}$$

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 $\overrightarrow{A_0A_i}$ sont linéairement indépendants (point (5) de la proposition 10.42) et donc $\lambda_i = \mu_i$ pour $i = 1, \dots, r$. La condition de somme des points égale à 1 impose alors immédiatement $\lambda_0 = \mu_0$. □

6. Définition 10.27.

Définition 10.46.
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 10.45 indique qu'il existe un unique choix de λ_i tel que

$$\begin{cases} \sum_i \lambda_i = 1 & \text{(10.100a)} \\ \sum_i \lambda_i \overrightarrow{MA_i} = 0. & \text{(10.100b)} \end{cases}$$

Ces λ_i sont les ***coordonnées barycentriques*** *de M dans le repère $\{A_i\}_{i=1,\dots,n}$.*

10.47.
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

$$\alpha\overrightarrow{XA} + \beta\overrightarrow{XB} + \gamma\overrightarrow{XC} = 0. \tag{10.101}$$

Exemple 10.48
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

$$A + \alpha\overrightarrow{AB} + \beta\overrightarrow{AC}, \tag{10.102}$$

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. △

Exemple 10.49
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

$$\frac{1}{6} + \frac{1}{3} + \frac{1}{2} = 1. \tag{10.103}$$

Ensuite nous cherchons $X \in \mathbb{R}^2$ tel que

$$\frac{1}{6}\overrightarrow{AX} + \frac{1}{3}\overrightarrow{BX} + \frac{1}{2}\overrightarrow{CX} = 0, \tag{10.104}$$

c'est-à-dire

$$\frac{1}{6}\begin{pmatrix} x-3 \\ y-1 \end{pmatrix} + \frac{1}{3}\begin{pmatrix} x+1 \\ y-2 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} x \\ y+1 \end{pmatrix} = 0. \tag{10.105}$$

Nous trouvons immédiatement $x = 1/6$ et $y = 1/3$. Le point cherché est donc le point $\begin{pmatrix} 1/6 \\ 1/3 \end{pmatrix}$. △

Lemme 10.50 ([1]).
Une application affine $f : \mathcal{E} \to \mathcal{E}$ 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 10.44 pour dire que $\big(A_0, \{\overrightarrow{A_0A_i}\}_{i=1,\dots,n}\big)$ est un repère cartésien.

En utilisant la formule du lemme 10.9,

$$f(A_i) = f(A_0 + \overrightarrow{A_0A_i}) = f(A_0) + u(\overrightarrow{A_0A_i}). \tag{10.106}$$

Donc $A_i = A_0 + u(\overrightarrow{A_0A_i})$, ce qui signifie que

$$u(\overrightarrow{A_0A_i}) = \overrightarrow{A_0A_i} \tag{10.107}$$

Par ailleurs, tout point M[7] de $\mathcal{E}$ peut être écrit sous la forme

$$M = A_0 + \sum_i \lambda_i \overrightarrow{A_0A_i}. \tag{10.108}$$

En appliquant M, et en utilisant (10.107),

$$f(M) = f(A_0) + \sum_i \lambda_i u(\overrightarrow{A_0A_i}) = A_0 + \sum_i \lambda_i \overrightarrow{A_0A_i} = M. \tag{10.109}$$

Donc tout point de $\mathcal{E}$ est fixé par f, ce qui signifie que f est l'identité. □

10.7.1 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

$$\begin{cases} x + y + z = 1 & \text{(10.110a)} \\ ax + by + cz = 0 & \text{(10.110b)} \\ a'x + b'y + c'z = 0 & \text{(10.110c)} \end{cases}$$

Donc deux droites affines ont un unique point d'intersection si et seulement si

$$d = \begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a' & b' & c' \end{vmatrix} \neq 0. \tag{10.111}$$

Elles seront parallèles ou confondues si et seulement si $d = 0$.

10.7.2 Associativité, coordonnées barycentriques dans un triangle

Lemme 10.51 ([135]).
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 définition de H et G nous avons

$$\alpha\overrightarrow{HA} + \beta\overrightarrow{HB} = 0 \tag{10.112a}$$
$$\alpha\overrightarrow{GA} + \beta\overrightarrow{GB} + \gamma\overrightarrow{GC} = 0. \tag{10.112b}$$

En utilisant les relations de Chasles nous introduisons H dans la seconde relation :

$$\alpha(\overrightarrow{GH} + \overrightarrow{HA}) + \beta(\overrightarrow{GH} + \overrightarrow{HB}) + \gamma\overrightarrow{GC} = 0 \tag{10.113a}$$
$$(\alpha + \beta)\overrightarrow{GH} + \underbrace{\alpha\overrightarrow{HA} + \beta\overrightarrow{HB}}_{=0} + \gamma\overrightarrow{GC} = 0 \tag{10.113b}$$
$$(\alpha + \beta)\overrightarrow{GH} + \gamma\overrightarrow{GC} = 0. \tag{10.113c}$$

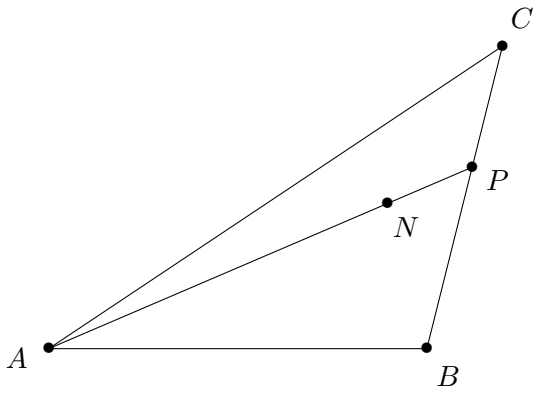
□

7. Même les points qui ne s'appellent pas « M » en fait.

Les coordonnées barycentriques dans un triangle (et plus généralement en fait) permettent de faire des projections.

Proposition 10.52.
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

$$\alpha\overrightarrow{NA} + \beta\overrightarrow{NB} + \gamma\overrightarrow{NC} = 0. \tag{10.114}$$

Nous voudrions montrer que le point P est bien le point de coordonnées $(0, \beta, \gamma)$. Soit donc le point P tel que

$$\beta\overrightarrow{PB} + \gamma\overrightarrow{PC} = 0 \tag{10.115}$$

et montrons que ce point est l'intersection $(BC) \cap (NA)$.

D'abord la relation (10.115) nous dit immédiatement que P est sur la droite (BC). Ensuite, en utilisant les relations de Chasles pour introduire N :

$$\beta(\overrightarrow{PN} + \overrightarrow{NB}) + \gamma(\overrightarrow{PN} + \overrightarrow{NC}) = 0. \tag{10.116}$$

Nous remplaçons $\beta\overrightarrow{NB} + \gamma\overrightarrow{NC}$ par $-\alpha\overrightarrow{NA}$ pour obtenir :

$$(\beta + \gamma)\overrightarrow{PN} - \alpha\overrightarrow{NA} = 0. \tag{10.117}$$

Cela montre que les vecteurs $\overrightarrow{PN}$ et $\overrightarrow{NA}$ sont colinéaires, et donc que P, N et A sont alignés. □

10.8 Applications affines sur $\mathbb{R}^n$

Soit $v \in \mathbb{R}^n$; nous notons $\tau_v \colon \mathbb{R}^n \to \mathbb{R}^n$ 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 10.4.

Lemme 10.53.
Décomposition d'une application affine.

(1) Une application $f \colon E \to E$ 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

$$f(M+x) = f(M) + u_f(x) = (\tau_{f(M)} + u_f)(x) \tag{10.118}$$

pour tout x et M. De plus l'application u_f ne dépend ni de M ni de x (c'est la proposition 10.12(1)). En posant $M = 0$ nous avons :

$$f(x) = (\tau_{f(0)} \circ u_f)(x). \tag{10.119}$$

Dans l'autre sens nous supposons avoir $v \in E$ et α linéaire sur E telles que

$$f(M) = (\tau_v \circ \alpha)(M). \tag{10.120}$$

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 :

$$\begin{aligned} f(M+x) = \tau_v\big(\alpha(M+x)\big) = \alpha(M+x) + v = \alpha(M) + v + \alpha(x) \\ = (\tau_v \circ \alpha)(M) + \alpha(x) = f(M) + \alpha(x). \end{aligned} \tag{10.121}$$

Donc la fonction f vérifie la définition 10.8. 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 surement bijective. □

Corollaire 10.54.
Une application affine qui conserve l'origine est linéaire.

Démonstration. Conserver l'origine demande de poser $v = 0$ dans l'expression du lemme 10.53. □

Proposition 10.55.
Soit une application affine $f : \mathbb{R}^n \to \mathbb{R}^n$. L'ensemble des points fixes

$$\mathrm{Fix}(f) = \{x \in \mathbb{R}^n \text{ tel que } f(x) = x\} \tag{10.122}$$

est soit vide soit un sous-espaces affine de $\mathbb{R}^n$.

Démonstration. Soit $f = \tau_v \circ \alpha$; nous avons $x \in \mathrm{Fix}(f)$ si et seulement si

$$x = \tau_v\big(\alpha(x)\big) = \alpha(x) + v, \tag{10.123}$$

autrement dit, en considérant l'application linéaire $\beta = \mathrm{Id} - \alpha$, si et seulement si $\beta(x) = v$. Nous écrivons $\mathrm{Fix}(f) = \beta^{-1}(v)$. Supposons que ce soit non vide et considérons $x_0 \in \beta^{-1}(v)$. Nous avons

$$\begin{aligned} \beta^{-1}(v) &= \{x \in \mathbb{R}^n \text{ tel que } \beta(x) = \beta(x_0)\} && \text{(10.124a)} \\ &= \{x \text{ tel que } \beta(x - x_0) = 0\} && \text{(10.124b)} \\ &= \{x \text{ tel que } x - x_0 \in \ker(\beta)\} && \text{(10.124c)} \\ &= \ker(\beta) + x_0 && \text{(10.124d)} \\ &= \tau_{x_0}\big(\ker(\beta)\big). && \text{(10.124e)} \end{aligned}$$

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. □

10.8.1 Structure de groupe pour les applications affines

Proposition-définition 10.56 ([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

$$(\tau_v \circ \alpha)(\tau_w \circ \beta) = \tau_{\alpha(w)+v} \circ \alpha\beta. \tag{10.125}$$

(3) L'inverse est donné par

$$(\tau_v \circ \alpha)^{-1} = \tau_{-\alpha^{-1}(v)} \circ \alpha^{-1}. \tag{10.126}$$

Ce groupe est noté $\mathrm{Aff}(\mathbb{R}^n)$.

Démonstration. Pour l'identité, oui, composer par l'identité est neutre.

Le fait que la formule (10.125) soit vraie est un simple calcul :

$$(\tau_v \circ \alpha) \circ (\tau_w \circ \beta)(x) = (\alpha\beta)(x) + \alpha(w) + v = \big(\tau_{\alpha(w)+v} \circ \alpha\beta\big)x. \tag{10.127}$$

Le fait que la formule (10.125) donne bien un produit pour tous les éléments de $\mathrm{Aff}(\mathbb{R}^n)$ est le lemme 10.53.

En ce qui concerne l'inverse, c'est un calcul :

$$\begin{aligned}(\tau_{-\alpha^{-1}(v)}\alpha^{-1})(\tau_v\alpha)(x) &= (\tau_{-\alpha^{-1}(v)\alpha^{-1}})\big(\alpha(x)+v\big) && \text{(10.128a)}\\ &= \tau_{-\alpha^{-1}(v)}\big(x+\alpha^{-1}(v)\big) && \text{(10.128b)}\\ &= x. && \text{(10.128c)}\end{aligned}$$

□

Si $f\colon \mathbb{R}^n \to \mathbb{R}^n$ est une application affine, la proposition 10.53 affirme qu'il existe une application linéaire u telle que

$$f(x+y) = f(x) + u(y). \tag{10.129}$$

En écrivant cela pour $x = 0$,

$$f(y) = f(0) + u(y), \tag{10.130}$$

ou encore $f = \tau_{f(0)} \circ u$.

Proposition 10.57.
L'ensemble $\mathrm{Aff}(\mathbb{R}^n)$ *est isomorphe au produit semi-direct*[8]

$$\mathrm{Aff}(\mathbb{R}^n) \simeq T(n) \times_{\boldsymbol{Ad}} \mathrm{GL}(n,\mathbb{R}) \tag{10.131}$$

où ***Ad*** *est l'action adjointe, c'est-à-dire*

$$\begin{aligned}\boldsymbol{Ad}\colon \mathrm{GL}(n,\mathbb{R}) &\to \mathrm{Aut}\big(T(n)\big)\\ \alpha &\mapsto \big(\tau_v \mapsto \alpha \circ \tau_v \circ \alpha^{-1}\big).\end{aligned} \tag{10.132}$$

Démonstration. L'application que nous allons montrer être un isomorphisme est ψ qui à $f = \tau_v \circ \alpha$ fait correspondre le couple $(\tau_v, \alpha) \in T(n) \times \mathrm{GL}(n,\mathbb{R})$.

Égalité d'ensembles Il faut que $\mathrm{Aff}(\mathbb{R}^n)$ soit en bijection avec $T(n) \times \mathrm{GL}(n,\mathbb{R})$. En effet si $f \in \mathrm{Aff}(\mathbb{R}^n)$, la décomposition $f = \tau_v \circ \alpha$ est unique. D'abord en appliquant à 0, $f(0) = \tau_v\big(\alpha(v)\big) = v$. Donc v est fixé par la valeur de $f(0)$. Ensuite $\alpha = f \circ \tau_v^{-1}$, donc α fixé.

8. Définition 2.76.

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

$$\alpha\tau_v\alpha^{-1}(x) = \alpha\big(\alpha^{-1}(x) + v\big) = x + \alpha(v) = \tau_{\alpha(v)}(x). \tag{10.133}$$

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 $\mathrm{Aff}(\mathbb{R}^n)$ est donnée par

$$(\tau_v \circ \alpha) \circ (\tau_w \circ \beta) = \tau_{v+\alpha(w)} \circ (\alpha \circ \beta). \tag{10.134}$$

Ensuite le loi de groupe de le produit semi-direct est donnée par

$$(\tau_v, \alpha) \cdot (\tau_w, \beta) = \big(\tau_v \mathbf{Ad}(\alpha)\tau_w, \alpha\beta\big) = \big(\tau_v\tau_{\alpha(w)}, \alpha\beta\big) = \big(\tau_{\alpha(w)+v}, \alpha\beta\big). \tag{10.135}$$

Nous avons donc bien

$$\psi\big((\tau_v, \beta) \cdot (\tau_w, \beta)\big) = \psi(\tau_v, \beta) \circ \psi(\tau_w, \beta). \tag{10.136}$$

□

10.9 Isométries

Définition 10.58 (Isométrie d'espace affine)**.**
Si $\mathcal{E}$ est un espace affine muni d'une distance d, une isométrie de $\mathcal{E}$ est une application $f : \mathcal{E} \to \mathcal{E}$ préservant d.

Notons que toutes les applications affines ne sont pas des isométries : par exemple les homothéties.

Proposition 10.59.
Si $\mathcal{E}$ est modelé sur un espace euclidien $(E, \|.\|)$ alors la formule

$$d(A, B) = \|\overrightarrow{AB}\| \tag{10.137}$$

définit une distance sur $\mathcal{E}$.

Démonstration. Étant donné ce qui est dit en 10.2, 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 64.

Chapitre 11

Espaces vectoriels (encore)

11.1 Formes bilinéaires et quadratiques

Plus à propos de formes bilinéaires dans le thème 47.

Définition 11.1 ([136]).
*Soient trois espaces vectoriels E, F et V sur le même corps commutatif $\mathbb{K}$. Une application $b\colon E \times F \to V$ est **bilinéaire** si elle est séparément linéaire en ses deux variables, c'est-à-dire si*

(1) $b(u_1 + u_2, v) = b(u_1, v) + b(u_2, v)$,

(2) $b(u, v_1 + v_2) = b(u, v_1) + b(u, v_2)$

(3) $b(\lambda u, v) = b(u, \lambda v) = \lambda b(u, v)$

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 $b(u, v) = b(v, u)$.*

11.2.
Une application bilinéaire $E \times E \to \mathbb{K}$ n'est pas une application linéaire ; la distinction est importante. La linéarité est

$$b(\lambda u, \lambda v) = b\big(\lambda(u, v)\big) = \lambda b(u, v) \tag{11.1}$$

et la bilinéarité est

$$b(\lambda u, v) = b(u, \lambda v) = \lambda b(u, v). \tag{11.2}$$

En réalité la seule forme qui soit à la fois linéaire et bilinéaire est la forme identiquement nulle : la condition

$$b(\lambda u, \lambda v) = \lambda^2 b(u, v) = \lambda b(u, v) \tag{11.3}$$

pour tout $\lambda \in \mathbb{K}$ implique $b(u, v) = 0$.

Exemple 11.3([137])
L'application

$$\begin{aligned} b\colon \mathbb{M}(n, \mathbb{K}) \times \mathbb{M}(n, \mathbb{K}) &\to \mathbb{K} \\ (A, B) &\mapsto \operatorname{Tr}(AB) \end{aligned} \tag{11.4}$$

est une forme bilinéaire symétrique.

La vérification est un calcul :

$$\operatorname{Tr}(BA) = \sum_i (BA)_{ii} = \sum_{ik} B_{ik} A_{ki} = \sum_{ik} A_{ki} A_{ik} = \sum_k (AB)_{kk} = \operatorname{Tr}(AB). \tag{11.5}$$

△

11.2 Produit scalaire, produit hermitien

Définition 11.4 (Définie positive, thème 40)**.**
Si g est une application bilinéaire[1] *sur un espace vectoriel E nous disons qu'elle est*

(1) ***définie positive*** *si $g(x,x) \geqslant 0$ pour tout $x \in E$ et $g(x,x) = 0$ si et seulement si $x = 0$.*

(2) ***semi-définie positive*** *si $g(x,x) \geqslant 0$ pour tout $x \in E$. Nous dirons aussi parfois qu'elle est simplement « positive ».*

Cela est évidemment à lier à la définition 11.191 et la proposition 11.195 : une application bilinéaires est définie positive si et seulement si sa matrice symétrique associée l'est.

Définition 11.5.
*Un **produit scalaire** sur un espace vectoriel réel est une forme bilinéaire*[2] *symétrique strictement définie positive*[3]*.*

La définition suivante est utile pour celles qui veulent faire de la relativité [4].

Définition 11.6.
*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 11.7.
*Un espace vectoriel **euclidien** est un espace vectoriel de dimension finie muni d'un produit scalaire (définition 11.5).*

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 3.129). C'est pas très profond, mais si ça peut vous servir de moyen mnémotechnique...

Définition 11.8 ([138])**.**
*Soit E est un espace vectoriel sur $\mathbb{C}$. Une application $\langle .,. \rangle : E \times E \to \mathbb{C}$ 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) $\langle x + y, z \rangle = \langle x, y \rangle + \langle y, z \rangle$,

(3) $\langle x, y + z \rangle = \langle x, y \rangle + \langle x, z \rangle$.

*Cette forme est **hermitienne** si de plus*

$$\langle x, y \rangle = \overline{\langle y, x \rangle}. \tag{11.6}$$

*Un **produit hermitien** est une forme hermitienne strictement définie positive, c'est-à-dire telle que $\langle x, x \rangle \geqslant 0$ pour tout $x \in E$ et $\langle x, x \rangle = 0$ si et seulement si $x = 0$.*

Exemple 11.9
L'ensemble $E = \mathbb{C}^n$ vu comme espace vectoriel de dimension n sur $\mathbb{C}$ est muni d'une forme sesquilinéaire

$$\langle x, y \rangle = \sum_{k=1}^{n} x_k \bar{y}_k \tag{11.7}$$

pour tout $x, y \in \mathbb{C}^n$. Cela est un espace vectoriel hermitien. △

1. Définition 11.1.
2. Définition 11.1.
3. Définition 11.4.
4. Voir le théorème 19.15 qui établit les transformations de Lorentz.

11.2.1 Norme, produit scalaire et Cauchy-Schwarz (cas réel)

Dans la suite, le produit scalaire de x et y pourra être noté indifféremment par $x \cdot y$, $\langle x, y\rangle$ ou $b(x, y)$ lorsque une forme bilinéaire est donnée.

Nous rappelons au passage que les espaces vectoriels réels sont susceptibles de recevoir un produit scalaire, alors que les espaces vectoriels complexes sont susceptibles de recevoir un produit hermitien. Bien que de nombreux résultats soient identiques ou très similaires, ces deux notions sont à ne pas confondre.

Nous commençons par prouver qu'un produit scalaire étant donné, nous pouvons définir une norme par la formule $\|x\|^2 = \langle x, x\rangle$. Pour cela nous aurons besoin de l'inégalité de Cauchy-Schwarz.

Théorème 11.10 (Inégalité de Cauchy-Schwarz, cas réel)**.**
Soit un espace vectoriel muni d'un produit scalaire $(x, y) \mapsto x \cdot y$. En posant[5]

$$\|x\| = \sqrt{x \cdot x}, \tag{11.8}$$

nous avons

$$|x \cdot y| \leqslant \|x\|\|y\|. \tag{11.9}$$

Nous avons une égalité si et seulement si x et y sont multiples l'un de l'autre.

Démonstration. Étant donné que les deux membres de l'inéquation sont positifs, nous allons travailler en passant au carré afin d'éviter les racines carrés dans le second membre.

Nous considérons le polynôme

$$P(t) = \|x + ty\|^2 = (x + ty) \cdot (x + ty) = x \cdot x + x \cdot ty + ty \cdot x + t^2 y \cdot y. \tag{11.10}$$

En utilisant la bilinéarité (pour sortir les t) et la symétrique du produit scalaire, puis en ordonnant les termes selon les puissances de t,

$$P(t) = \|y\|^2 t^2 + 2(x \cdot y)t + \|x\|^2. \tag{11.11}$$

Cela est un polynôme du second degré en t dont le signe est toujours positif (ou nul). Par conséquent le discriminant[6] doit être négatif ou nul. Nous avons donc

$$\Delta = 4(x \cdot y)^2 - 4\|x\|^2\|y\|^2 \leqslant 0, \tag{11.12}$$

ce qui donne immédiatement

$$(x \cdot y)^2 \leqslant \|x\|^2\|y\|^2. \tag{11.13}$$

En ce qui concerne le cas d'égalité, si nous avons $x \cdot y = \|x\|\|y\|$, alors le discriminant Δ ci-dessus est nul et le polynôme P admet une racine double t_0. Pour cette valeur nous avons

$$P(t_0) = |x + t_0 y| = 0, \tag{11.14}$$

ce qui implique $x + t_0 y = 0$ et donc que x et y sont liés. □

Proposition 11.11.
Si $x, y \mapsto x \cdot y$ est un produit scalaire sur un espace vectoriel réel E. Nous posons $\|x\| = \sqrt{x \cdot x}$. Alors

(1) L'opération $\|.\|$ est une norme[7]*.*

(2) Cette norme vérifie l'identité du parallélogramme :

$$\|x - y\|^2 + \|x + y\|^2 = 2\|x\|^2 + 2\|y\|^2. \tag{11.15}$$

5. Attention à la notation : pour l'instant nous ne savons pas que c'est une norme. Ce sera justifié dans la proposition 11.11.

6. Le fameux $b^2 - 4ac$.

7. Définition 7.106.

Démonstration. En deux parties.

C'est une norme Nous allons nous contenter de prouver l'inégalité triangulaire. Si $x, y \in E$ nous avons

$$\|x+y\| = \sqrt{\|x\|^2 + \|y\|^2 + 2x \cdot y}. \tag{11.16}$$

Par l'inégalité de Cauchy-Schwarz, théorème 11.10 nous avons aussi

$$2x \cdot y \leqslant 2\|x\|\|y\|. \tag{11.17}$$

Nous pouvons donc majorer ce qui est dans la racine carré :

$$\|x\|^2 + \|y\|^2 + 2x \cdot y \leqslant \|x\|^2 + \|y\|^2 + 2\|x\|\|y\| = \big(\|x\| + \|y\|\big)^2. \tag{11.18}$$

En remettant les bouts ensemble,

$$\|x+y\| = \sqrt{\|x\|^2 + \|y\|^2 + 2x \cdot y} \leqslant \sqrt{\big(\|x\| + \|y\|\big)^2} = \|x\| + \|y\|. \tag{11.19}$$

Inégalité du parallélogramme Cette assertion est seulement un calcul :

$$\begin{aligned} \|x-y\|^2 + \|x+y\|^2 &= (x-y) \cdot (x-y) + (x+y) \cdot (x+y) \\ &= x \cdot x - x \cdot y - y \cdot x + y \cdot y \\ &\quad + x \cdot x + x \cdot y + y \cdot x + y \cdot y \\ &= 2x \cdot x + 2y \cdot y \\ &= 2\|x\|^2 + 2\|y\|^2. \end{aligned} \tag{11.20}$$

□

11.12.
Un produit scalaire fourni donc toujours une norme et donc une topologie. Il ne faudrait cependant pas croire que toute norme dérive d'un produit scalaire, même pas en dimension finie. Et ce, malgré l'équivalence de toutes les normes du théorème 12.6 dont vous avez déjà peut-être entendu parler.

Exemple 11.13
Sur $\mathbb{R}^2$, l'application $N(x,y) = |x| + |y|$ est une norme[8]. Nous allons voir qu'elle ne dérive pas d'un produit scalaire en montrant qu'elle ne vérifie pas l'identité du parallélogramme.

Voici un petit bout de code qui nous permet de ne pas faire de recherches à la main :

```
# Dans un cas réel, vous avez nettement intérêt à
# créer une classe 'Vecteur' qui implémente somme, différence
# et norme.
def N(v):
    return abs( v[0] )+abs(v[1])

def parall(v,w):
    # La différence v-w
    d=( v[0]-w[0],v[1]-w[1] )
    # La somme v+w
    s=( v[0]+w[0],v[1]+w[1] )

    return N(d)**2+N(s)**2-2*N(v)**2-2*N(w)**2
```

tex/sage/sageSnip018.sage

8. Proposition 9.46.

Il est vite vu qu'avec $v = (-1, 1)$ et $w = (1, 1)$, l'identité du parallélogramme n'est pas vérifiée. △

Lemme 11.14 ([43])**.**
Soit V un espace vectoriel muni d'un produit scalaire et de la norme associée. Si $x, y \in V$ satisfont à $\|x + y\| = \|x\| + \|y\|$, alors il existe $\lambda \geqslant 0$ tel que $x = \lambda y$.

Démonstration. Quitte à raisonner avec $x/\|x\|$ et $y/\|y\|$, nous supposons que $\|x\| = \|y\| = 1$. Dans ce cas l'hypothèse signifie que $\|x+y\|^2 = 4$. D'autre part en écrivant la norme en terme de produit scalaire,

$$\|x + y\|^2 = \|x\|^2 + \|y\|^2 + 2\langle x, y\rangle, \tag{11.21}$$

ce qui nous mène à affirmer que $\langle x, y\rangle = 1 = \|x\|\|y\|$. Nous sommes donc dans le cas d'égalité de l'inégalité de Cauchy-Schwarz [9], ce qui nous donne un λ tel que $x = \lambda y$. Étant donné que $\|x\| = \|y\| = 1$ nous avons obligatoirement $\lambda = \pm 1$, mais si $\lambda = -1$ alors $\langle x, y\rangle = -1$, ce qui est le contraire de ce qu'on a prétendu plus haut. Par soucis de cohérence, nous allons donc croire que $\lambda = 1$. □

Proposition 11.15.
si $v_1, \cdots, v_k$ sont des vecteurs non nuls, orthogonaux deux à deux, alors ces vecteurs forment une famille libre.

Lemme 11.16.
Une isométrie d'un espace euclidien fixe l'origine.

Démonstration. Soit une isométrie f d'un espace euclidien : $f(x) \cdot f(y) = x \cdot y$ pour tout $x, y \in E$. En particulier pour $x = 0$ nous avons

$$f(0) \cdot f(y) = 0 \tag{11.22}$$

pour tout y. Vu que f est une bijection, nous avons $f(0) \cdot x = 0$ pour tout x. Comme le produit scalaire est non dégénéré cela implique que $f(0) = 0$. □

11.2.2 Cauchy-Schwarz etc. cas complexe

Théorème 11.17 (Inégalité de Cauchy-Schwarz, cas complexe[139])**.**
Soit un espace vectoriel complexe muni d'un produit hermitien $\langle ., .\rangle$. Alors pour tout vecteurs x, y nous avons

$$|\langle x, y\rangle| \leqslant \|x\|\|y\| \tag{11.23}$$

où nous avons posé $\|x\| = \sqrt{\langle x, x\rangle}$.

Démonstration. Si $\langle x, y\rangle = 0$, le résultat est évident ; nous supposons que non. Nous posons

$$\theta = \frac{\langle x, y\rangle}{|\langle x, y\rangle|}. \tag{11.24}$$

C'est un élément de $\mathbb{C}$ de norme 1. Nous avons

$$\langle \frac{1}{\theta}x, y\rangle = \frac{|\langle x, y\rangle|}{\langle x, y\rangle}\langle x, y\rangle = |\langle x, y\rangle| \geqslant 0 \tag{11.25}$$

où le symbole « $\geqslant$ » signifie « est réel et positif ». Nous posons $x' = \frac{1}{\theta}x$ et nous considérons $t \in \mathbb{R}$. Remarquons que $\|x'\|^2 = \|x\|^2$:

$$\|x'\|^2 = \langle x', x'\rangle = \frac{1}{\theta\bar{\theta}}\langle x, x\rangle = \|x\|^2 \tag{11.26}$$

9. Théorème 11.10.

parce que $|\theta| = 1$.

En utilisant le fait que $\langle a, b\rangle + \langle b, a\rangle = \operatorname{Re}(\langle a, b\rangle)$ nous avons :

$$0 \leqslant \|x' + ty\|^2 = \|x'\|^2 + t\langle x', y\rangle + t\langle y, x'\rangle + t^2\|y\|^2 \tag{11.27a}$$
$$= \|y\|^2t^2 + 2\operatorname{Re}(\langle x', y\rangle)t + \|x'\|^2. \tag{11.27b}$$

Cela est un polynôme de degré 2 en t qui n'est jamais strictement négatif. Autrement dit, il a au maximum une seule racine, ce qui signifie que son discriminant est négatif ou nul :

$$\operatorname{Re}(\langle x', y\rangle)^2 - \|y\|^2\|x'\|^2 \leqslant 0. \tag{11.28}$$

Mais nous avons choisi x' de telle sorte que $\langle x', y\rangle = |\langle x, y\rangle| \in \mathbb{R}$ et $\|x'\|^2 = \|x\|^2$; nous avons donc

$$|\langle x, y\rangle|^2 \leqslant \|x\|^2\|y\|^2, \tag{11.29}$$

comme il se devait. □

Proposition 11.18 (Identité du parallélogramme[140])**.**
Soit une espace vectoriel complexe E muni d'un produit hermitien $\langle ., .\rangle$. Nous posons $\|x\| = \sqrt{\langle x, x\rangle}$. Nous avons

(1) $\|.\|$ est une norme.

(2) Elle vérifie l'identité du parallélogramme :

$$\|x + y\|^2 + \|x - y\|^2 = 2\|x\|^2 + 2\|b\|^2 \tag{11.30}$$

pour tout $x, y \in E$.

Démonstration. En ce qui concerne le fait que $\|.\|$ soit une norme, tout est essentiellement dans la définition 11.8 d'un produit hermitien. Voyons tout de même l'inégalité triangulaire. Nous avons :

$$\|x + y\|^2 = \langle x + y, x + y\rangle \tag{11.31a}$$
$$= \|x\|^2 + \|y\|^2 + \langle x, y\rangle + \langle y, x\rangle \tag{11.31b}$$
$$= \|x\|^2 + \|y\|^2 + 2\Re\big(\langle x, y\rangle\big) \tag{11.31c}$$
$$\leqslant \|x\|^2 + \|y\|^2 + 2|\Re\big(\langle x, y\rangle\big)| \tag{11.31d}$$
$$\leqslant \|x\|^2 + \|y\|^2 + 2|\langle x, y\rangle| \tag{11.31e}$$
$$\leqslant \|x\|^2 + \|y\|^2 + 2\|x\|\|y\| \tag{11.31f}$$
$$= \big(\|x\| + \|y\|\big)^2. \tag{11.31g}$$

Pour (11.31f) nous avons utilisé Cauchy-Schwarz 11.17. □

11.2.3 Projection et orthogonalité

Proposition 11.19 (Propriétés du produit scalaire)**.**
Si X et Y sont des vecteurs de $\mathbb{R}^3$, alors

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 $X \cdot X \geqslant 0$ *et* $X \cdot X = 0$ *si et seulement si* $X = 0$.

Note : lorsque nous écrivons $X = 0$, nous voulons voulons dire $X = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$.

Définition 11.20.
*La **norme** du vecteur X, notée $\|X\|$, est définie par*

$$\|X\| = \sqrt{X \cdot X} = \sqrt{x^2 + y^2 + z^2} \tag{11.32}$$

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 11.21.
*Deux vecteurs X et Y sont **orthogonaux** si $X \cdot Y = 0$.*

Cette définition de l'orthogonalité est motivée par la proposition suivante.

Proposition 11.22.
Si nous écrivons $\texttt{proj}_Y$ l'opération de projection sur la droite qui sous-tend Y, alors nous avons

$$\| \texttt{proj}_Y X\| = \frac{X \cdot Y}{\|Y\|}. \tag{11.33}$$

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

$$X = \begin{pmatrix} x \\ y \\ 0 \end{pmatrix}, \quad Y = \begin{pmatrix} l \\ 0 \\ 0 \end{pmatrix} \tag{11.34}$$

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 $\| \texttt{proj}_Y X\| = x$. Par conséquent,

$$\| \texttt{proj}_Y X\| = \frac{X \cdot Y}{l} = \frac{X \cdot Y}{\|Y\|}. \tag{11.35}$$

□

Corollaire 11.23.
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 11.22. □

Remarque 11.24.
Outre l'orthogonalité, le produit scalaire permet de savoir l'angle entre deux vecteurs à travers la définition 19.53. D'autres interprétations géométriques du déterminant sont listées dans le thème 54.

Nous sommes maintenant en mesure de déterminer, pour deux vecteurs quelconques u et v, la projection orthogonale de u sur v. Ce sera le vecteur $\bar{u}$ parallèle à v tel que $u - \bar{u}$ est orthogonal à v. Nous avons donc

$$\bar{u} = \lambda v \tag{11.36}$$

et

$$(u - \lambda v) \cdot v = 0. \tag{11.37}$$

La seconde équation donne $u \cdot v - \lambda v \cdot v = 0$, ce qui fournit λ en fonction de u et v :

$$\lambda = \frac{u \cdot v}{\|v\|^2}. \tag{11.38}$$

Nous avons par conséquent

$$\bar{u} = \frac{u \cdot v}{\|v\|^2} v. \tag{11.39}$$

Armés de cette interprétation graphique du produit scalaire, nous comprenons pourquoi nous disons que deux vecteurs sont orthogonaux lorsque leur produit scalaire est nul.

Nous pouvons maintenant savoir quel est le coefficient directeur d'une droite orthogonale à une droite donnée. En effet, supposons que la première droite soit parallèle au vecteur X et la seconde au vecteur Y. Les droites seront perpendiculaires si $X \cdot Y = 0$, c'est-à-dire si

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = 0. \tag{11.40}$$

Cette équation se développe en

$$x_1 y_1 = -x_2 y_2. \tag{11.41}$$

Le coefficient directeur de la première droite est $\frac{x_2}{x_1}$. Isolons cette quantité dans l'équation (11.41) :

$$\frac{x_2}{x_1} = -\frac{y_1}{y_2}. \tag{11.42}$$

Donc le coefficient directeur de la première est l'inverse et l'opposé du coefficient directeur de la seconde.

Exemple 11.25
Soit la droite $d \equiv y = 2x + 3$. Le coefficient directeur de cette droite est 2. Donc le coefficient directeur d'une droite perpendiculaires doit être $-\frac{1}{2}$. △

Preuve alternative. La preuve peut également être donnée en ne faisant pas référence au produit scalaire. Il suffit d'écrire toutes les quantités en termes des coordonnées de X et Y. Si nous posons

$$X = \begin{pmatrix} x_1 \\ x_2 \\ x_2 \end{pmatrix}, \quad Y = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}, \tag{11.43}$$

l'inégalité à prouver devient

$$(x_1y_1 + x_2y_2 + x_3y_3)^2 \leqslant (x_1^2 + x_2^2 + x_3^2)(y_1^2 + y_2^2 + y_3^2). \tag{11.44}$$

Nous considérons la fonction

$$\varphi(t) = (x_1 + ty_1)^2 + (x_2 + ty_2)^2 + (x_3 + ty_3)^2 \tag{11.45}$$

En tant que norme, cette fonction est évidemment positive pour tout t. En regroupant les termes de chaque puissance de t, nous avons

$$\varphi(t) = (y_1^2 + y_2^2 + y_3^2)t^2 + 2(x_1y_1 + x_2y_2 + x_3y_3)t + (x_1^2 + x_2^2 + x_3^2). \tag{11.46}$$

Cela est un polynôme du second degré en t. Par conséquent le discriminant doit être négatif. Nous avons donc

$$4(x_1y_1 + x_2y_2 + x_3y_3)^2 - (x_1^2 + x_2^2 + x_3^2)(y_1^2 + y_2^2 + y_3^2) \leqslant 0. \tag{11.47}$$

La thèse en découle aussitôt. □

Proposition 11.26.
La norme euclidienne a les propriétés suivantes :

(1) Pour tout vecteur X et réel λ, $\|\lambda X\| = |\lambda|\|X\|$. Attention à ne pas oublier la valeur absolue !
(2) Pour tout vecteurs X et Y, $\|X + Y\| \leqslant \|X\| + \|Y\|$.

Démonstration. Pour le second point, nous avons les inégalités suivantes :

$$\begin{aligned} \|X + Y\|^2 &= \|X\|^2 + \|Y\|^2 + 2X \cdot Y && \text{(11.48a)} \\ &\leqslant \|X\|^2 + \|Y\|^2 + 2|X \cdot Y| && \text{(11.48b)} \\ &\leqslant \|X\|^2 + \|Y\|^2 + 2\|X\|\|Y\| && \text{(11.48c)} \\ &= \big(\|X\| + \|Y\|\big)^2 && \text{(11.48d)} \end{aligned}$$

Nous avons utilisé d'abord la majoration $|x| \geqslant x$ qui est évidente pour tout nombre x ; et ensuite l'inégalité de Cauchy-Schwarz 11.10. □

11.2.4 Théorème de Pythagore

Nous allons donner une preuve du théorème de Pythagore.

Théorème 11.27 (Pythagone[1])**.**
Soient $A, B, S \in \mathbb{R}^2$ un triangle rectangle en A, c'est à dire tel que

$$(B - A) \cdot (A - S) = 0. \tag{11.49}$$

Alors

$$\|S - B\|^2 = \|S - A\|^2 + \|B - A\|^2. \tag{11.50}$$

Démonstration. En développant l'hypothèse (11.49) nous avons :

$$B \cdot A - B \cdot S - \|A\|^2 + A \cdot S = 0. \tag{11.51}$$

Et de même,

$$\|S - B\|^2 = (S - B) \cdot (S - B) = \|S\|^2 - 2B \cdot S + \|B\|^2. \tag{11.52}$$

En substituant dans cette dernière $B \cdot S$ par $B \cdot S = B \cdot A - \|A\|^2 + A \cdot S$ tirée de (11.51), nous trouvons

$$\|S - B\|^2 = \|S\|^2 - 2B \cdot A + 2\|A\|^2 - 2A \cdot S + \|B\|^2 = \|S - A\|^2 + \|B - A\|^2. \tag{11.53}$$

□

Je profite de l'occasion pour montrer mon scepticisme quant aux preuves de Pythagore basées sur différents pliages et découpages des carrés construits sur les côtés du triangle. Pour autant que je le sache, la géométrie dans « le plan » (c'est à dire pas dans $\mathbb{R}^2$ muni de son produit scalaire) ne définit pas « longueur » et « aire ». Donc bon ... Il y a peut-être moyen de s'en sortir, mais je ne le connais pas.

11.2.5 Produit vectoriel

Définition 11.28.
*Soient u et v, deux vecteurs de $\mathbb{R}^3$. Le **produit vectoriel** de u et v est le vecteur $u \times v$ défini par*

$$u \times v = \det \begin{pmatrix} e_1 & e_2 & e_3 \\ u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \end{pmatrix} \tag{11.54}$$

où les vecteurs e_1, e_2 et e_3 sont les vecteurs de la base canonique de $\mathbb{R}^3$.

Lemme 11.29.
Le produit vectoriel $u \times v$ est également exprimé par

$$u \times v = (u_2v_3 - u_3v_2)e_1 + (u_3v_1 - u_1v_3)e_2 + (u_1v_2 - u_2v_1)e_3 \tag{11.55a}$$

$$= \sum_{i,j,k} \epsilon_{ijk} v_i w_j e_k \tag{11.55b}$$

où ϵ_{ijk} est défini par $\epsilon_{xyz} = 1$ et ensuite ϵ_{ijk} est 1 ou -1 suivant que la permutation des x, y et z est paire ou impaire. C'est-à-dire que ϵ_{ijk} est la signature de la permutation qui amène $(1, 2, 3)$ sur (i, j, k).

Démonstration. Il s'agit seulement de développer explicitement le déterminant (11.54). □

11.30.
Mettons que $a \times b = v$. En calculant le même produit vectoriel dans la base $f_i = -e_i$, les composantes de a et b changent de signe et la formule (11.55) dit que le produit vectoriel ne change pas. On serait tenter d'écrire, dans la base $\{f_i\}$

$$(-a) \times (-b) = v, \tag{11.56}$$

tout en pleurant parce que dans la base des f_i, le vecteur v devient $-v$.

Il a des personnes que cela tracasse tellement qu'on entend parler de « le produit vectoriel est une pseudo-vecteur sous SO(2) ».

Il suffit d'être clair. Le produit vectoriel n'est défini que sur $\mathbb{R}^3$, et est définit par sa formule dans la base canonique, point barre. Si vous avez des vecteurs a et b dont vous connaissez les composantes dans une autre base, vous devez calculer les composantes dans la base canonique, utiliser la formule pour trouver les composantes de $a \times b$ dans la base canonique. Ensuite, si ça vous chante, vous pouvez calculer à nouveau les composantes de $a \times b$ dans une autre base.

Tout cela pour dire que le produit vectoriel n'est pas une opération très généralisable. Il est possible, pour sembler plus intrinsèque, de tenter cette définition : le produit vectoriel $a \times b$ est le vecteur perpendiculaire à a et b, de longueur égale à l'aire du parallélogramme construit sur a et b.

Cette « définition » a plusieurs inconvénients.

— Elle demande quand même un produit scalaire et des aires ; bref, elle demande une structure métrique,

— Elle ne donne pas le sens. En effet, dans $\mathbb{R}^3$, il y a deux vecteurs de longueur donnée perpendiculaires à a et b. Il faut donc préciser le sens. Cela revient à donner une orientation et donc, fondamentalement, à choisir une base.

Bref, on retiendra que le produit vectoriel est une opération accrochée à $\mathbb{R}^3$ et a sa base canonique.

Une des principales utilités du produit vectoriel est donnée dans la proposition suivante.

Proposition 11.31.
Si u et v sont des vecteurs de $\mathbb{R}^3$ alors le vecteur $u \times v$ est perpendiculaire à u et à v.

La chose importante à retenir est que le produit vectoriel permet de construire un vecteur simultanément perpendiculaire à deux vecteurs donnés. Le vecteur $u \times v$ est donc linéairement indépendant de u et v. En pratique, si u et v sont déjà linéairement indépendants, alors le produit vectoriel permet de compléter une base de $\mathbb{R}^3$.

Lemme-définition 11.32.
Nous avons l'égalité suivante pour tout $u, v, w \in \mathbb{R}^3$:

$$(u \times v) \cdot w = \det \begin{pmatrix} u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \\ w_1 & w_2 & w_3 \end{pmatrix}. \tag{11.57}$$

*Le résultat est nommé le **produit mixte** de trois vecteurs de $\mathbb{R}^3$.*

11.33.
Nous avons donné un nom à la combinaison $(u \times v) \cdot w$. J'imagine que vous voyez pourquoi nous ne considérons pas la combinaison $(u \cdot v) \times w$.

Le lemme suivant donne un moyen compliqué et peu pratique de calculer la valeur absolue du produit mixte. La formule (11.58) ne sera utilisée que pour faire le lien entre un jacobien et un élément de volume en dimension trois lorsque nous verrons les intégrales sur des variétés. Voir l'équation (21.37).

Lemme 11.34 ([1]).
Le produit mixte peut également être exprimé par

$$|(u\times v)\cdot w|^2=\det\begin{pmatrix}\|u\|^2 & u\cdot v & u\cdot w\\ v\cdot u & \|v\|^2 & v\cdot w\\ w\cdot u & w\cdot v & \|w\|^2\end{pmatrix}. \tag{11.58}$$

Démonstration. Si nous notons

$$a=\begin{pmatrix}u_1 & u_2 & u_3\\ v_1 & v_2 & v_3\\ w_1 & w_2 & w_3\end{pmatrix}, \tag{11.59}$$

il faut simplement remarquer que

$$\begin{pmatrix}\|u\|^2 & u\cdot v & u\cdot w\\ v\cdot u & \|v\|^2 & v\cdot w\\ w\cdot u & w\cdot v & \|w\|^2\end{pmatrix}=aa^t. \tag{11.60}$$

Donc au niveau des déterminants, en utilisant les propositions 4.93 et le lemme 4.70 nous avons

$$\det\begin{pmatrix}\|u\|^2 & u\cdot v & u\cdot w\\ v\cdot u & \|v\|^2 & v\cdot w\\ w\cdot u & w\cdot v & \|w\|^2\end{pmatrix}=\det(aa^t)=\det(a)\det(a^t)=\det(a)^2. \tag{11.61}$$

Et maintenant, par définition, $\det(a)=(u\times w)\cdot w$. Donc le résultat annoncé. □

Proposition 11.35.
Les applications produit scalaire, vectoriel et mixte sont multilinéaires. Spécifiquement, nous avons les propriétés suivantes.

(1) *Les applications produit scalaire et vectoriel sont bilinéaires. C'est-à-dire que pour tout vecteurs a, b, c et pour tout nombre α et β nous avons*

$$\begin{aligned}a\times(\alpha b+\beta c)&=\alpha(a\times b)+\beta(a\times c)\\ (\alpha a+\beta b)\times c&=\alpha(a\times c)+\beta(b\times c).\end{aligned} \tag{11.62}$$

(2) *Le produit mixte est trilinéaire.*

(3) *Le produit vectoriel est antisymétrique, c'est-à-dire $u\times v=-v\times u$.*

(4) *Nous avons $u\times v=0$ si et seulement si u et v sont colinéaires, c'est-à-dire si et seulement si l'équation $\alpha u+\beta v=0$ a une solution différente de la solution triviale $(\alpha,\beta)=(0,0)$.*

Proposition 11.36 (Identité de Lagrange[141]).
Si $x,y\in\mathbb{R}^n$, alors

$$\|x\|^2\|y\|^2-(x\cdot y)^2=\sum_j\sum_{i<j}(x_iy_j-x_jy_i)^2. \tag{11.63}$$

Et si $n=3$ alors

$$\|x\times y\|=\|y\|^2\|y\|^2-(x\cdot y)^2. \tag{11.64}$$

Démonstration. C'est un calcul. D'abord nous avons

$$\|x\|^2\|y\|^2-(x\cdot y)^2=\sum_i x_i^2\sum_j y_j^2-\big(\sum_k x_ky_k\big)^2=\sum_{ij}x_i^2y_j^2-\sum_{kl}x_ky_kx_ly_l. \tag{11.65}$$

Ensuite nous coupons les sommes de la façon suivante

$$\sum_{ij}=\sum_j\sum_{i<j}+\sum_j(i=j)+\sum_j\sum_{i>j} \tag{11.66}$$

pour obtenir

$$\begin{aligned}\|x\|^2\|y\|^2 - (x\cdot y)^2 = &\sum_j\sum_{i<j} x_i^2y_j^2 + \sum_j x_j^2y_j^2 + \sum_j\sum_{i>j} x_i^2y_j^2\\ &- \sum_l\sum_{k<l} x_ky_kx_ly_l - \sum_k x_k^2y_k^2 - \sum_l\sum_{k>l} x_ky_kx_ly_l.\end{aligned} \tag{11.67}$$

Il y a deux termes qui se simplifient. Notez que si A_{kl} est symétrique en kl nous avons

$$\sum_l\sum_{k<l} A_{kl} = \sum_k\sum_{l<k} A_{lk} = \sum_k\sum_{l<k} A_{kl}. \tag{11.68}$$

La première égalité était seulement un renommage des indices. Le coup des indices symétriques est justement ce qu'il se passe dans les deux termes en$x_ky_kx_ly_l$, donc nous les regroupons :

$$\|x\|^2\|y\|^2 - (x\cdot y)^2 = \sum_j\big(\sum_{i<j} x_i^2x_j^2 + \sum_{i>j} x_i^2y_j^2 - 2\sum_{i>j} x_iy_ix_jy_j\big) \tag{11.69a}$$

$$= \sum_j\sum_{i<j}(x_i^2y_j^2 + x_j^2y_i^2 - 2x_iy_ix_jy_j) \tag{11.69b}$$

$$= \sum_j\sum_{i<j}(x_iy_j - x_jy_i)^2. \tag{11.69c}$$

Voila qui prouve la première formule. Pour la seconde, il faut seulement poser $n = 3$ et écrire les sommes explicitement.

— Pour $j = 1$, la somme sur i est $\sum_{i<1}$, c'est-à-dire aucun termes.
— Pour $j = 2$, il y a seulement $i = 1$, donc le terme $(x_1y_2 - x_2y_1)^2$.
— Pour $j = 3$, il y a les termes $i = 1$ et $i = 2$, donc les termes $(x_1y_3 - x_3y_1)^2 + (x_2y_3 - x_3y_2)^2$.

Ces trois termes collectés sont justement les composants (au carré) de $x\times y$ données dans la formule (11.55a). □

Les trois vecteurs de base e_x, e_y et e_y ont des produits vectoriels faciles à retenir :

$$\begin{aligned}e_x\times e_y &= e_z\\ e_y\times e_z &= e_x\\ e_z\times e_x &= e_y\end{aligned} \tag{11.70}$$

Les deux formules suivantes, qui mêlent le produit scalaire et le produit vectoriel, sont souvent utiles en analyse vectorielle :

$$\begin{aligned}(u\times v)\cdot w &= u\cdot(v\times w)\\ (u\times v)\times w &= -(v\cdot w)u + (u\cdot w)v\end{aligned} \tag{11.71}$$

pour tout vecteurs u, v et w dans $\mathbb{R}^3$. Nous les admettons sans démonstration. La seconde formule est parfois appelée **formule d'expulsion**.

Exemple 11.37
Calculons le produit vectoriel $v\times w$ avec

$$v = \begin{pmatrix}3\\-1\\1\end{pmatrix}\quad w = \begin{pmatrix}1\\2\\-1\end{pmatrix}. \tag{11.72}$$

Les vecteurs s'écrivent sous la forme $v = 3e_x - e_y + e_z$ et $w = e_x + 2e_y - e_z$. Le produit vectoriel s'écrit

$$\begin{aligned}(3e_x - e_y + e_z)\times(e_x + 2e_y - e_z) &= 6e_x\times e_y - 3e_x\times e_z\\ &\quad - e_y\times e_x + e_y\times e_z\\ &\quad + e_z\times e_x + 2e_z\times e_y\\ &= 6e_z + 3e_y + e_z + e_x + e_y - 2e_x\\ &= -e_x + 4e_y + 7e_z.\end{aligned} \tag{11.73}$$

△

11.2.6 Produit mixte

Si a, b et c sont trois vecteurs, leur **produit mixte** est le nombre $a \cdot (b \times c)$. En écrivant le produit vectoriel sous forme de somme de trois déterminants 2×2, nous avons

$$\begin{aligned} & a \cdot (b \times c) \\ & = (a_1 e_x + a_2 e_y + a_3 e_z) \cdot \left(\begin{vmatrix} b_2 & b_3 \\ c_2 & c_3 \end{vmatrix} e_x - \begin{vmatrix} b_1 & b_3 \\ c_1 & c_3 \end{vmatrix} e_y + \begin{vmatrix} b_1 & b_2 \\ c_1 & c_2 \end{vmatrix} \right) \\ & = a_1 \begin{vmatrix} b_2 & b_3 \\ c_2 & c_3 \end{vmatrix} - a_2 \begin{vmatrix} b_1 & b_3 \\ c_1 & c_3 \end{vmatrix} + a_3 \begin{vmatrix} b_1 & b_2 \\ c_1 & c_2 \end{vmatrix} \\ & = \begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix}. \end{aligned} \tag{11.74}$$

Le produit mixte s'écrit donc sous forme d'un déterminant. Nous retenons cette formule :

$$a \cdot (b \times c) = \begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix}. \tag{11.75}$$

Un grand intérêt du produit vectoriel est qu'il fournit un vecteur qui est simultanément perpendiculaire aux deux vecteurs donnés.

Proposition 11.38.
Le produit vectoriel[10] $a \times b$ *est un vecteur orthogonal à* a *et* b.

Démonstration. Vérifions que $a \perp (a \times b)$. Pour cela, nous calculons $a \cdot (a \times b)$, c'est-à-dire le produit mixte

$$a \cdot (a \times b) = \begin{vmatrix} a_1 & a_2 & a_3 \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix} = 0. \tag{11.76}$$

L'annulation de ce déterminant est due au fait que deux de ses lignes sont égales. □

Ces résultats admettent une intéressante généralisation.

Lemme 11.39.
Soit $X \in \mathbb{R}^n$ *ainsi que* $v_1, \dots, v_{n-1} \in \mathbb{R}^n$. *Alors*

(1) Nous avons

$$\det(X, v_1, \dots, v_{n-1}) = X \cdot \det \begin{pmatrix} e_1 & \dots & e_n \\ & v_1 & \\ & \vdots & \\ & v_{n-1} & \end{pmatrix} \tag{11.77}$$

(2) Le vecteur

$$\det \begin{pmatrix} e_1 & \dots & e_n \\ & v_1 & \\ & \vdots & \\ & v_{n-1} & \end{pmatrix} \tag{11.78}$$

est orthogonal à tous les v_i.

10. Définition 11.28.

Démonstration. Vu que les deux côtés de (11.77) vus comme fonctions de X, sont des applications linéaires de $\mathbb{R}^n$ dans $\mathbb{R}$, il suffit de vérifier l'égalité sur une base.

Nous posons $\tau_i\colon \mathbb{R}^n \to \mathbb{R}^{n-1}$,

$$\tau_i(v)_k = \begin{cases} v_k & \text{si } k < i \\ v_{k+1} & \text{si } k \geqslant i. \end{cases} \tag{11.79}$$

et nous avons d'une part

$$e_k \cdot \det \begin{pmatrix} e_1 & \dots & e_n \\ & v_1 & \\ & \vdots & \\ & v_{n-1} & \end{pmatrix} = \det \begin{pmatrix} \tau_k v_1 \\ \vdots \\ \tau_k v_{n-1} \end{pmatrix} \tag{11.80}$$

et d'autre part,

$$\det(e_k, v_1, \dots, v_{n-1}) = \det \begin{pmatrix} 0 & & & \\ \vdots & & & \\ 1 & v_1 & \cdots & v_{n-1} \\ \vdots & & & \\ 0 & & & \end{pmatrix} = \det(\tau_k v_1, \dots, \tau_k v_{n-1}). \tag{11.81}$$

La première assertion est démontrée.

En ce qui concerne la seconde, il suffit d'appliquer la première et se souvenir qu'un déterminant est nul lorsque deux lignes sont égales [11]. En effet :

$$v_k \cdot \det \begin{pmatrix} e_1 & \dots & e_n \\ & v_1 & \\ & \vdots & \\ & v_{n-1} & \end{pmatrix} = \det(v_k, v_1, \dots, v_n) = 0. \tag{11.82}$$

□

11.2.7 Procédé de Gram-Schmidt

Proposition 11.40 (Procédé de Gram-Schmidt)**.**
Un espace euclidien possède une base orthonormée.

Démonstration. Soit E un espace euclidien et $\{v_1, \dots, v_n\}$, une base quelconque de E. Nous posons d'abord

$$f_1 = v_1, \quad e_1 = \frac{f_1}{\|f_1\|}. \tag{11.83}$$

Ensuite

$$f_2 = v_2 - \langle v_2, e_1\rangle e_1, \quad e_2 = \frac{f_2}{\|f_2\|}. \tag{11.84}$$

Notons que $\{e_1, e_2\}$ est une base de $\mathrm{Span}\{v_1, v_2\}$. De plus elle est orthogonale :

$$\langle e_1, f_2\rangle = \langle e_1, v_2\rangle - \langle v_2, e_1\rangle \underbrace{\langle e_1, e_1\rangle}_{=1} = 0. \tag{11.85}$$

Le fait que $\|e_1\| = \|e_2\| = 1$ est par construction. Nous avons donc donné une base orthonormée de $\mathrm{Span}\{v_1, v_2\}$.

11. Corollaire 4.73.

Nous continuons par récurrence en posant

$$f_k = v_k - \sum_{i=1}^{k-1} \langle v_k, e_i \rangle e_i, \quad e_k = \frac{f_k}{\|f_k\|}. \tag{11.86}$$

Pour tout $j < k$ nous avons

$$\langle e_j, f_k \rangle = \langle e_j, v_k \rangle - \sum_{i=1}^{k-1} \langle v_k, e_i \rangle \underbrace{\langle e_i, e_j \rangle}_{=\delta_{ij}} = 0 \tag{11.87}$$

□

Cet algorithme de Gram-Schmidt nous donne non seulement l'existence de bases orthonormée pour tout espace euclidien, mais aussi le moyen d'en construire à partir de n'importe quelle base.

11.2.8 Approximation

Le lemme suivant est surtout intéressant en dimension infinie.

Lemme 11.41.
Soit un espace vectoriel normé V et un sous-espace vectoriel dense A. Soit $v \in V$; il existe une suite (v_n) dans A telle que $v_n \xrightarrow{V} v$ et $\|v_n\| \leqslant \|v\|$ pour tout n.

Démonstration. Vu que A est dense, il existe une suite a_n dans A telle que $a_n \to v$. Ensuite il suffit de poser

$$v_n = \frac{n}{n+1} \frac{\|v\|}{\|a_n\|} a_n. \tag{11.88}$$

Par construction nous avons toujours

$$\|v_n\| = \frac{n}{n+1} \|v\| \leqslant \|v\|. \tag{11.89}$$

Et de plus, la norme étant continue [12],

$$\lim_{n\to\infty} v_n = \lim_{n\to\infty} \frac{n}{n+1} \lim_{n\to\infty} \frac{\|v\|}{\|v_n\|} \lim_{n\to\infty} v_n = v. \tag{11.90}$$

Le fait que v_n soit dans A est dû au fait que A soit vectoriel. □

Proposition 11.42.
Soit un espace vectoriel normé V et un sous-espace vectoriel dense A. Soit $v \in V$; pour tout $a \in \mathbb{R}$ nous avons

$$\sup\{|v \cdot a| \text{ tel que } a \in A \text{ et } \|a\| \leqslant \lambda\} = \lambda \|v\|. \tag{11.91}$$

Démonstration. D'abord pour tout $a \in A$ vérifiant $\|a\| \leqslant \lambda$ l'inégalité de Cauchy-Schwarz 11.10 donne

$$|v \cdot a| \leqslant \|v\|\|a\| \leqslant \lambda \|v\|. \tag{11.92}$$

Donc le supremum dont on parle est majoré par $\lambda\|v\|$.

Il nous faut l'inégalité dans l'autre sens. Par densité nous pouvons choisir une suite $v_n \in A$ tel que $v_n \to v$. Ensuite nous posons

$$a_n = \frac{\lambda}{\|v_n\|} v_n. \tag{11.93}$$

Nous avons $\|a_n\| = \lambda$ pour tout n et

$$|v \cdot a_n| = \frac{\lambda}{\|v_n\|} |v \cdot v_n|, \tag{11.94}$$

12. Où dans le calcul suivant nous utilisons la continuité de la norme ? Posez-vous la question.

et en passant à la limite,

$$\lim_{n\to\infty} |v \cdot a_n| = \frac{\lambda}{\|v\|}\|v \cdot v\| = \lambda\|v\|. \tag{11.95}$$

Donc l'ensemble sur lequel nous prenons le supremum contient une suite convergente vers $\lambda\|v\|$. Le supremum est donc au moins aussi grand que cela. □

11.3 Déterminants

11.3.1 Formes multilinéaires alternées

Définition 11.43.
*Soit E, un $\mathbb{K}$-espace vectoriel. Une forme linéaire **alternée** sur E est une application linéaire $f\colon E \to \mathbb{K}$ telle que $f(v_1, \dots, v_k) = 0$ dès que $v_i = v_j$ pour certains $i \neq j$.*

Lemme 11.44.
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

$$0 = f(x + y, x + y) = f(x, x) + f(x, y) + f(y, x) + f(y, y) = f(x, y) + f(y, x). \tag{11.96}$$

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. □

Proposition 11.45 ([142])**.**
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 $f\colon E \to \mathbb{K}$ ainsi que des vecteurs $(v_1, \dots, v_n)$ de E. Nous pouvons les écrire dans la base

$$v_j = \sum_{i=1}^{n} \alpha_{ij} e_i \tag{11.97}$$

et alors exprimer f par

$$f(v_1, \dots, v_n) = f\Big(\sum_{i_1=1}^{n} \alpha_{1i_1} e_{i_1}, \dots, \sum_{i_n=1}^{n} \alpha_{ni_n} e_{i_n}\Big) \tag{11.98a}$$

$$= \sum_{i,j} \alpha_{1i_1} \dots \alpha_{ni_n} f(e_{i_1}, \dots, e_{i_n}). \tag{11.98b}$$

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

$$f(v_1, \dots, v_n) = \sum_{\sigma\in S_n} \alpha_{\sigma(1)1} \dots \alpha_{\sigma(n)n} f(e_{\sigma(1)}, \dots, e_{\sigma(n)}). \tag{11.99}$$

En utilisant encore une fois le fait que la forme f soit alternée, $f = f(e_1, \dots, e_n)\Pi$ où

$$\Pi(v_1, \dots, v_n) = \sum_{\sigma\in S_n} \epsilon(\sigma)\alpha_{\sigma(1)1} \dots \alpha_{\sigma(n)n}. \tag{11.100}$$

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 11.44, il suffit de prouver que cette forme est antisymétrique [13].

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 $\alpha_{i1} = \alpha_{i2}$:

$$\begin{aligned}
\Pi(v, v, v_3, \dots, v_n) &= \sum_{\sigma\in S_n} \epsilon(\sigma)\alpha_{\sigma(1)1}\alpha_{\sigma(2)2}\alpha_{\sigma(3)3}\dots\alpha_{\sigma(n)n} && \text{(11.101a)}\\
&= \sum_{\sigma\in S_n} \epsilon(\sigma\tau)\alpha_{\sigma\tau(1)1}\alpha_{\sigma\tau(2)2}\alpha_{\sigma\tau(3)3}\dots\alpha_{\sigma\tau(n)n} \qquad \text{où } \tau = (12) && \text{(11.101b)}\\
&= -\sum_{\sigma\in S_n} \epsilon(\sigma)\alpha_{\sigma(1)1}\alpha_{\sigma(2)2}\alpha_{\sigma(3)3}\dots\alpha_{\sigma(n)n} && \text{(11.101c)}\\
&= -\Pi(v, v, v_3, \dots, v_n). && \text{(11.101d)}
\end{aligned}$$

□

11.3.2 Déterminant d'une famille de vecteurs

Nous considérons un corps $\mathbb{K}$ et l'espace vectoriel E de dimension n sur $\mathbb{K}$.

Définition 11.46 (Déterminant d'une famille de vecteurs[6])**.**
*Le **déterminant** de la famille de vecteurs $(v_1, \dots, v_n)$ dans la base B est l'élément de $\mathbb{K}$*

$$\det_{(e_1,\dots,e_n)}(v_1, \dots, v_n) = \sum_{\sigma\in S_n} \epsilon(\sigma) \prod_{i=1}^{n} e^*_{\sigma(i)}(v_i) \tag{11.102}$$

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 $\det_{(e_1,\dots,e_n)}(v_1, \dots, v_n)$.

11.47.
La base $\{e_i\}$ est la base canonique de $\mathbb{K}^n$, et l'élément e_k^* est la forme linéaire définie par

$$\begin{aligned}
e_k^*\colon \mathbb{K}^n &\to \mathbb{K}\\
\sum_i x_i e_i &\mapsto x_k.
\end{aligned} \tag{11.103}$$

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 11.51 va un peu parler du cas où $\mathbb{K}^n$ est muni d'une base orthonormée.

Lemme 11.48 ([6])**.**
Les propriétés du déterminant. Soit B une base de E.

(1) L'application $\det_B\colon E^n \to \mathbb{K}$ *est n-linéaire.*

(2) L'application $\det_B\colon E^n \to \mathbb{K}$ *est n-linéaire est antisymétrique et alternée* [14].

(3) Pour toute base, $\det_B(B) = 1$.

13. C'est ici que joue l'hypothèse sur la caractéristique de $\mathbb{K}$.
14. Alternée, définition 11.43. En caractéristique 2, alternée n'est pas équivalent à symétrique.

(4) *Le déterminant ne change pas si on remplace un vecteur par une combinaison linéaire des autres :*

$$\det_B(v_1,\dots,v_n)=\det_B\big(v_1+\sum_{s=2}^{n}a_sv_s,v_2,\dots,v_n\big).\tag{11.104}$$

(5) *Si on permute les vecteurs,*

$$\det_B(v_1,\dots,v_n)=\epsilon(\sigma)\det_B(v_{\sigma(1)},\dots,v_{\sigma(n)}).\tag{11.105}$$

(6) *Si B' est une autre base :*

$$\det_B=\det_B(B')\det_{B'}\tag{11.106}$$

(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

$$\det_B(x_1+\lambda x_2,v_2,\dots,v_n)=\sum_\sigma\epsilon(\sigma)\prod_{i=1}^{n}e^*_{\sigma(i)}(v_i)\tag{11.107a}$$

$$=\sum_\sigma\epsilon(\sigma)\Big(e^*_{\sigma(1)}(x_1+\lambda x_2)\Big)\prod_{i=2}^{n}e^*_{\sigma(i)}(v_i).\tag{11.107b}$$

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 11.49.

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 :

$$\sigma_{\sigma\in S_n}(-1)^\sigma\prod_i\epsilon^*_{\sigma(i)}(v_i)=\sum_{\sigma\in A_n}(-1)^\sigma\prod_i\epsilon^*_{\sigma(i)}(v_i)+\sum_{\sigma\in A_n}(-1)^{\sigma\beta}\prod_i\epsilon^*_{(\sigma\beta)(i)}(v_i).\tag{11.108}$$

D'abord $(-1)^\sigma=1$ et $(-1)^{\sigma\beta}=-1$. Ensuite, pour un $\sigma\in A_n$ donné, nous avons

$$\prod_i\epsilon^*_{(\sigma\beta)(i)}(v_i)=\epsilon^*_{(\sigma\beta)(k)}(v_k)\epsilon^*_{(\sigma\beta)(l)}(v_l)\prod i^{i\neq k}_{\neq l}\epsilon^*_{(\sigma\beta)(i)}(v_i)\tag{11.109a}$$

$$=\epsilon^*_{\sigma(l)}(v_k)\epsilon^*_{\sigma(k)}(v_l)\prod_{\substack{i\neq k\\ i\neq l}}\epsilon^*_{\sigma(i)}(v_i)\tag{11.109b}$$

$$=\epsilon^*_{\sigma(l)}(v_l)\epsilon^*_{\sigma(k)}(v_k)\prod_{\substack{i\neq k\\ i\neq l}}\epsilon^*_{\sigma(i)}(v_i)\tag{11.109c}$$

$$=\prod_i\epsilon^*_{\sigma(i)}(v_i).\tag{11.109d}$$

Donc les deux termes de la somme (11.108) 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 11.44.

(3) Nous avons

$$\det_B(B)=\sum_{\sigma\in S_n}\epsilon(\sigma)\prod_{i=1}^{n}\underbrace{e^*_{\sigma(i)}(e_i)}_{=\delta_{\sigma(i),i}}.\tag{11.110}$$

Si σ n'est pas l'identité, le produit contient forcément un facteur nul. Il ne reste de la somme que $\sigma=\mathrm{Id}$ et le résultat est 1.

(4) Vu que $\det_B$ est linéaire en tous ses arguments,

$$\det_B\left(v_1+\sum_{s=2}^{n}a_sv_s,v_2,\dots,v_n\right)=\det_B(v_1,\dots,v_n)+\sum_{s=2}^{n}a_s\det_B(v_s,v_2,\dots,v_n).\tag{11.111}$$

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 :

$$\begin{aligned}\det_B(v_{\sigma(1)},\dots,v_{\sigma(n)})&=\sum_{\sigma'}\epsilon(\sigma')\prod_{i=1}^{n}e^*_{\sigma'(i)}(w_i)&(11.112a)\\&=\sum_{\sigma'}\epsilon(\sigma')\prod_{i=1}^{n}e^*_{\sigma'(i)}(v_{\sigma(i)})&(11.112b)\\&=\sum_{\sigma'}\epsilon(\sigma')\prod_{i=1}^{n}e^*_{\sigma^{-1}\sigma'(i)}(v_i)&(11.112c)\\&=\sum_{\sigma'}\epsilon(\sigma\sigma')\prod_{i=1}^{n}e^*_{\sigma'(i)}(v_i)&(11.112d)\\&=\epsilon(\sigma)\det_B(v_1,\dots,v_n).&(11.112e)\end{aligned}$$

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 $\epsilon\colon S_n\to\{0,1\}$ était un morphisme de groupe (proposition 2.73).

(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' :

$$\det_B(B')=\lambda\det_{B'}(B'),\tag{11.113}$$

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 $\det_B(B')\neq0$, 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.

□

11.49.
Si la caractéristique du corps de base n'est pa deux, une forme antisymétrique est alternée (lemme 11.44). Il est alors plus facile de prouver que le déterminant est antisymétrique et d'en déduire qu'il est alterné.

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 $\det_B(v_1,v_1)=-\det_B(v_1,v_1)$ (permutation de v_1 et 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 11.45, il existe une unique forme n-linéaire alternée égale à 1 sur B, et c'est $\det_B\colon E^n\to\mathbb{K}$.

11.3.3 Déterminant d'un endomorphisme

L'interprétation géométrique du déterminant en termes d'aires et de volumes est donnée après la théorème 15.251.

Lemme-définition 11.50.
Si $f\colon E \to E$ est un endomorphisme, et si les parties B et B' sont deux bases, alors

$$\det_B\big(f(B)\big) = \det_{B'}\big(f(B')\big). \tag{11.114}$$

Ce nombre, indépendant de la base choisie est nommé le ***déterminant*** *de f et est noté* $\det(f)$.

Démonstration. L'application

$$\begin{aligned}\varphi\colon E^n &\to \mathbb{K}\\ v_1,\dots,v_n &\mapsto \det_B\big(f(v_1),\dots,f(v_n)\big)\end{aligned} \tag{11.115}$$

est n-linéaire et alternée ; il existe donc $\lambda \in \mathbb{K}$ tel que $\varphi = \lambda \det_B$. En appliquant cela à B :

$$\det_B\big(f(B)\big) = \lambda \det_B(B) = \lambda. \tag{11.116}$$

Nous avons donc déjà prouvé que $\lambda = \det_B\big(f(B)\big)$, c'est-à-dire

$$\det_B\big(f(v)\big) = \det_B\big(f(B)\big)\det_B(v). \tag{11.117}$$

Nous allons maintenant introduire B' là où il y a du v en utilisant les formules (11.106) :

$$\det_B\big(f(v)\big) = \det_B(B')\det_{B'}\big(f(v)\big) \tag{11.118a}$$
$$\det_B(v) = \det_B(B')\det_{B'}(v). \tag{11.118b}$$

Nous obtenons

$$\det_{B'}\big(f(v)\big) = \det_B\big(f(B)\big)\det_{B'}(v). \tag{11.119}$$

Et on applique cela à $v = B'$:

$$\det_{B'}\big(f(B')\big) = \det_B\big(f(B)\big)\underbrace{\det_{B'}(B')}_{=1}. \tag{11.120}$$

□

Couplé à la formule (11.102), nous pouvons écrire la formule pratique à utiliser le plus souvent.

Lemme 11.51.
Soit un espace vectoriel euclidien[15] *E sur le corps $\mathbb{K}$. Si $\{e_i\}_{i=1,\dots,n}$ est une base orthonormée de E et si $f\colon E \to E$ est un endomorphisme, alors*

$$\det(f) = \sum_{\sigma\in S_n} \epsilon(\sigma)\prod_{i=1}^{n}\langle e_{\sigma(i)}, f(e_i)\rangle. \tag{11.121}$$

Démonstration. Nous utilisons la définition 11.50 du déterminant d'un endomorphisme $\det(f) = \det_B\big(f(B)\big)$ en prenant la liste des vecteurs $\{e_i\}$ comme B. En l'occurrence, le i^{e} vecteur de la famille B est $f(e_i)$.

Vu que la base est orthonormée, nous avons $e_k^*(v) = \langle e_k, v\rangle$ et donc aussi

$$e^*_{\sigma(i)}(v_i) = \langle e^*_{\sigma(i)}, f(e_i)\rangle. \tag{11.122}$$

□

15. C'est-à-dire qu'il possède un produit scalaire, voir la définition 11.7.

Et si vous avez tout suivi, vous aurez remarqué que les produits scalaires impliqués dans la formule (11.121) sont les éléments de la matrice de f dans la base $\{e_i\}$ parce que $\langle e_i, f(e_j)\rangle$ est la composante i de l'image de e_j par f. Si la matrice est composée en mettant en colonne les images des vecteurs de base, le compte est bon.

Proposition 11.52.
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 automorphisme*[16] *si et seulement si* $\det(f)\neq 0$.
(3) *Si* $\det(f)\neq 0$ *alors* $\det(f^{-1})=\det(f)^{-1}$.
(4) *L'application* $\det\colon \mathrm{GL}(E)\to\mathbb{K}\backslash\{0\}$ *est un morphisme de groupe.*

Démonstration. Point par point.

(1) Nous considérons l'application
$$\begin{aligned}\varphi\colon E^n &\to \mathbb{K}\\ v &\mapsto \det_B\big(f(v)\big).\end{aligned}\tag{11.123}$$
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 $\det_B\big(f(B)\big)=\lambda$. Autrement dit :
$$\lambda=\det(f).\tag{11.124}$$
Calculons à présent $\varphi\big(g(B)\big)$: d'une part,
$$\varphi\big(g(B)\big)=\det_B\big((f\circ g)(B)\big)\tag{11.125}$$
et d'autre part,
$$\varphi\big(g(B)\big)=\lambda\det_B\big(g(B)\big)=\lambda\det(g)\tag{11.126}$$
En égalisant et en reprenant la la valeur déjà trouvée de λ,
$$\det\big(f\circ g)(B)\big)=\det(f)\det(g),\tag{11.127}$$
ce qu'il fallait.

(2) Supposons que f soit un automorphisme. Alors si B est une base, $f(B)$ est une base. Par conséquent $\det(f)=\det_B\big(f(B)\big)\neq 0$ parce que $f(B)$ est une base (lemme 11.48(8)).
Réciproquement, supposons que $\det(f)\neq 0$. Alors si B est une base quelconque nous avons $\det_B\big(f(B)\big)\neq 0$, 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 11.53.
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 $A\in$
$eM(m\times n,\mathbb{K})$ nous associons l'application linéaire[17]
$$f_A(x)=\sum_{i\alpha}A_{\alpha i}x_i f_\alpha.\tag{11.128}$$
Alors, en ce qui concerne les déterminants[18]*, nous avons*

16. Endomorphisme inversible, définition 4.29.
17. Dont nous avons déjà beaucoup parlé entre autres dans la proposition 4.65.
18. Définition 11.50 pour les applications linéaires et 4.68 pour les matrices.

(1) $\det(f_A) = \det(A)$

(2) $\det(f_{AB}) = \det(f_A)\det(f_B)$

Démonstration. Nous devons étudier la formule

$$\det(f_A) = \sum_{\sigma\in S_n} \epsilon(\sigma) \prod_{i=1}^{n} e^*_{\sigma(i)}\big(f_A(e_i)\big). \tag{11.129}$$

En premier lieu nous avons

$$f_A(e_i) = \sum_{jk} A_{jk}(e_i)_k e_j = \sum_j A_{ji} e_j. \tag{11.130}$$

Nous avons alors

$$e^*_{\sigma(i)}\big(f_A(e_i)\big) = \sum_j A_{ji} \underbrace{e^*_{\sigma(i)}(e_j)}_{\delta_{j\sigma(i)}} = A_{\sigma(i)i}. \tag{11.131}$$

Au final,

$$\det(f_A) = \sum_{\sigma} \epsilon(\sigma) \prod_{i=1}^{n} A_{\sigma(i)i} = \det(A^t) = \det(A) \tag{11.132}$$

où la dernière égalité est autorisée par le lemme 4.70.

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 4.65 qui donne $f_{AB} = f_A \circ f_B$, et ensuite de la proposition 11.52(1) qui donne $\det(f_A \circ f_B) = \det(f_A)\det(f_B)$. □

11.3.4 Déterminant de Vandermonde

Proposition 11.54 ([57]).
*Le **déterminant de Vandermonde** est le polynôme en n variables donné par*

$$V(T_1,\dots,T_n) = \det\begin{pmatrix} 1 & 1 & \dots & 1 \\ T_1 & T_2 & \dots & T_n \\ \vdots & \ddots & \ddots & \vdots \\ T_1^{n-1} & T_2^{n-1} & \dots & T_n^{n-1} \end{pmatrix} = \prod_{1\leqslant i<j\leqslant n} (T_j - T_i). \tag{11.133}$$

Notez que l'inégalité du milieu est stricte (sinon d'ailleurs l'expression serait nulle).

Démonstration. Nous considérons le polynôme

$$f(X) = V(T_1,\dots,T_{n-1},X) \in \big(\mathbb{K}[T_1,\dots,T_{n-1}]\big)[X]. \tag{11.134}$$

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 conséquent il existe $\alpha \in \mathbb{K}[T_1,\dots,T_{n-1}]$ tel que

$$f = \alpha(X - T_{n-1})\dots(X - T_1). \tag{11.135}$$

Nous trouvons α en écrivant $f(0)$. D'une part la formule (11.135) nous donne

$$f(0) = \alpha(-1)^{n-1} T_1 \dots T_{n-1}. \tag{11.136}$$

D'autre par la définition donne

$$f(0) = \det \begin{pmatrix} 1 & \cdots & 1 & 1 \\ T_1 & & T_{n-1} & 0 \\ \vdots & & \vdots & \vdots \\ T_1^{n-1} & \cdots & T_{n-1}^{n-1} & 0 \end{pmatrix} \tag{11.137a}$$

$$= (-1)^{n-1} \det \begin{pmatrix} T_1 & \ldots & T_{n-1} \\ \vdots & \ddots & \vdots \\ T_1^{n-1} & \ldots & T_{n-1}^{n-1} \end{pmatrix} \tag{11.137b}$$

$$= (-1)^{n-1} T_1 \ldots T_{n-1} \det \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ T_1^{n-1} & \cdots & T_{n-1}^{n-1} \end{pmatrix} \tag{11.137c}$$

$$= (-1)^{n-1} T_1 \ldots T_{n-1} V(T_1, \ldots, T_{n-1}) \tag{11.137d}$$

En égalisant avec (11.136), nous trouvons $\alpha = V(T_1, \ldots, T_{n-1})$, et donc

$$f = V(T_1, \ldots, T_{n-1}) \prod_{j \leqslant n-1} (X - T_j) \tag{11.138}$$

Enfin, une récurrence montre que

$$V(T_1, \ldots, T_n) = f(T_n) \tag{11.139a}$$

$$= V(T_1, \ldots, T_{n-1}) \prod_{j \leqslant n-1} (T_n - T_j) \tag{11.139b}$$

$$= \prod_{k \leqslant n} \prod_{j \leqslant k-1} (T_k - T_j) \tag{11.139c}$$

$$= \prod_{1 \leqslant j < k \leqslant n} (T_i - T_j). \tag{11.139d}$$

□

Exemple 11.55
Le déterminant de Vandermonde (proposition 11.54) 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. △

Proposition 11.56.
Un polynôme semi-symétrique $f \in \mathbb{K}[T_1, \ldots, T_n]$ se décompose de façon unique en

$$f = P + VQ \tag{11.140}$$

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 $\{1, \ldots, n\}$, alors $\sigma_1 \cdot f = \sigma_2 \cdot f$ parce que l'élément $\sigma_2^{-1}\sigma_1$ est pair (proposition 2.73), 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

$$g = \tau \cdot f = P - VQ. \tag{11.141}$$

Donc $f+g=2P$ et $f-g=2VQ$. Cela donne P et Q en terme 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,

$$\sigma\cdot(f+g)=\sigma\cdot f+\sigma\tau\cdot f=g+f \tag{11.142}$$

parce que $\sigma\tau$ est pair. De la même façon,

$$\sigma\cdot(f-g)=g-f=\epsilon(\sigma)(f-g). \tag{11.143}$$

Dans les deux cas nous concluons en utilisant le fait que toute permutation est un produit de transpositions (proposition 2.70) et que ϵ est un homomorphisme.

Soient maintenant deux entiers $h<k$ dans $\{1,\dots,n\}$ et l'anneau

$$\big(\mathbb{K}[T_1,\dots,\hat{T}_k,\dots,T_n]\big)[T_k]. \tag{11.144}$$

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 :

$$f-g=(T_k-T_h)q+r \tag{11.145}$$

où $\deg_{T_k} r<1$, c'est-à-dire que r ne dépends pas de T_k. Nous revoyons maintenant l'égalité (11.145) 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

$$-(f-g)=-(T_k-T_h)\tau_{kh}\cdot q+\tau_{kh}\cdot r \tag{11.146}$$

où $\tau_{kh}\cdot r$ ne dépend pas de T_h. Nous appliquons à (11.146) l'application

$$\begin{aligned} t\alpha\colon\mathbb{K}[T_1,\dots,T_n]&\to\mathbb{K}[T_1,\dots,\hat{T}_k,\dots,T_n]\\ \alpha(PT_1,\dots,\hat{T}_k,\dots,T_n)&=P(T_1,\dots,T_h,\dots,T_n).\end{aligned} \tag{11.147}$$

Cette application vérifie $\alpha\big(\tau_{kh}\cdot r\big)=\alpha(r)$ et nous avons

$$-\alpha(f-g)=\alpha(r). \tag{11.148}$$

Puis en appliquant α à la relation $f-g=(T_k-T_h)q+r$, nous trouvons

$$\alpha(f-g)=\alpha(r), \tag{11.149}$$

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

$$f-g=2Q\prod_{h<k}\prod_{k\leqslant n}(T_k-T_h)=2Q(T_1,\dots,T_n)V(T_1,\dots,T_n), \tag{11.150}$$

où nous avons utilisé la formule du déterminant de Vandermonde de la proposition 11.54.

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

$$\sigma\cdot(f-g)=\epsilon(\sigma)(f-g)=\epsilon(\sigma)2QV, \tag{11.151}$$

Mais en appliquant σ à l'équation (11.150),

$$\sigma \cdot (f-g) = 2(\sigma \cdot V)(T_1,\dots,,T_n)(\sigma \cdot Q)(T_1,\dots,T_n) \tag{11.152a}$$
$$= 2\epsilon(\sigma)V(T_1,\dots,T_n)(\sigma \cdot Q)(T_1,\dots,T_n). \tag{11.152b}$$

Nous égalisons cela avec (11.151) et nous souvenant que l'anneau $\mathbb{K}[T_1,\dots,T_n]$ est intègre par le théorème 3.157. Ensuite nous simplifions par $2\epsilon(\sigma)V$ pour obtenir

$$Q = \sigma \cdot Q, \tag{11.153}$$

c'est-à-dire que Q est symétrique.

Au final nous avons $f+q = 2P$ et $f-g = 2VQ$ avec P et Q symétriques. En faisant la somme,

$$f = P + VQ. \tag{11.154}$$

□

11.3.5 Déterminant de Gram

Si $x_1,\dots,x_r$ sont des vecteurs d'un espace vectoriel, alors le **déterminant de Gram** est le déterminant

$$G(x_1,\dots,x_r) = \det\big(\langle x_i, x_j\rangle\big). \tag{11.155}$$

Notons que la matrice est une matrice symétrique.

Proposition 11.57.
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

$$d(x,F)^2 = \frac{G(x,x_1,\dots,x_n)}{G(x_1,\dots,x_n)}. \tag{11.156}$$

11.3.6 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

$$D_n = \det\left(\frac{1}{a_i+b_j}\right). \tag{11.157}$$

Proposition 11.58 ([143])**.**
Le déterminant de Cauchy est donné par la formule

$$D_n = \frac{\prod_{i<j}(a_j-a_i)\prod_{i<j}(b_j-b_i)}{\prod_{ij}(a_i+b_j)}. \tag{11.158}$$

11.3.7 Matrice de Sylvester

La définition est pompée de wikipédia. Soient P et Q deux polynômes non nuls, de degrés respectifs m et n :

$$P(x) = p_0 + p_1x + \cdots + p_nx^n \tag{11.159a}$$
$$Q(x) = q_0 + q_1x + \cdots + q_mx^m. \tag{11.159b}$$

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 :

$$\begin{pmatrix} p_n & p_{n-1} & \cdots & p_1 & p_0 & 0 & \cdots & 0 \end{pmatrix}; \tag{11.160}$$

(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 :

$$\begin{pmatrix} q_m & q_{m-1} & \cdots & q_1 & q_0 & 0 & \cdots & 0 \end{pmatrix}; \tag{11.161}$$

(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

$$S_{p,q} = \begin{pmatrix} p_4 & p_3 & p_2 & p_1 & p_0 & 0 & 0 \\ 0 & p_4 & p_3 & p_2 & p_1 & p_0 & 0 \\ 0 & 0 & p_4 & p_3 & p_2 & p_1 & p_0 \\ q_3 & q_2 & q_1 & q_0 & 0 & 0 & 0 \\ 0 & q_3 & q_2 & q_1 & q_0 & 0 & 0 \\ 0 & 0 & q_3 & q_2 & q_1 & q_0 & 0 \\ 0 & 0 & 0 & q_3 & q_2 & q_1 & q_0 \end{pmatrix}. \tag{11.162}$$

Le déterminant de la matrice de Sylvester associée à P et Q est appelé le **résultant** de P et Q et noté $\operatorname{res}(P, Q)$.

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 11.59 ([144]).
Si P et Q sont deux polynômes de degrés n et m à coefficients dans l'anneau $\mathbb{A}$, alors pour tout $\lambda \in \mathbb{A}$,

$$\operatorname{res}(\lambda P, Q) = \lambda^m \operatorname{res}(P, Q) \tag{11.163a}$$
$$\operatorname{res}(P, \lambda Q) = \lambda^n \operatorname{res}(P, Q). \tag{11.163b}$$

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. □

L'équation de Bézout (6.71) peut être traitée avec une matrice de Sylvester. Soient P et Q, deux polynômes donnés et à résoudre l'équation

$$xP + yQ = 0 \tag{11.164}$$

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 (11.164) sous la forme

$$S_{PQ}^t \begin{pmatrix} \tilde{x} \\ \tilde{y} \end{pmatrix} = 0. \tag{11.165}$$

Pour s'en convaincre, écrivons pour les polynômes de l'exemple (11.162) :

$$\begin{pmatrix} p_4 & 0 & 0 & q_3 & 0 & 0 & 0 \\ p_3 & p_4 & 0 & q_2 & q_3 & 0 & 0 \\ p_2 & p_3 & p_4 & q_1 & q_2 & q_3 & 0 \\ p_1 & p_2 & p_3 & q_0 & q_1 & q_2 & q_3 \\ p_0 & p_1 & p_2 & 0 & q_0 & q_1 & q_2 \\ 0 & p_0 & p_1 & 0 & 0 & q_0 & q_1 \\ 0 & 0 & p_0 & 0 & 0 & 0 & q_0 \end{pmatrix} \begin{pmatrix} x_2 \\ x_1 \\ x_0 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{pmatrix} = \begin{pmatrix} x_2p_4 + y_2q_3 \\ p_3x_2 + p_4x_1 + q_2y_3 + q_3y_2 \\ \\ \\ \vdots \end{pmatrix} \tag{11.166}$$

Nous voyons que sur la ligne numéro k (en partant du bas et en numérotant de à partir de zéro) nous avons les produits p_ix_j et q_iy_j avec $i + j = k$. La colonne de droite représente donc bien les coefficients du polynôme $xP + yQ$.

Proposition 11.60.
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 21.95 sur l'intégration de fractions rationnelles.

Exemple 11.61
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

$$S_{P,P'} = \begin{pmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{pmatrix}. \tag{11.167}$$

Le résultant est alors

$$\operatorname{res}(P, P') = -a(b^2 - 4ac). \tag{11.168}$$

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. △

La matrice de Sylvester permet aussi de récrire l'équation de Bézout pour les polynômes ; voir le théorème 6.40 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 11.62.
Si

$$P(X) = a_p \prod_{i=1}^{p} (X - \alpha_i) \tag{11.169a}$$

$$Q(X) = b_q \prod_{j=1}^{q} (X - \beta_i) \tag{11.169b}$$

alors nous avons les expressions suivantes pour le résultant :

$$\operatorname{res}(P, Q) = a_p^q b_q^p \prod_{i=1}^{p} \prod_{j=1}^{q} (\beta_j - \alpha_i) = b_q^p \prod_{j=1}^{q} P(\beta_j) = (-1)^{pq} a_p^q \prod_{i=1}^{p} Q(\alpha_i). \tag{11.170}$$

Démonstration. Si P et Q ne sont pas premiers entre eux, d'une part la proposition 11.60 nous dit que $\operatorname{res}(P, Q) = 0$ 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 (11.170) 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

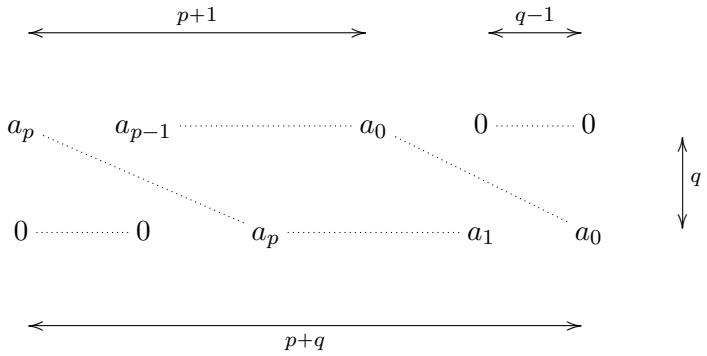
$$\mathbb{A} = \mathbb{Z}[\alpha_1, \ldots, \alpha_p, \beta_1, \ldots, \beta_q]. \tag{11.171}$$

Dans cet anneau, l'élément $\beta_j - \alpha_i$ est irréductible (tout comme $X - Y$ est irréductible dans $\mathbb{Z}[X, Y]$). Le résultant $R = \operatorname{res}(P, Q)$ 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

$$R = \lambda(\alpha_1, \ldots, \beta_q) \prod_{i=1}^{p} \prod_{j=1}^{r} (\beta_j - \alpha_i). \tag{11.172}$$

Comptons les degrés. Pour donner une idée de ce calcul de degré, voici comment se présente, au niveau des dimensions, le déterminant :



(11.173)

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 (11.173). Le même raisonnement montre que R est de degré p en les β_j. Par ailleurs le polynôme $\prod_{i=1}^{p}\prod_{j=1}^{r}(\beta_j-\alpha_i)$ 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 11.59 nous permet de conclure.

□

11.3.8 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

$$P=X^n+\sum_{k=0}^{n-1}a_kX^k. \tag{11.174}$$

Théorème 11.63 (Kronecker[43])**.**
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 $R=X^n+\sum_{k=0}^{n-1}b_kX^k$ un élément de K_n dont nous notons $\beta_1,\dots,\beta_n$ les racines dans $\mathbb{C}$. Les relations coefficients-racines stipulent que

$$b_k=\sum_{1\leqslant i_1<\dots<i_{n-k}\leqslant n}\prod_{j=1}^{n-k}\beta_{i_j}. \tag{11.175}$$

En prenant le module et en se souvenant que $|\beta_l|\leqslant 1$ pour tout l, nous trouvons que

$$|b_k|\leqslant\binom{n}{n-k}. \tag{11.176}$$

Mais comme $b_k\in\mathbb{Z}$, nous avons

$$b_k\in\Big\{-\binom{n}{n-k},-\binom{n}{n-k}+1,\dots,0,\cdots,\binom{n}{n-k}\Big\} \tag{11.177}$$

qui est de cardinal $\binom{n}{n-k}+1$. Nous avons donc

$$\text{Card}(K_n) \leqslant \prod_{k=0}^{n-1}\left(1+\binom{n}{n-k}\right) < \infty. \tag{11.178}$$

La conclusion jusqu'ici est que K_n est un ensemble fini.

Pour chaque $k \in \mathbb{N}^*$ nous considérons les polynômes

$$P_k = \prod_{i=1}^{n}(X-\alpha_i^k) \tag{11.179a}$$

$$Q_k = X^k - Y \in \mathbb{Z}[X,Y], \tag{11.179b}$$

et puis nous considérons le résultant $R_k = \text{res}_X(P,Q_k) \in \mathbb{Z}[Y]$:

$$R_k = \text{res}_X(P,Q_k) = \begin{pmatrix} 1 & a_{n-1} & \cdots & a_0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & a_{n-1} & \cdots & a_0 & 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & & & \\ 0 & \cdots & 0 & 1 & a_{n-1} & \cdots & a_0 & 0 & 0 \\ 0 & \cdots & 0 & 0 & 1 & a_{n-1} & \cdots & a_0 & 0 \\ 0 & \cdots & 0 & 0 & 0 & 1 & a_{n-1} & \cdots & a_0 \\ 1 & 0 & \ldots & 0 & -Y & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & -Y & 0 & \ldots & 0 \\ & & \ddots & & & \ddots & \ddots & & \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 & -Y & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 & -Y \end{pmatrix} \tag{11.180}$$

Cela est un polynôme en Y dont le terme de plus haut degré est $(-1)^nY^n$. Les petites formules de la proposition 11.62 nous permettent d'exprimer $R_k(Y)$ en termes des racines de P :

$$R_k(Y) = \prod_{i=1}^{n}Q_k(\alpha_i) = \prod_{i=1}^{n}(\alpha_i^k - Y) = (-1)^n\prod_{i=1}^{n}(Y-\alpha_i^k) = (-1)^nP_k(Y). \tag{11.181}$$

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) [19]. 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

$$\alpha^{2^l/2^k} = \alpha^{2^{l-k}} \tag{11.182}$$

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 (11.182) est racine de P_{2^l}, il est aussi racine de P_{2^k}. Donc

$$\left(\alpha^{2^{l-k}}\right)^{2^{l-k}} = \alpha^{2^{2(l-k)}} \tag{11.183}$$

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

$$\alpha^{2^{n(l-k)}} = \alpha^{2^{m(l-k)}} \tag{11.184}$$

pour certains entiers $m > n$, alors

$$\alpha^{2^{n(l-k)}-2^{m(l-k)}} = 1, \tag{11.185}$$

ce qui prouver 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. □

19. Ici dans [43], il déduit qu'on a un k tel que $P_k = P_1 = P$. Mois 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.

11.4 Orientation

11.4.1 Cas vectoriel

Proposition-définition 11.64 ([145]).
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 $\det_{\mathcal{B}}(\mathcal{B}') > 0$ [20].

Cela est une relation d'équivalence [21] *sur l'ensemble des bases de E, et les classes sont les* ***orientations*** *de E.*

Démonstration. Tout est dans le lemme 11.48. 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

$$\det_{\mathcal{B}}(\mathcal{B}'') = \det_{\mathcal{B}}(\mathcal{B}') \det_{\mathcal{B}'}(\mathcal{B}''), \tag{11.186}$$

nous voyons que $\det_{\mathcal{B}}(\mathcal{B}'') > 0$.

□

Lemme 11.65.
Soit un espace vectoriel réel E. L'ensemble des bases de E possède exactement deux orientations [22]

Démonstration. Nous considérons une base $\mathcal{B} = (e_1, \dots, e_n$ [23] 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 (11.106),

$$\underbrace{\det_{\mathcal{B}}(\mathcal{B}'')}_{<0} = \underbrace{\det_{\mathcal{B}}(\mathcal{B}')}_{<0} \det_{\mathcal{B}'}(\mathcal{B}''), \tag{11.187}$$

et nous déduisons que $\det_{\mathcal{B}'}(\mathcal{B}'') > 0$.

□

11.66.
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 11.67 ([145]).
Si $\mathcal{B}$ est une base de l'espace vectoriel E de dimension n, et si τ est une transposition [24] *de S_n, alors la base $\tau(\mathcal{B})$ est de sens contraire.*

20. Définition 11.46.
21. Définition 1.23.
22. Définition 11.64.
23. Nous notons (e_1, e_2) et non $\{e_1, e_2\}$ parce que l'ordre est important.
24. Définition 2.61.

Démonstration. Le lemme 11.48(2) dit que $\det_{\mathcal{B}}$ est une forme anti-symétrique ; donc

$$\det_{\mathcal{B}}(\mathcal{B}') = -\det_{\mathcal{B}}\big(\tau(\mathcal{B})'\big). \tag{11.188}$$

Si l'un est positif, l'autre est négatif. Elles ont donc des orientations contraires. □

Corollaire 11.68.
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 2.71). 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 11.69 ([145])**.**
Soit un espace vectoriel réel, et un endomorphisme f de E. Deux définitions.

*(1) L'endomorphisme f est **direct** si sont déterminant est strictement positif.*

*(2) L'endomorphisme **préserve l'orientation** si il transforme toutes base de E en une base de même orientation.*

Un endomorphisme est direct si et seulement si il préserve l'orientation.

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 11.52(2). Donc u transforme une base en une base par le lemme 4.7.

La définition 11.50 du déterminant de u est que

$$\det(u) = \det_{\mathcal{B}}\big(u(\mathcal{B})\big) > 0. \tag{11.189}$$

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,

$$0 < \det_{\mathcal{B}}\big(u(\mathcal{B})\big) = \det(u). \tag{11.190}$$

□

11.4.2 Cas affine

Définition 11.70.
Soit un espace affine $\mathcal{E}$ modelé sur E. Les repères cartésiens[25] *$(O, \mathcal{B})$ 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 $f : \mathcal{E} \to \mathcal{E}$ **préserve l'orientation** si sa partie linéaire*[26] *préserve l'orientation.*

25. Définition 10.5.
26. Définition 10.9.

11.5 Hermitien, orthogonal, adjoint

Proposition-définition 11.71 (Définition de la transposée[1]).
Soient deux espaces vectoriels euclidiens ou hermitiens E et F et une application linéaire $A\colon E \to F$.

(1) Il existe une unique application linéaire $B\colon F \to E$ telle que

$$\langle Ax, y\rangle_F = \langle x, By\rangle_E \tag{11.191}$$

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

$$B_{i\alpha} = A_{\alpha i}. \tag{11.192}$$

*L'application B ainsi définie set nommée **adjoint** de A et sera notée $B = A^*$.*

Démonstration. Pour l'unicité, nous écrivons la condition avec $x = e_j$ pour obtenir :

$$\langle Ae_j, y\rangle = \langle e_j, By\rangle = (By)_j \tag{11.193}$$

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

$$B(y) = \sum_j \langle Ae_j, y\rangle e_j \tag{11.194}$$

fonctionne. Pour cela il faut utiliser la bilinéarité du produit scalaire et le fait que $\langle x, e_j\rangle = x_j$. Nous avons :

$$\langle x, B(y)\rangle = \langle x, \sum_j \langle A(e_j), y\rangle e_j\rangle \tag{11.195a}$$

$$= \sum_j \langle A(e_j), y\rangle\langle x, e_j\rangle \tag{11.195b}$$

$$= \sum_j \langle A(x_j e_j), y\rangle \tag{11.195c}$$

$$= \langle A(x), y\rangle. \tag{11.195d}$$

En ce qui concerne la matrice de l'application B ainsi définie, nous écrivons la condition (11.191) avec $y = e'_\alpha$ et $x = e_i$, de telle sorte que

$$A(x) = A(e_i) = \sum_\beta A_{\beta i} e'_\beta \tag{11.196}$$

et

$$B(y) = B(e'_\alpha) = \sum_j B_{j\alpha} e_j. \tag{11.197}$$

Alors nous avons :

$$\sum_\beta A_{\beta i}\langle e'_\beta, e'_\alpha\rangle = \sum_j B_{j\alpha}\langle e_i, e_j\rangle, \tag{11.198}$$

donc

$$A_{\alpha i} = B_{i\alpha}. \tag{11.199}$$

□

11.72.
À cause de l'expression (11.192) 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 $A^t\colon F^* \to E^*$ donnée par la définition 4.118. Il nous arrivera donc d'écrire des égalités comme $\langle Ax, y\rangle = \langle x, A^t y\rangle$.

Proposition 11.73.
En ce qui concerne le déterminant,

$$\det(A^*) = \det(A)^* \tag{11.200}$$

où l'étoile à droite dénote la conjugaison complexe dans $\mathbb{C}$.

Démonstration. Écrivons l'expression explicite (11.102) du déterminant. Le tout avec la base canonique :

$$\det(A) = \det_{(e_1,\dots,e_n)}(Ae_1,\dots,Ae_n) = \sum_{\sigma\in S_n}\epsilon(\sigma)\prod_{i=1}^{n} e^*_{\sigma(i)}(Ae_i). \tag{11.201}$$

Mais nous pouvons développer :

$$e^*_{\sigma(i)}(Ae_i) = \langle e_{\sigma(i)}, Ae_i\rangle = \langle A^*e_{\sigma(i)}, e_i\rangle = \langle e_i, A^*e_{\sigma(i)}\rangle^* = e_i^*(A^*e_{\sigma(i)})^*. \tag{11.202}$$

Notez que dans la dernière expression, les trois * ont trois significations différentes. Par conséquent,

$$\det(A) = \sum_{\sigma\in S_n}\epsilon(\sigma)\prod_{i=1}^{n} e_i^*(A^*e_{\sigma(i)})^*. \tag{11.203}$$

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 :

$$\det(A) = \sum_{\sigma\in S_n}\epsilon(\sigma)\prod_{i=1}^{n} e^*_{\sigma(i)}(A^*e_i)^* = \det(A^*)^*. \tag{11.204}$$

Nous avons donc $\det(A) = \det(A^*)^*$, c'est-à-dire $\det(A)^* = \det(A^*)$. Pour information, la dernière étoile est la conjugaison complexe. □

Proposition 11.74 ([1]).
Si $A\colon E_2 \to E_3$ *et* $B\colon E_1 \to E_2$ *sont des applications linéaires, alors*

$$(AB)^* = B^*A^* \tag{11.205}$$

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 11.71 ne souffre pas de discussions. La propriété que $(AB)^*$ est unique a avoir est que

$$\langle ABx, y\rangle = \langle x, (AB)^*y\rangle \tag{11.206}$$

pour tout $x \in E_1$ et $y \in E_3$. Or l'application B^*A^* possède également cette propriété parce que

$$\langle x, B^*A^*y\rangle = \langle Bx, A^*y\rangle = \langle ABx, y\rangle. \tag{11.207}$$

La partie unicité de la proposition 11.71 nous impose donc d'accepter que les applications $(AB)^*$ et B^*A^* sont en réalité les mêmes [27]. □

11.75.
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 21.9.

Définition 11.76.
Un opérateur A *est* ***hermitien*** *si* $A^* = A$. *On dit aussi* ***autoadjoint***.

27. Et ce même si vous croyez les avoir déjà vu ensemble dans la même pièce.

11.77.
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 $\mathrm{S}(E)$. Cette notation provient du fait que dans $\mathbb{R}^n$ muni du produit scalaire usuel, les opérateurs autoadjoints sont les matrices symétriques.

Remarque 11.78.
Le fait d'être hermitien n'implique en rien le fait d'être inversible.

Lemme 11.79.
Si E est un espace euclidien, un endomorphisme $f\colon E \to E$ 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

$$\langle f(x), y\rangle = \langle x, f^*(y)\rangle = \langle x, f(y)\rangle. \tag{11.208}$$

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 11.71(1) spécifie que f^* est l'unique endomorphisme à satisfaire cette égalité. Donc $f = f^*$. □

11.5.1 Opérateur orthogonal, matrice orthogonale

Définition 11.80.
*Un opérateur est **orthogonal** lorsque $A^* = A^{-1}$ où A^* est l'adjoint de A définit en 11.71.*

Définition 11.81.
*Une matrice U est **orthogonale** si $U^t = U^{-1}$. Le **groupe orthogonal** noté $\mathrm{O}(n)$ est l'ensemble des matrices orthogonales $n \times n$.*

Lemme 11.82.
Soit un opérateur $A\colon \mathbb{R}^n \to \mathbb{R}^n$ muni du produit scalaire usuel. Il est orthogonal si et seulement si sa matrice dans la base canonique est orthogonale[28].

Démonstration. Soit la base canonique $\{e_i\}_{i=1,\dots,n}$ de $\mathbb{R}^n$. Nous avons

$$\langle AA^*e_i, e_j\rangle = \langle e_i, e_j\rangle = \delta_{ij}, \tag{11.209}$$

donc $\big((AA^*)e_i\big)_j = \delta_{ij}$, ou encore $(AA^*)_{ij} = \delta_{ij}$, ce qui signifie que la matrice AA^* est l'identité. □

Proposition 11.83 (Thème 64)**.**
À propos de matrices orthogonales.

(1) L'ensemble des matrices réelles orthogonales forme un groupe noté $\mathrm{O}(n, \mathbb{R})$.

(2) Si A est une matrice orthogonale, alors $\det(A) = \pm 1$.

(3) Le groupe $\mathrm{O}(n)$ est le groupe des isométries linéaires[29] *de $\mathbb{R}^n$.*

Démonstration. Si A et B sont orthogonales, alors

$$(AB)(AB)^t = ABB^tA^t = A\mathbb{1}A^t = \mathbb{1}. \tag{11.210}$$

Vu que $\mathbb{1}$ est orthogonale, nous avons bien un groupe.

28. Définition 11.81.

29. Au sens où, parmi les applications linéaires, les isométries sont les éléments de $\mathrm{O}(n)$. À part ça, il y a aussi les translations, mais c'est une autre histoire qui vous sera contée une autre fois.

En ce qui concerne le déterminant, $AA^t = \mathbb{1}$ donne $\det(A)\det(A^t) = 1$, mais la proposition 11.73 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,

$$\langle A^t Ax, y\rangle = \langle x, y\rangle \tag{11.211}$$

pour tout $x, y \in \mathbb{R}^n$. En prenant $y = e_i$ nous trouvons

$$(A^t Ax)_i = x_i, \tag{11.212}$$

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

$$\langle x, y\rangle = \langle A^t Ax, y\rangle = \langle Ax, Ay\rangle, \tag{11.213}$$

ce qui prouve que A est une isométrie. □

En ce qui concerne les valeurs propres des matrices de $\mathrm{O}(n)$ ainsi que leurs formes canoniques (avec des fonctions trigonométriques) pour $\mathrm{O}(3)$ et $\mathrm{SO}(3)$, ce sera pour la proposition 19.184 et ce qui s'ensuit.

Définition 11.84.
Le sous-groupe des matrices orthogonales de déterminant 1 *est le groupe* ***spécial orthogonal*** *noté* $\mathrm{SO}(n)$.

11.6 Topologie

11.6.1 Boules et sphères

Définition 11.85.
Soit $(V, \|.\|)$, *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*** $\bar{B}(a, r) = \{x \in V \text{ tel que } \|x - a\| \leqslant r\}$;

(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

$$\bar{B}(a, r) = B(a, r) \cup S(a, r). \tag{11.214}$$

Définition 11.86.
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 11.87
Dans $\mathbb{R}$, les boules sont les intervalles ouverts et fermés tandis que la sphère est donnée par les points extrêmes des intervalles :

$$\begin{aligned} B(a, r) &=]a - r, a + r[, \\ \bar{B}(a, r) &= [a - r, a + b], \\ S(a, r) &= \{a - r, a + r\}. \end{aligned} \tag{11.215}$$

△

Exemple 11.88
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 $\|.\|_1$, $\|.\|_2$ et $\|.\|_\infty$.

Pour la norme $\|.\|_1$, la sphère de rayon r est donnée par l'équation

$$|x| + |y| = r. \tag{11.216}$$

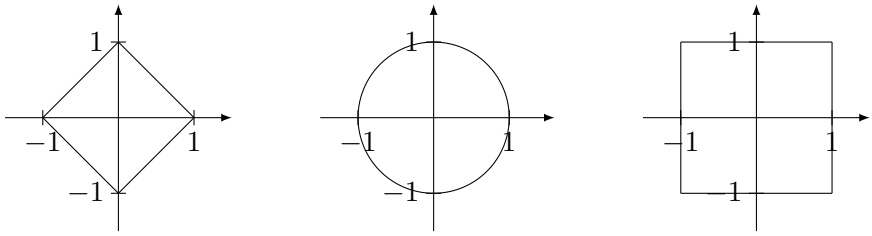
Pour la norme $\|.\|_2$, l'équation de la sphère de rayon r est

$$\sqrt{x^2 + y^2} = r, \tag{11.217}$$

et pour la norme supremum, la sphère de rayon r a pour équation

$$\max\{|x|, |y|\} = r. \tag{11.218}$$

Elles sont dessinées sur la figure 11.1



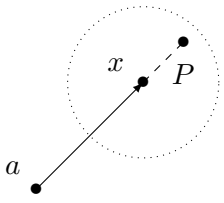
(a) La sphère unité pour la norme $\|.\|_1$ (b) La sphère unité pour la norme $\|.\|_2$ (c) La sphère unité pour la norme $\|.\|_\infty$

FIGURE 11.1 – Les sphères de rayon 1 pour les trois normes classiques.

△

Proposition 11.89.
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 :



Plus précisément, nous considérons le point

$$P = x + \frac{v}{N} \tag{11.219}$$

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

$$d(P,x) = \|P - x\| = \frac{\|v\|}{N} \tag{11.220}$$

peut être rendu aussi petit que l'on veut par un choix approprié de N. Montrons maintenant que $d(a,P) > d(a,x)$:

$$\begin{aligned} d(a,P) &= \|a - x - \frac{v}{N}\| \\ &= \|a - x + \frac{a}{N} - \frac{x}{N}\| \\ &= \|\big(1 + \frac{1}{N}(a-x)\big)\| \\ &> \|a - x\| = d(a,x). \end{aligned} \tag{11.221}$$

Nous laissons en exercice le soin de trouver un point Q tel que $d(Q,a) < r$ et $d(Q,x) < \delta$. □

11.6.2 Ouverts, fermés, intérieur et adhérence

Définition 11.90.
*Soit $(V, \|.\|)$ 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 11.91
Trouver l'intérieur d'un intervalle dans $\mathbb{R}$ consiste à « ouvrir là où c'est fermé ».

(1) $\text{Int}\big([0,1[\big) =]0,1[$.
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 11.2). Cela prouve que a est dans l'intérieur de $[0,1[$.

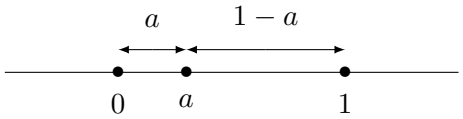


FIGURE 11.2 – Trouver le rayon d'une boule autour de a. Une boule qui serait centrée en a avec un rayon strictement plus petit à la fois de a et de $1-a$ est entièrement contenue dans le segment $]0,1[$.

Prouvons maintenant que $\text{Int}\big([0,1[\big) \subset]0,1[$. Vu que l'intérieur d'un ensemble est inclus dans l'ensemble, nous savons déjà que $\text{Int}\big([0,1[\big) \subset [0,1[$. 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) $\text{Int}\Big([0,\infty[\Big) =]0,\infty[$.

(3) $\text{Int}\big(]2,3[\big) =]2,3[$.

△

Exemple 11.92
Les intérieurs des boules et sphères sont importantes à savoir.

(1) $\text{Int}\big(B(a,r)\big) = B(a,r)$. Si $x \in B(a,r)$, nous avons $d(a,x) < r$. Alors la boule $B\big(x, r - d(x,a)\big)$ est incluse à $B(a,r)$, et donc x est dans l'intérieur de $B(a,r)$. Conseil : faire un dessin.

(2) $\text{Int}\big(\bar{B}(a,r)\big) = B(a,r)$. 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 11.89.

(3) $\text{Int}\big(S(a,r)\big) = \varnothing$. 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 11.93.
Une partie A de l'espace vectoriel normé $(V, \|.\|)$ 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 $\varnothing$ est ouvert.*

Une partie est dite ***fermée*** *si son complémentaire est ouvert. La partie A est donc fermée si $V \backslash A$ est ouverte.*

Remarque : un ensemble A est ouvert si et seulement si $\text{Int}(A) = A$.

Définition 11.94.
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 11.95
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 11.96.
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 inclues à V. Le vide est alors fermé (parce que son complémentaire est V).

(2) Soit une famille $(\mathcal{O}_i)_{i\in I}$ d'ouverts[30], et l'union

$$\mathcal{O} = \bigcup_{i\in I} \mathcal{O}_i. \tag{11.222}$$

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

30. L'ensemble I avec lequel nous « numérotons » 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.

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

$$\mathcal{O} = \bigcap_{k=1}^{n} \mathcal{O}_k. \tag{11.223}$$

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 inclue dans toutes les autres (parce que $B(a,r) \subset B(a,r')$ lorsque $r \leqslant r'$), par conséquent

$$B(a,r) \subset \bigcap_{k=1}^{n} B(a,r_k) \subset \bigcap_{k=1}^{n} \mathcal{O}_k = \mathcal{O}, \tag{11.224}$$

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 :

$$\bigcap_{i=1}^{\infty}]-\frac{1}{n},\frac{1}{n}[= \{0\}. \tag{11.225}$$

Chacun des ensembles $]-\frac{1}{n},\frac{1}{n}[$ est ouvert, mais le singleton $\{0\}$ est fermé (pourquoi ?).

Nous reportons à la proposition 1.122 la preuve du fait que tout ensemble borné de $\mathbb{R}$ possède un infimum et un supremum.

Définition 11.97.
*L'ensemble des ouverts de V est la **topologie** de V. La topologie dont nous parlons ici est dite **induite** par la norme $\|.\|$ 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 11.98
Les ensemble 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 $\mathbb{R}$:

— $]1,3[$;
— $]1,3]$;
— $[0,5[\backslash\{3\}$.

△

Proposition 11.99.
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 :

$$\bigcup_{n=1}^{\infty}[-1+\frac{1}{n},1-\frac{1}{n}]=]-1,1[. \tag{11.226}$$

Chacun des intervalles dont on prend l'union est fermé tandis que l'union est ouverte.

Définition 11.100.
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 $\varepsilon>0$,*

$$B(a,\varepsilon)\cap A\neq\emptyset. \tag{11.227}$$

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 11.101
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 $\bar{A}\subset A$. Cela est fondamentalement le sens de la définition 7.17.

(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 11.95.

△

Exemple 11.102
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. △

Exemple 11.103
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. △

Lemme 11.104.
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. □

Exemple 11.105
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) $\overline{]3,\infty]} = [3,\infty[$.

△

Proposition 11.106.
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 11.107.
Pour toute partie A d'un espace vectoriel normé nous avons

(1) $V\backslash\bar{A} = \text{Int}(V\backslash A)$,
(2) $V\backslash \text{Int}(A) = \overline{V\backslash A}$.

En utilisant les notations du complémentaire (1.1.4), 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 $a \in V\backslash\bar{A}$ 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 $B(a,\varepsilon) \subset V\backslash A$. Or cela est exactement la définition du fait que a est à l'intérieur de $V\backslash A$. Nous avons donc montré que $a \in V\backslash\bar{A}$ si et seulement si $a \in \text{Int}(V\backslash A)$. Cela prouve la première affirmation.

Pour prouver la seconde affirmation, nous appliquons la première au complémentaire de A : $\complement(\overline{\complement A}) = \text{Int}(\complement\complement A)$. En prenant le complémentaire des deux membres nous trouvons successivement

$$\begin{aligned} \complement\complement(\overline{\complement A}) &= \complement \text{Int}(\complement\complement A), \\ \overline{\complement A} &= \complement \text{Int}(A), \end{aligned} \tag{11.228}$$

ce qu'il fallait démontrer. □

Attention à ne pas confondre $\complement\bar{A}$ et $\overline{\complement A}$. Ces deux ensembles ne sont pas égaux. En effet, en tant que complément d'un fermé, l'ensemble $\complement\bar{A}$ est certainement ouvert, tandis que, en tant que fermeture, l'ensemble $\overline{\complement A}$ est fermé. Pouvez-vous trouver des exemples d'ensembles A tels que $\complement\bar{A} = \overline{\complement A}$?

Proposition 11.108.
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, $\overline{A \cup B} = \overline{A} \cup \overline{B}$ 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

$$\begin{aligned} B(a, \varepsilon_1) \cap A = \varnothing, \\ B(a, \varepsilon_2) \cap B = \varnothing. \end{aligned} \tag{11.229}$$

En prenant $r = \min\{\varepsilon_1, \varepsilon_2\}$, la boule $B(a, r)$ est inclue 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 $\complement A$ et $\complement B$, nous trouvons

$$\overline{\complement A \cup \complement B} = \overline{\complement A} \cup \overline{\complement B}. \tag{11.230}$$

En utilisant les propriétés du lemme 1.20, le membre de gauche devient

$$\overline{\complement A \cup \complement B} = \overline{\complement(A \cap B)} = \complement \operatorname{Int}(A \cap B), \tag{11.231}$$

tandis que le membre de droite devient

$$\overline{\complement A} \cup \overline{\complement B} = \complement \operatorname{Int}(A) \cup \complement \operatorname{Int}(A) = \complement\Big(\operatorname{Int}(A) \cap \operatorname{Int}(B)\Big). \tag{11.232}$$

En égalisant le membre de droite de (11.231) avec celui de (11.232) et en passant au complémentaire nous trouvons

$$\operatorname{Int}(A \cap B) = \operatorname{Int}(A) \cap \operatorname{Int}(B), \tag{11.233}$$

comme annoncé.

La dernière affirmation provient du fait que $\operatorname{Int}(A) \subset \operatorname{Int}(A \cup B)$ et de la propriété équivalente pour B.

□

Remarque 11.109.
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 $A \cap B = \varnothing$ et donc $\overline{A \cap B} = \varnothing$. Par contre nous avons $\bar{A} \cap \bar{B} = \{1\}$.

Définition 11.110.
*La **frontière** d'un sous-ensemble A de l'espace vectoriel normé V est l'ensemble des points $a \in V$ tels que*

$$\begin{aligned} B(a, r) \cap A \neq \varnothing, \\ B(a, r) \cap \complement A \neq \varnothing, \end{aligned} \tag{11.234}$$

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 11.111.
La frontière d'une partie A d'un espace vectoriel normé V s'exprime sous la forme

$$\partial A = \bar{A} \setminus \operatorname{Int}(A). \tag{11.235}$$

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 $\complement A$. □

La description de la frontière donnée par la proposition 11.111 est celle qu'en pratique nous utilisons le plus souvent. Dans certains textes, elle est prise comme définition de la frontière.

Lemme 11.112.
La frontière de A peut également s'exprimer des façons suivantes :

$$\partial A = \bar{A} \cap \complement \,\text{Int}(A) = \bar{A} \cap \overline{\complement A}, \tag{11.236}$$

Démonstration. En partant de $\partial A = \bar{A} \backslash \text{Int}(A)$, la première égalité est une application de la propriété (4) du lemme 1.20. La seconde égalité est alors la proposition 11.107. □

Exemple 11.113
Dans $\mathbb{R}$, la frontière d'un intervalle est la paire constituée des points extrêmes. En effet

$$\partial[a,b[= \overline{[a,b[} \backslash \text{Int}\left([a,b[\right) = [a,b] \backslash]a,b[= \{a,b\}. \tag{11.237}$$

Toujours dans $\mathbb{R}$ nous avons

$$\partial\mathbb{R} = \bar{\mathbb{R}} \backslash \text{Int}(\mathbb{R}) = \mathbb{R} \backslash \mathbb{R} = \varnothing, \tag{11.238}$$

et

$$\partial\mathbb{Q} = \bar{\mathbb{Q}} \backslash \text{Int}(\mathbb{Q}) = \mathbb{R} \backslash \varnothing = \mathbb{R}. \tag{11.239}$$

△

Exemple 11.114
Dans $\mathbb{R}^n$, nous avons

$$\partial B(a,r) = \partial \bar{B}(a,r) = S(a,r). \tag{11.240}$$

Cela est un boulot pour la proposition 11.89. Si $x \in S(a,r)$ alors tout 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 $d(a,x) \leqslant r$. 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 $d(a,x) \geqslant r$. Nous avons donc $d(a,x) = r$. △

Remarque 11.115.
Il serait toutefois faux de croire que $\partial A = \partial \bar{A}$ pour toute partie A de $\mathbb{R}^n$. En effet si $A = \mathbb{R}\backslash\{0\}$ nous avons $\partial A = \{0\}$ et $\bar{A} = \mathbb{R}$, donc $\partial \bar{A} = \varnothing$.

11.6.3 Point isolé, point d'accumulation

Définition 11.116.
Soit D, une partie de V.

*(1) Un point $a \in D$ est dit **isolé** dans D relativement à V s'il existe un $\varepsilon > 0$ tel que*

$$B(a,\varepsilon) \cap D = \{a\}. \tag{11.241}$$

*(2) Un point $a \in V$ est un **point d'accumulation** de D si pour tout $\varepsilon > 0$,*

$$\Big(B(a,\varepsilon) \backslash \{a\}\Big) \cap D \neq \varnothing. \tag{11.242}$$

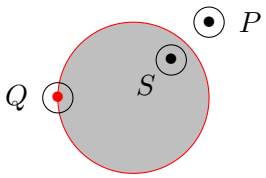


FIGURE 11.3 – L'ensemble décrit par l'équation (11.243). Le point P est un point isolé de D, tandis que les points S et Q sont des points d'accumulation.

Exemple 11.117
Considérons la partie suivante de $\mathbb{R}^2$:

$$D = \{(x, y) \text{ tel que } x^2 + y^2 < 1\} \cup \{(1, 1)\}. \tag{11.243}$$

Comme on peut le voir sur la figure 11.3, 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. △

Remarque 11.118.
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 11.119
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. △

Remarque 11.120.
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.

11.7 Valeur propre et vecteur propre

11.7.1 Généralités

Nous savons qu'une application *linéaire* $A\colon \mathbb{R}^3 \to \mathbb{R}^3$ est complètement définie par la donnée de son action sur les trois vecteurs de base, c'est-à-dire par la donnée de

$$Ae_1, \quad Ae_2 \quad \text{et} \quad Ae_3. \tag{11.244}$$

Nous allons former la matrice de A en mettant simplement les vecteurs Ae_1, Ae_2 et Ae_3 en colonne. Donc la matrice

$$A = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \tag{11.245}$$

signifie que l'application linéaire A envoie le vecteur e_1 sur $\begin{pmatrix}3\\0\\0\end{pmatrix}$, le vecteur e_2 sur $\begin{pmatrix}0\\0\\1\end{pmatrix}$ 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×matrice :

$$\begin{pmatrix}1&2&3\\4&5&6\\7&8&9\end{pmatrix}\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}x+2y+3z\\4x+5y+6z\\7x+8y+9z\end{pmatrix}. \tag{11.246}$$

Une chose intéressante est de savoir quelles sont les directions invariantes de la transformation linéaire. Par exemple, on peut lire sur la matrice (11.245) 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 récrit $(A-\lambda\mathbb{1})v=0$, c'est-à-dire qu'il faut résoudre l'équation

$$(A-\lambda\mathbb{1})\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}0\\0\\0\end{pmatrix}. \tag{11.247}$$

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.

11.7.2 Dans le vif du sujet

Définition 11.121.
Soit un $\mathbb{K}$-espace vectoriel E et un endomorphisme $A\colon V\to V$. 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*[31] *est l'ensemble des vecteurs propres de A pour la valeur propre λ et zéro.*

Définition 11.122.
L'ensemble de valeurs propres de l'endomorphisme u est son ***spectre*** *et est noté* $\mathrm{Spec}(u)$.

Remarque 11.123.
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 11.124.
Soit u un endomorphisme et $E_\lambda(u)$ ses espaces propres. La somme des V_λ est directe.

Démonstration. Soit $v_i\in V_{\lambda_i}$ un choix de vecteurs propres de u. Si la somme n'est pas directe, nous pouvons considérer une combinaison linéaire des v_i qui soit nulle :

$$v_1+\cdots+v_p=0. \tag{11.248}$$

Appliquons $(A-\lambda_1\mathbb{1})$ à cette égalité :

$$(\lambda_2-\lambda_1)v_1+\cdots+(\lambda_p-\lambda_1)v_p=0. \tag{11.249}$$

En appliquant encore successivement les opérateurs $(A-\lambda_i\mathbb{1})$ nous réduisons le nombre de termes jusqu'à obtenir $v_p=0$. □

31. Nous laissons au lecteur le soin de vérifier que c'est bien un sous-espace vectoriel de E.

Proposition 11.125 ([146]).
Soit E, un espace vectoriel sur un corps infini et $(F_k)_{k=1,\dots,r}$, des sous-espaces vectoriels propres[32] *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.

11.8 Polynômes d'endomorphismes

Soit A un anneau commutatif et $\mathbb{K}$, un corps commutatif. L'injection canonique $A \to A[X]$ se prolonge en une injection

$$\mathbb{M}(A) \to \mathbb{M}\big(A[X]\big). \tag{11.250}$$

11.8.1 Polynômes d'endomorphismes

Soit $u \in \mathrm{End}(E)$ où E est un $\mathbb{K}$-espace vectoriel. Nous considérons l'application

$$\begin{aligned} \varphi_u \colon \mathbb{K}[X] &\to \mathrm{End}(E) \\ P &\mapsto P(u). \end{aligned} \tag{11.251}$$

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 11.126.
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

$$(PQ)(u) = P(u) \circ Q(u). \tag{11.252}$$

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

$$\sum_l a_l b_{k-l}. \tag{11.253}$$

Par conséquent $(PQ)(u)$ contient $\sum_l a_l b_{k-l} u^k$. Par ailleurs $P(u) \circ Q(u)$ est donné par

$$\sum_i a_i u^i \left(\sum_j b_j u^j \right)(x) = \sum_{ij} a_i b_j u^{i+j}(x). \tag{11.254}$$

Le coefficient du terme en u^k est bien le même que celui donné par (11.253). □

Théorème 11.127 (Décomposition des noyaux ou lemme des noyaux).
Soit u un endomorphisme du $\mathbb{K}$-espace vectoriel E. Soit $P \in \mathbb{K}[X]$ un polynôme tel que $P(u) = 0$. Nous supposons que P s'écrive comme le produit $P = P_1 \dots P_n$ de polynômes deux à deux étrangers[33]*. Alors*

$$E = \ker P_1(u) \oplus \dots \oplus \ker P_n(u). \tag{11.255}$$

De plus les projecteurs associés à cette décomposition sont des polynômes en u.

Ce résultat est utilisé pour prouver que toute représentation est décomposable en représentations irréductibles, proposition 17.9 ainsi que pour le théorème 11.167 qui dit que si le polynôme minimal d'un endomorphisme est scindé à racine simple alors il est diagonalisable.

32. Définition 11.121.
33. Définition 3.164.

Démonstration. Nous posons

$$Q_i = \prod_{j \neq i} P_i. \tag{11.256}$$

Par le lemme 6.41 ces polynômes sont étrangers entre eux et le théorème de Bézout (théorème 6.40) donne l'existence de polynômes R_i tels que

$$R_1Q_1 + \cdots + R_nQ_n = 1. \tag{11.257}$$

Si nous appliquons cette égalité à u et ensuite à $x \in E$ nous trouvons

$$\sum_{i=1}^{n} (R_iQ_i)(u)(x) = x, \tag{11.258}$$

et en particulier si nous posons $E_i = \text{Image}\big(P_iQ_i(u)\big)$ nous avons

$$E = \sum_{i=1}^{n} E_i. \tag{11.259}$$

Cette dernière somme n'est éventuellement pas une somme directe. Si $i \neq j$, alors Q_iQ_j est multiple de P et nous avons, en utilisant le lemme 11.126,

$$(R_iQ_i)(u) \circ (R_jQ_j)(u) = \big(R_iQ_iR_jQ_j\big)(u) = S_{ij}(u) \circ P(u) = 0 \tag{11.260}$$

où S_{ij} est un polynôme.

Nous pouvons voir E comme un $\mathbb{K}$-module et appliquer le théorème 3.68. Les opérateurs $R_iQ_i(u)$ ont l'identité comme somme et sont orthogonaux, et nous avons donc la décomposition en somme directe :

$$E = \bigoplus_{i=1}^{n} R_iQ_i(u)E. \tag{11.261}$$

Afin de terminer la preuve, nous devons montrer que $R_iQ_i(u)E = \ker P_i(u)$. D'abord nous avons

$$P_iR_iQ_i(u) = (R_iP)(u) = R_i(u) \circ P(u) = 0, \tag{11.262}$$

par conséquent $\text{Image}(R_iQ_i(u)) \subset \ker P_i(u)$. Pour obtenir l'inclusion inverse, nous reprenons l'équation (11.258) avec $x \in \ker P_i(u)$. Elle se réduit à

$$(R_iQ_i)(u)x = x. \tag{11.263}$$

Par conséquent $x \in \text{Image}\big(R_iQ_i(u)\big)$. □

Corollaire 11.128.
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

$$F = \bigoplus_{i=1}^{r} \ker M_i^{\alpha_i}(f) \cap F \tag{11.264}$$

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 (11.127) s'applique et

$$E = E_1 \oplus \ldots \oplus E_r. \tag{11.265}$$

Nous pouvons décomposer $x \in F$ en termes de cette somme :

$$x = x_1 + \cdots + x_r \tag{11.266}$$

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 $\texttt{proj}_i : E \to E_i$, et en appliquant $\texttt{proj}_i$ à (11.266), $\texttt{proj}_i(x) = x_i$. Vu que $x \in F$, le membre de gauche est encore dans F et $x_i \in E_i \cap F$. Nous avons donc

$$F \subset \bigoplus_{i=1}^{r} F_i. \tag{11.267}$$

L'inclusion inverse est immédiate parce que $F_i \subset F$ pour chaque i. □

Lemme 11.129.
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 $P(X) = \sum_{k=0}^{n} c_k X^n$:

$$P(u)x = \sum_{k=0}^{n} c_k u^k(x) = \sum_{k=0}^{n} c_k \lambda^k u = P(\lambda)x. \tag{11.268}$$

□

11.8.2 Polynôme minimal et minimal ponctuel

Lemme-définition 11.130.
Soit un endomorphisme $f : E \to E$ d'un $\mathbb{K}$-espace vectoriel de dimension finie. Il existe un unique polynôme annulateur normalisé de degré minimum.

*Il est nommé le **polynôme minimal** de f et il est noté μ_f ou simplement μ lorsque la dépendance en f est claire.*

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, ... ne peuvent pas être tous linéairement indépendants parce que la dimension de $\mathrm{End}(E)$ 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.

Une autre façon de le dire est que l'application linéaire $\varphi : \mathbb{K}[X] \to \mathrm{End}(E)$ 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. □

Remarque 11.131.
La preuve donnée ci-dessus montre que $\deg(\mu) \leqslant \dim(E)^2$. Comme conséquence du théorème de Caley-Hamilton 11.154 nous verrons qu'en réalité le degré du polynôme minimal est majoré par la dimension de l'espace.

Exemple 11.132(Pas en dimension infinie)
L'endomorphisme de dérivation △

Dans la suite, l'endomorphisme f du $\mathbb{K}$-espace vectoriel E de dimension n est fixé. Pour $x \in E$ nous notons

$$E_x = \{P(f)x \text{ tel que } P \in \mathbb{K}[X]\}. \tag{11.269}$$

Nous considérons le morphisme d'algèbres

$$\begin{aligned} \varphi : \mathbb{K}[X] &\to \mathrm{End}(E) \\ P &\mapsto P(f) \end{aligned} \tag{11.270}$$

et si $x \in E$ est donné nous considérons le morphisme de $\mathbb{K}$-espaces vectoriels

$$\begin{aligned} \varphi_x : \mathbb{K}[X] &\to E \\ P &\mapsto P(f)x. \end{aligned} \tag{11.271}$$

Les noyaux de ces applications sont des idéaux, entre autres par le lemme 11.126. Ils ont donc un unique générateur unitaire (chacun) par le théorème 6.36. En termes de vocabulaire, l'ensemble

$$\ker(\phi) = \{Q \in \mathbb{K}[X] \text{ tel que } Q(f) = 0\} \tag{11.272}$$

est l'**idéal annulateur** de f et un polynôme Q tel que $Q(f) = 0$ est une polynôme annulateur de f.

Définition 11.133.
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 11.134(Pas en dimension infinie)
En dimension infinie, il n'y a pas toujours de polynôme annulateur. Si E est un espace vectoriel de dimension infine 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 soir.

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 16.63 donnera un habillage à peine subtil à cet exemple. △

Proposition 11.135.
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 $\ker(\varphi) = \{Q \in \mathbb{K}[X] \text{ tel que } Q(u) = 0\}$ est un idéal par le lemme 11.126. Le polynôme minimal de u est un élément de degré plus bas dans I et par conséquent $I = (\mu_u)$ par le théorème 6.36. Nous concluons que μ_u divise tous les éléments de I. □

La proposition suivante permet de caractériser le polynôme minimal.

Proposition 11.136 ([66]).
Soit une application linéaire f *sur un* $\mathbb{K}$*-espace vectoriel. Il existe un unique polynôme unitaire*[34] $P \in \mathbb{K}[X]$ *tel que*

(1) $P(f) = 0$;

(2) l'application

$$\begin{aligned}\varphi\colon \frac{\mathbb{K}[X]}{(P)} &\to \mathrm{End}(E)\\ \bar{Q} &\mapsto Q(f)\end{aligned} \tag{11.273}$$

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 (11.273) 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 6.36(3) nous dit alors que $P = \mu$ parce que μ est également générateur unitaire. □

Lemme 11.137 ([147]).
Soit $f\colon E \to E$ *un endomorphisme de l'espace vectoriel* E. *Il existe un élément* $x \in E$ *tel que* $\mu_{f,x} = \mu_f$.

34. À mon avis, « unitaire » manque dans [66].

Démonstration. Soit une décomposition en irréductibles du polynôme minimal $\mu = P_1^{\alpha_1}\dots P_r^{\alpha_r}$. Nous notons $E_i = \ker\big(P_i^{\alpha_i}(f)\big)$. 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 11.127 nous donne la somme directe

$$E = \bigoplus_{i=1}^{r} \ker\big(P_i^{\alpha_i}(f)\big). \tag{11.274}$$

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 $a = x_1 + \cdots + x_r$; par définition du polynôme annulateur μ_a, nous avons

$$0 = \mu_a(f)a = \mu_a(f)x_1 + \cdots + \mu_a(f)x_r. \tag{11.275}$$

Mais $m_a(f)x_j \in E_i$, et la somme des E_j est directe, donc l'annulation de la somme (11.275) 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 :

$$\prod_{i=1}^{r} \mu_{x_i} \mid \mu_a, \tag{11.276}$$

c'est-à-dire $\mu \mid \mu_a$. Comme nous avons aussi $\mu_a \mid \mu$, nous déduisons $\mu_a = \mu$. □

Définition 11.138 (Matrices, endomorphismes et vecteurs cycliques)**.**
Une matrice est ***cyclique*** *si elle est semblable à une matrice compagnon. Un endomorphisme $f\colon E \to E$ 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 11.139.
Soit E un espace vectoriel de dimension finie et un endomorphisme cyclique[35] *f de E. Soit un 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 11.135. 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

$$P(f)x = \big(P(f)\circ Q(f)\big)v = \big(Q(f)\circ P(f)\big)v = 0 \tag{11.277}$$

où nous avons utilisé le lemme 11.126. □

Lemme 11.140 ([147])**.**
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 $e_1 = a$, $e_2 = f(a)$,..., $e_l = k^{l-1}(a)$ forment une base de E_a. Nous pouvons la compléter en une base $\{e_1,\dots,e_n\}$ de E. Et nous posons[36]

$$G = \{x \in E \text{ tel que } e_l^*\big(f^k(x)\big) = 0\ \forall k \geqslant 0\} \tag{11.278a}$$
$$= \bigcap_{k\geqslant 0} \ker\{e_l^* \circ f^k\} \tag{11.278b}$$
$$= \bigcap_{k=0}^{l-1} \ker(e_l^* \circ f^k). \tag{11.278c}$$

35. Voir la définition 11.138.
36. ici, comme presque partout, e_l^* est le dual de e_l, c'est-à-dire l'application linéaire sur E donnée par $e_l^*(e_i) = \delta_{li}$.

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 $i \leqslant l-1$.

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 $f^j(a)$ $(j \leqslant l)$. 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

$$\sum_{j=0}^{l-1} \lambda_j \big(e_l^* \circ f^j\big) = 0 \tag{11.279}$$

et montrons que $\lambda_j = 0$ pour tout j est l'unique solution. Soit $x \in E$ et appliquons l'opération (11.279) au vecteur $f^i(x)$; le résultat est zéro :

$$0 = \sum_{j=0}^{l-1} \lambda_j (e_l^* \circ f^i \circ f^j) = (e_l^* \circ f^i)P(u) \tag{11.280}$$

où nous avons posé $P(X) = \sum_{j=0}^{l-1} \lambda_j X^j$. Appliquons cela à a : pour tout i nous avons

$$(e_l^* \circ f^i)\big(P(f)a\big) = 0. \tag{11.281}$$

Mais par définition de E_a, l'élément $P(f)a$ est dans E_a. Nous en déduisons que

$$P(f)a \in G \cap E_a = \{0\}, \tag{11.282}$$

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. □

Définition 11.141.
Un endomorphisme d'un espace vectoriel est ***semi-simple*** *si tout sous-espace stable par u possède un supplémentaire stable.*

Lemme 11.142.
Si le polynôme minimal d'un endomorphisme est irréductible, alors il est semi-simple[37].

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 $u_1 \in E \backslash F$ et

$$E_{u_1} = \{P(f)u_1 \text{ tel que } P \in \mathbb{K}[X]\}, \tag{11.283}$$

qui est un espace stable par f.

Montrons que $E_{u_1} \cap F = \{0\}$. Pour cela nous regardons l'idéal

$$I_{u_1} = \{P \in \mathbb{K}[X] \text{ tel que } P(f)u_1 = 0\}. \tag{11.284}$$

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 6.40) qui nous donne $A, B \in \mathbb{K}[X]$ tels que

$$AP + BP_{u_1} = 1. \tag{11.285}$$

37. Définition 11.141.

Nous appliquons cette égalité à f et puis à u_1 :

$$u_1 = A(f) \circ \underbrace{P(f)u_1}_{=y} + B(f) \circ \underbrace{P_{u_1}(u_1)}_{=0} = A(f)y. \tag{11.286}$$

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 $u_2 \in E \backslash (E_{u_1} \oplus F)$. Étant donné que E est de dimension finie, ce procédé s'arrête à un certain moment et nous aurons

$$E = F \oplus E_{u_1} \oplus \ldots \oplus E_{u_k} \tag{11.287}$$

où chacun des E_{u_i} sont stables. □

Théorème 11.143.
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 $\mu_f = M_1^{\alpha_1} \ldots M_r^{\alpha_r}$ 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 $\alpha_i \geqslant 1$ 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

$$F = \ker M(f) \tag{11.288}$$

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.

D'abord nous prenons $x \in S$. Étant donné que F est le noyau de $M(f)$,

$$M(f)\big(MN(f)x\big) = \mu_f(f)x = 0, \tag{11.289}$$

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

$$MN(f) = N(f)\big(M(f)y\big) = 0 \tag{11.290}$$

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 $\mu_f = M^2 N$.

Nous passons au sens inverse. Soit $m_f = M_1 \ldots M_r$ 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

$$E_i = \ker(M_i(f)) \tag{11.291}$$

et $f_i = f|_{E_i}$. Par le lemme 11.128 nous avons

$$F = \bigoplus_{i=1}^{r} (F \cap E_i). \tag{11.292}$$

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 11.142.

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 :

$$E_i = S_i \oplus (F \cap E_i). \tag{11.293}$$

Étant donné que sur chaque S_i nous avons $f|_{S_i} = f_i$, l'espace $S = S_1 \oplus \ldots \oplus S_r$ est stable par f. Du coup nous avons

$$\begin{aligned} E &= E_1 \oplus \ldots \oplus E_r && (11.294a)\\ &= \big(S_1 \oplus (F \cap E_1)\big) \oplus \ldots \oplus \big(S_r \oplus (F \cap E_r)\big) && (11.294b)\\ &= \big(\bigoplus_{i=1}^{r} S_i\big) \oplus \big(\bigoplus_{i=1}^{r} F \cap E_i\big) && (11.294c)\\ &= S \oplus F, && (11.294d) \end{aligned}$$

ce qui montre que F a bien un supplémentaire stable par f et donc que f est semi-simple. □

Exemple 11.144(L'espace engendré par $\mathbb{1}$, A, A^2,...)
Soit A une matrice, et

$$V = \text{Span}\{A^k \text{ tel que } k \in \mathbb{N}\}. \tag{11.295}$$

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 minimal[38] que nous notons $\mu = \sum_{k=0}^{p} a_k X^k$. La partie $\{\mathbb{1}, \ldots, A^{p-1}\}$ est libre parce qu'une combinaison linéaire nulle de cela serait un polynôme annulateur en A de degré plus petit que p. Donc $\dim(V) \geqslant p$.

La partie $\{\mathbb{1}, A, \ldots, A^p\}$ 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 $\{\mathbb{1}, A, \ldots, A^{p-1}\}$ est génératrice (alors $\dim(V) \leqslant p$). Soit un entier $q \geqslant p$et de division euclidienne[39] $np + r = q$ avec $r < p$. Nous avons $A^q = A^{np}A^r$. D'une part

$$A^{np} = (A^p)^n = f(A)^n \tag{11.296}$$

est de degré $n(p-1)$. Par conséquent

$$A^q = f(A)^n A^r \tag{11.297}$$

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 $\{\mathbb{1}, A, \ldots, A^{p-1}\}$ est génératrice de V.

La dimension de V est donc p, le degré du polynôme minimal. △

Proposition 11.145.
Soit f un endomorphisme d'un espace vectoriel de dimension finie. Nous avons l'isomorphisme d'espace vectoriel

$$\mathbb{K}[f] \simeq \frac{\mathbb{K}[X]}{(\mu_f)} \tag{11.298}$$

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

$$\bar{P} = \{P + S\mu\}_{S \in \mathbb{K}[X]}. \tag{11.299}$$

Nous allons montrer que l'application suivante fournit l'isomorphisme :

$$\begin{aligned} \psi\colon \frac{\mathbb{K}[X]}{(\mu)} &\to \mathbb{K}[f]\\ \bar{P} &\mapsto P(f). \end{aligned} \tag{11.300}$$

38. Proposition 11.135.
39. Théorème 3.6.

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

$$\psi(\bar{Q}) = P(f) + (S\mu)(f). \tag{11.301}$$

Mais $\mu(f) = 0$ donc le deuxième terme est nul. Donc $\psi(\bar{P})$ est bien définit.

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 corollaire 6.37 en parle déjà : une base est donné par les projections de $1, X, \dots, X^{\deg(\mu_a)-1}$. □

11.8.3 Polynôme caractéristique

Définition 11.146.
Soit un anneau commutatif A. Si $u \in \mathbb{M}(n, A)$, nous définissons le ***polynôme caractéristique de*** *u :*

$$\chi_u(X) = \det(u - X\mathbb{1}_n). \tag{11.302}$$

Nous définissons de même le polynôme caractéristique d'un endomorphisme $u : E \to E$.

Remarque 11.147.
Quelques remarques à propos du signe[40].

- 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.
- 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 11.148.
Le polynôme caractéristique χ_u est unitaire en dimension paire et a pour degré la dimension de l'espace vectoriel E..

Théorème 11.149.
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n et un endomorphisme $u \in \mathrm{End}(E)$. 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 11.150.
Soit $u \in \mathrm{End}(E)$ et $\lambda \in \mathbb{K}$. Les conditions suivantes sont équivalentes

(1) $\lambda \in \mathrm{Spec}(u)$

(2) $\chi_u(\lambda) = 0$

(3) $\mu_u(\lambda) = 0$.

Démonstration. (1) ⇔ (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 11.52(1) ou encore que λ est une racine du polynôme caractéristique de u.

(2) ⇔ (3). Cela est une application directe du théorème 11.149 qui précise que le polynôme caractéristique a les mêmes racines dans $\mathbb{K}$ que le polynôme minimal. □

40. Attention : je crois qu'il y a des incohérences dans le Frido à propos de ce choix

Exemple 11.151

Sur $\mathbb{R}^2$, nous considérons la matrice $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ qui a pour polynôme caractéristique[41] 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 :

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \tag{11.303}$$

entraine $x = 0$.

Ici la multiplicité algébrique est différente de la multiplicité géométrique. △

La proposition suivante donne une utilisation amusante de la notion de polynôme caractéristique[42].

Proposition 11.152 ([148]).
Soit un espace vectoriel V de dimension finie pour lequel il existe un endomorphisme $f : V \to V$ 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 :

$$-v = \lambda f(v) = \lambda^2 v. \tag{11.304}$$

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. □

Une autre preuve possible est d'utiliser le déterminant : si la dimension de V est n nous avons :

$$\det(f^2) = \det(-\mathrm{Id}) = (-1)^n. \tag{11.305}$$

Donc $(-1)^n$ est positif, ce qui montre que n est pair.

Proposition 11.153 ([146]).
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

$$p_{f,x} = \dim E_{f,x} = \deg(\mu_{f,x}) \tag{11.306}$$

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

$$\chi_{f|_{E_{f,x}}}(f)x = \mu_{f,x}(f)x = 0. \tag{11.307}$$

Démonstration. Le fait que $E_{f,x}$ soit stable par f est classique. Le point (4) est un 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

$$B = \{f^k(x) \text{ tel que } 0 \leqslant k \leqslant p_{f,x} - 1\} \tag{11.308}$$

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

$$\mu_{f,x}(X) = X^{p_{f,x}} - \sum_{i=0}^{p_{f,x}-1} a_i X^k. \tag{11.309}$$

41. Définition 11.146.
42. Définition 11.146.

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

$$0 = f^{p_{f,x}}(x) - \sum_{i=0}^{p_{f,x}-1} a_i f^i(x) \tag{11.310}$$

nous trouvons

$$f^{p_{f,x}+k}(x) = \sum_{i=0}^{p_{f,x}-1} a_i f^{i+k}(x), \tag{11.311}$$

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

$$\mu_{f,x}(f)x = 0. \tag{11.312}$$

En y appliquant f^k et en profitant de la commutativité des polynômes sur les endomorphismes (proposition 11.126), nous avons

$$0 = f^k\big(\mu_{f,x}(f)x\big) = \mu_{f,x}(f)f^k(x), \tag{11.313}$$

de telle sorte que $\mu_{f,x}(f)$ est nul sur B et donc est nul sur $E_{f,x}$. Autrement dit,

$$\mu_{f,x}\big(f|_{E_{f,x}}\big) = 0. \tag{11.314}$$

Montrons que $\mu_{f,x}$ est même minimal pour $f|_{E_{f,x}}$. Sot 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 $f|_{E_{f,x}}$. □

Cette histoire de densité permet de donner une démonstration alternative du théorème de Cayley-Hamilton.

Théorème 11.154 (Cayley-Hamlilton)**.**
Le polynôme caractéristique est un polynôme annulateur.

Une démonstration plus simple via la densité des diagonalisables est donnée en théorème 14.24.

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 $f|_{E_{j,x}}$ divise χ_f, c'est-à-dire qu'il existe un polynôme Q_x tel que

$$\chi_f = Q_x\chi_{f,x}, \tag{11.315}$$

et donc aussi

$$\chi_f(f)x = Q_x(f)\big(\chi_{f,x}(f)x\big) = 0 \tag{11.316}$$

parce que la proposition 11.153 nous indique que $\chi_{f,x}$ est un polynôme annulateur de $f|_{E_{f,x}}$. □

Corollaire 11.155.
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 11.135. Or le degré du polynôme caractéristique est la dimension de l'espace par le lemme 11.148. □

Exemple 11.156(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

$$\chi_f(X) = \sum_{k=0}^{n} a_k X^k. \tag{11.317}$$

Nous aurons alors

$$0 = \chi_f(f) = \sum_{k=0}^{n} a_k f^k. \tag{11.318}$$

Nous appliquons f^{-1} à cette dernière égalité en sachant que $f^{-1}(0) = 0$:

$$0 = a_0 f^{-1} + \sum_{k=1}^{n} a_k f^{k-1}, \tag{11.319}$$

et donc

$$u^{-1} = -\frac{1}{\det(f)} \sum_{k=1}^{n} a_k f^{k-1} \tag{11.320}$$

où nous avons utilisé le fait que $a_0 = \chi_f(0) = \det(f)$. △

Proposition 11.157.
Si $(X-z)^l$ $(l \geqslant 1)$ est la plus grande puissance de $(X-z)$ dans le polynôme caractéristique d'un endomorphisme u alors

$$1 \leqslant \dim(E_e) \leqslant l. \tag{11.321}$$

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

$$\det(u - X\mathbb{1}) = (X-z)P(X), \tag{11.322}$$

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 $\dim(E_z) \geqslant 1$.

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

$$\begin{pmatrix} z & & & * \\ & \ddots & & \vdots \\ & & z & * \\ & & & * \end{pmatrix} \tag{11.323}$$

où les étoiles représentent des blocs a priori non nuls. En tout cas il est vu sous cette forme que $(X - z\mathbb{1})^k$ divise χ_u. □

11.9 Diagonalisation et trigonalisation

Ici encore $\mathbb{K}$ est un corps commutatif.

11.9.1 Matrices semblables

Définition 11.158 (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 $P \in \mathrm{GL}(n, \mathbb{K})$ telle que $B = P^{-1}AP$. Deux matrices équivalentes en ce sens sont dites ***semblables****.*

Le polynôme caractéristique [43] est un invariant sous les similitudes. En effet si P est une matrice inversible,

$$\begin{aligned}\chi_{PAP^{-1}} &= \det(PAP^{-1} - \lambda X) && (11.324a)\\ &= \det\left(P^{-1}(PAP^{-1} - \lambda X)P^{-1}\right) && (11.324b)\\ &= \det(A - \lambda X). && (11.324c)\end{aligned}$$

La permutation de lignes ou de colonnes ne sont pas de similitudes, comme le montrent les exemples suivants :

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \quad B = \begin{pmatrix} 2 & 1 \\ 4 & 3 \end{pmatrix}. \tag{11.325}$$

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.

11.9.2 Endomorphismes nilpotents

La **trace** d'une matrice $A \in \mathbb{M}(n, \mathbb{K})$ est la somme de ses éléments diagonaux :

$$\mathrm{Tr}(A) = \sum_{i=1}^{n} A_{ii}. \tag{11.326}$$

Une propriété importante est son invariance cyclique.

Lemme 11.159.
Quelque propriétés de la trace.

(1) Si A et B sont des matrices carrées, alors $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$.

(2) La trace est un invariant de similitude.

Démonstration. C'est un simple calcul :

$$\mathrm{Tr}(AB) = \sum_{ik} A_{ik}B_{ki} = \sum_{ik} A_{ki}B_{ik} = \sum_{ik} B_{ik}A_{ki} = \sum_{i} (BA)_{ii} = \mathrm{Tr}(BA) \tag{11.327}$$

où nous avons simplement renommé les indices $i \leftrightarrow k$.

En particulier, la trace est un invariant de similitude parce que $\mathrm{Tr}(ABA^{-1}) = \mathrm{Tr}(A^{-1}AB) = \mathrm{Tr}(B)$ par l'invariance cyclique démontrée en 4.59(2). □

La trace étant un invariant de similitude, nous pouvons donc définir la **trace** comme étant la trace de sa matrice dans une base quelconque. Si la matrice est diagonalisable, alors la trace est la somme des valeurs propres.

Lemme 11.160 ([57])**.**
L'endomorphisme $u \in \mathrm{End}(\mathbb{C}^n)$ est nilpotent si et seulement si $\mathrm{Tr}(u^p) = 0$ pour tout p.

Démonstration. Supposons que u est nilpotent. Alors ses valeurs propres sont toutes nulles et celles de u^p le sont également. La trace étant la somme des valeurs propres, nous avons alors tout de suite $\mathrm{Tr}(u^p) = 0$.

43. Définition 11.146.

Supposons maintenant que $\mathrm{Tr}(u^p) = 0$ pour tout p. Le polynôme caractéristique (11.302) est

$$\chi_u = (-1)^n X^\alpha (X - \lambda_1)^{\alpha_1} \dots (X - \alpha_r)^{\alpha_r}. \tag{11.328}$$

où les λ_i $(i = 1, \dots, r)$ sont les valeurs propres non nulles distinctes de u.

Il est vite vu que le coefficient de X^{n-1} dans χ_u est $-\mathrm{Tr}(u)$ parce que le coefficient de X^{n-1} se calcule en prenant tous les X sauf une fois $-\lambda_i$. D'autre part le polynôme caractéristique de u^p est le même que celui de u, en remplaçant λ_i par λ_i^p ; cela est dû au fait que si v est vecteur propre de valeur propre λ, alors $u^p v = \lambda^p v$.

Par l'équation (11.328), nous voyons que le coefficient du terme X^{n-1} dans les polynôme caractéristique est

$$0 = \mathrm{Tr}(u^p) = \alpha_1 \lambda_1^p + \dots + \alpha_r \lambda_r^p. \tag{11.329}$$

Donc les nombres $(\alpha_1, \dots, \alpha_r)$ est une solution non triviale [44] du système

$$\begin{cases} \alpha_1 X_1 + \dots + \lambda_r X_r = 0 & \text{(11.330a)} \\ \quad \vdots & \text{(11.330b)} \\ \lambda_1^r X_1 + \dots + \lambda_r^r X_r = 0. & \text{(11.330c)} \end{cases}$$

Cela sont les équations (11.329) écrites avec $p = 1, \dots, r$. Le déterminant de ce système est

$$\lambda_1 \dots \lambda_r \det \begin{pmatrix} 1 & \dots & 1 \\ \lambda_1 & \dots & \lambda_1 \\ \vdots & & \vdots \\ \lambda_1^{r-1} & \dots & \lambda_r^{r-1} \end{pmatrix} \neq 0, \tag{11.331}$$

qui est un déterminant de Vandermonde (proposition 11.54) valant

$$0 = \lambda_1 \dots \lambda_r \prod_{1 \leqslant i \leqslant j \leqslant r} (\lambda_i - \lambda_j). \tag{11.332}$$

Étant donné que les λ_i sont distincts et non nuls, nous avons une contradiction et nous devons conclure que $(\alpha_1, \dots, \alpha_r)$ était une solution triviale du système (11.330). □

Proposition 11.161 ([149]).
Soit un $\mathbb{K}$-espace vectoriel E. Un endomorphisme $u \in \mathrm{End}(E)$ 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 intègre [45].

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

$$\{x, e_2, \dots, e_n\} \tag{11.333}$$

donnée par le théorème de la base incomplète 4.11. La matrice de u dans cette base s'écrit

$$\left(\begin{array}{c|ccc} 0 & * & * & * \\ \hline 0 & & & \\ 0 & & A & \\ 0 & & & \end{array}\right). \tag{11.334}$$

44. Si $\alpha_1 = \dots = \alpha_r = 0$, alors les valeurs propres sont toutes nulles et la matrice est en réalité nulle dès le départ.
45. Lemme 1.64.

Un tout petit peu de calcul de produit de matrice montre que la matrice de u^k est de la forme

$$\left(\begin{array}{c|ccc} 0 & * & * & * \\ \hline 0 & & & \\ 0 & & A^k & \\ 0 & & & \end{array}\right). \tag{11.335}$$

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

$$\text{Span}\{e_1, \dots, e_k\} \to \text{Span}\{e_1, \dots, e_{k-1}\}. \tag{11.336}$$

Donc tout vecteur finit sur zéro si on lui applique u assez souvent.

□

Proposition 11.162 (Thème 42)**.**
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

$$(\mathbb{1} - A)^{-1} = \sum_{k=0}^{\infty} A^k, \tag{11.337}$$

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 doutes 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 :

$$\sum_{k=0}^{n} A^k(\mathbb{1} - A) = \sum_{k=0}^{n} (A^k - A^{k+1}) = \mathbb{1} - A^{n+1}. \tag{11.338}$$

Par conséquent

$$\|\mathbb{1} - \sum_{k=0}^{n} A^k(\mathbb{1} - A)\| = \|A^{n+1}\| \to 0. \tag{11.339}$$

La dernière limite est en réalité une égalité pour n assez grand. □

Proposition 11.163.
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 $\text{Spec}(A) \subset \text{S}^1$.

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

$$A = \begin{pmatrix} \lambda_1\mathbb{1} + N_1 & & \\ & \ddots & \\ & & \lambda_s\mathbb{1} + N_s \end{pmatrix}, \tag{11.340}$$

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

$$(\lambda\mathbb{1} + N)^n = \sum_{k=0}^{r-1} \binom{n}{k} N^k \lambda^{n-k}. \tag{11.341}$$

Par la proposition 11.161, une matrice nilpotente s'écrit dans une base sous la forme

$$N = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ & & & & 0 \end{pmatrix} \tag{11.342}$$

et effectuer A^k revient à décaler la diagonale de 1. Donc la famille

$$\{\mathbb{1}, N, \dots, N^{r-1}\} \tag{11.343}$$

est libre. Par conséquent la suite $(\lambda\mathbb{1} + N)^n$ restera bornée si et seulement si chacun des termes

$$\binom{n}{k} N^k \lambda^{n-k} \tag{11.344}$$

reste borné. Le premier terme étant $\lambda^n\mathbb{1}$, nous avons obligatoirement $|\lambda| \leqslant 1$. 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 (11.344) 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

$$\lambda\mathbb{1} + N = \lambda(\mathbb{1} + \lambda^{-1}N), \tag{11.345}$$

et nous pouvons appliquer la proposition 11.162 à l'opérateur nilpotent $-\lambda^{-1}N$ pour avoir

$$(\mathbb{1} + \lambda^{-1}N)^{-1} = \mathbb{1} + \sum_{k=1}^{\infty} (-\lambda)^{-1} N^k. \tag{11.346}$$

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 $N = N' = 0$. □

11.9.3 Endomorphismes diagonalisables

Définition 11.164.
Une matrice est ***diagonalisable*** *si elle est semblable*[46] *à une matrice diagonale.*

Lemme 11.165.
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 $\mathrm{Spec}(A) = \{1\}$. Pour la diagonaliser, il faudrait une matrice $P \in \mathrm{GL}(n, \mathbb{K})$ telle que $\mathbb{1} = P^{-1}AP$, ce qui est uniquement possible si $A = \mathbb{1}$. □

46. Définition 11.158.

Lemme 11.166.
Soit F un sous-espace stable par u. Soit une décomposition du polynôme minimal

$$\mu_u = P_1^{n_1} \dots P_r^{n_r} \tag{11.347}$$

où les P_i sont des polynômes irréductibles unitaires distincts. Si nous posons $E_i = \ker P_i^{n_i}$, alors

$$F = (F \cap E_1) \oplus \dots \oplus (F \cap E_r). \tag{11.348}$$

Théorème 11.167.
Soit E, un espace vectoriel de dimension n sur le corps commutatif $\mathbb{K}$ et $u \in \mathrm{End}(E)$. 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 simples[47]*.*

(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 6.36.

(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

$$\mu_u(X) = (X - \lambda_1) \dots (X - \lambda_r) \tag{11.350}$$

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 11.127) nous enseigne que

$$E = \ker(u - \lambda_1) \oplus \dots \oplus \ker(u - \lambda_r). \tag{11.351}$$

Mais $\ker(u - \lambda_i)$ est l'espace propre $E_{\lambda_i}(u)$. Donc u est diagonalisable.

(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 $\dim E = n \geqslant 2$. 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

$$P(x) = (X - \lambda_1) \dots (X - \lambda_r). \tag{11.352}$$

47. Le polynôme *caractéristique*, lui, n'a pas spécialement ses racines simples ; il peut encore être de la forme

$$\chi_u(X) = \prod_{i=1}^{r} (X - \lambda_i)^{\alpha_i}, \tag{11.349}$$

mais alors $\dim(E_{\lambda_i}) = \alpha_i$.

Alors $P(u) = 0$. En effet si e_i est un vecteur propre pour la valeur propre λ_i,

$$P(u)e_i = \prod_{j\neq i}(u - \lambda_j) \circ (u - \lambda_i)e_i = 0 \tag{11.353}$$

par le lemme 11.126. 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

$$\mu = (X - \lambda_1)\dots(X - \lambda_r), \tag{11.354}$$

et les espaces E_i du lemme 11.166 sont les espaces propres $E_i = \ker(u - \lambda_i)$. Nous avons donc une somme directe

$$E = E_1 \oplus \dots \oplus E_r. \tag{11.355}$$

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.

□

Corollaire 11.168.
Si u est diagonalisable et si F est une sous-espace stable par u, alors

$$F = \bigoplus_{\lambda} E_\lambda(u) \cap F \tag{11.356}$$

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 11.167, le polynôme μ_u est scindé et ne possède que des racines simples. Notons le

$$\mu_u(X) = (X - \lambda_1)\dots(X - \lambda_r). \tag{11.357}$$

Les espaces E_i du lemme 11.166 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 11.169.
Soit E un $\mathbb{K}$-espace vectoriel et $u \in \mathrm{End}(E)$. Si $\mathrm{Card}\big(\mathrm{Spec}(u)\big) = \dim(E)$ 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 11.124). Par conséquent $\mathrm{Span}\{E_{\lambda_i}(u)\}$ est de dimension n est u est diagonalisable. □

Voici un résultat de diagonalisation simultanée. Nous donnerons un résultat de trigonalisation simultanée dans le lemme 11.264.

Proposition 11.170 (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 $u_j\big(E_\lambda(u)\big) \subset E_\lambda(u)$.

(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 $u_j x \in E_\lambda(u)$. Nous avons

$$u_i\big(u_j(x)\big) = u_j\big(u_i(x)\big) = \lambda u_j(x). \tag{11.358}$$

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

$$E_{\lambda_k}(u_0) \neq E, \tag{11.359}$$

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 :

$$E = \bigoplus_k E_{\lambda_k}(u_0). \tag{11.360}$$

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 $u_i \colon E_{\lambda_k}(u_0) \to E_{\lambda_k}(u_0)$, et nous pouvons considérer la famille d'opérateurs

$$\Big(u_i|_{E_{\lambda_k}(u_0)}\Big)_{i\in I}. \tag{11.361}$$

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. □

Exemple 11.171

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 $1 \neq -1$, $X^1 - 1$ est donc scindé à racines simples et les involutions sont diagonalisables (11.167). 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

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tag{11.362a}$$

$$A^1 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{11.362b}$$

Ce A est donc une involution mais n'est pas diagonalisable. △

11.9.4 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 11.167(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 11.172

La matrice

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \tag{11.363}$$

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. △

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.

11.9.5 Trigonalisation : généralités

Définition 11.173 ([150]).
*Une matrice dans $\mathbb{M}(n,\mathbb{K})$ est **trigonalisable** lorsqu'elle est semblable*[48] *à une matrice triangulaire supérieure.*

Proposition 11.174 (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 scindé[49].

Démonstration. **(2)⇒(1)** Nous avons par hypothèse que

$$\chi_u(X) = \prod_{i=1}^{r}(X-\lambda_i)^{\alpha_i} \tag{11.364}$$

où les λ_i sont les valeurs propres de u. Le théorème de Cayley-Hamilton 11.154 dit que $\chi_u(u)=0$, ce qui permet d'utiliser le théorème de décomposition des noyaux 11.127 :

$$E = \ker(X-\lambda_1)^{\alpha_1} \oplus \ldots \oplus \ker(X-\lambda_r)^{\alpha_r}. \tag{11.365}$$

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 bloc [50]. Cela signifie que u est triangulaire supérieure avec les valeurs propres sur la diagonale.

(1)⇒(2) C'est immédiat parce que le déterminant d'une matrice triangulaire est le produit des éléments de sa diagonale.

□

Remarque 11.175.
La méthode des pivots de Gauss [51] certes permet de trigonaliser n'importe quoi, mais elle ne 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* (définition 4.103). Lorsqu'on parle de changement de base, de matrice trigonalisable ou diagonalisable, nous parlons de similarité et non d'équivalence.

11.9.6 Trigonalisation : cas complexe

La proposition 11.174 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 11.179 utilisant la proposition 11.174.

48. Définition 11.158.
49. Définition 6.32.
50. Proposition 11.161.
51. Le lemme 4.104.

Lemme 11.176 (Lemme de Schur complexe, trigonisation[151]).
Si $A \in \mathbb{M}(n, \mathbb{C})$, il existe une matrice unitaire U telle que UAU^{-1} soit triangulaire supérieure[52].

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)

$$Q = \begin{pmatrix} \uparrow & \uparrow & & \uparrow \\ v & u_2 & \cdots & u_n \\ \downarrow & \downarrow & & \downarrow \end{pmatrix}. \tag{11.366}$$

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

$$Q^{-1}AQ = \begin{pmatrix} \lambda_1 & * \\ 0 & A_1 \end{pmatrix} \tag{11.367}$$

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). □

En particulier les matrices hermitiennes, anti-hermitiennes et unitaires sont trigonalisables par une matrice unitaire, qui peut être choisie de déterminant 1.

Lemme 11.177.
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, $\mathrm{Spec}(A) = \mathrm{Spec}(T)$.

(3) Les valeurs propres de A sont les éléments diagonaux de T.

Démonstration. Vu que U commute évidemment avec $\mathbb{1}$ nous avons

$$\chi_A(\lambda) = \det(A - \lambda\mathbb{1}) = \det(UTU^{-1} - \lambda\mathbb{1}) = \det\big(U(T - \lambda\mathbb{1})U^{-1}\big). \tag{11.368}$$

À ce niveau nous utilisons le fait que le déterminant soit multiplicatif 11.52 pour conclure :

$$\chi_A(\lambda) = \det\big(U(T - \lambda\mathbb{1})U^{-1}\big) = \det(U)\det(T - \lambda\mathbb{1})\det(U^{-1}) = \det(T - \lambda\mathbb{1}) = \chi_T(\lambda). \tag{11.369}$$

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 11.150.

Les valeurs propres d'une matrice triangulaire sont les valeurs sur la diagonale. □

Remarque 11.178.
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

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tag{11.370}$$

a deux 1 sur la diagonale. Le nombre 1 est bien une valeur propre de A, mais le système

$$A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \tag{11.371}$$

donne $y = 0$ et donc un espace propre de dimension seulement 1.

52. « 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 11.179.
Si $\mathbb{K}$ est algébriquement clos (comme $\mathbb{C}$ par exemple), alors tous les polynômes sont scindés et toutes les matrices sont trigonalisables[53]. Un exemple un peu simple de cela est la matrice

$$u = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{11.372}$$

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

$$\{\begin{pmatrix} i \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ i \end{pmatrix}\} \tag{11.373}$$

de $\mathbb{C}^2$, la matrice u se note $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$.

Remarque 11.180.
Cela nous donne une autre façon de prouver qu'une matrice nilpotente de $\mathbb{M}(n, \mathbb{C})$ ou $\mathbb{M}(n, \mathbb{R})$ est trigonalisable[152]. D'abord dans $\mathbb{M}(n, \mathbb{C})$, toutes les matrices sont trigonalisables[54], 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 $u \in \mathbb{M}(n, \mathbb{R})$ nous pouvons voir u comme une matrice dans $\mathbb{M}(n, \mathbb{C})$ et y calculer son polynôme caractéristique qui sera tout de même X^n. Ce polynôme étant scindé, la proposition 11.174 nous assure que u est trigonalisable. Une fois de plus, les valeurs propres étant sur la diagonale, elle est triangulaire supérieure stricte.

Corollaire 11.181.
Le polynôme caractéristique[55] *sur $\mathbb{C}$ d'une matrice s'écrit sous la forme*

$$\chi_A(X) = \prod_{i=1}^{r} (X - \lambda_i)^{m_i} \tag{11.374}$$

où les λ_i sont les valeurs propres distinctes de A et m_i sont les multiplicités correspondantes.

Démonstration. Le lemme 11.176 nous donne l'existence d'une base de trigonalisation ; dans cette base les valeurs propres de A sont sur la diagonale et nous avons

$$\chi_A(X) = \det(A - X\mathbb{1}) = \det \begin{pmatrix} X - \lambda_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & X - \lambda_r \end{pmatrix}, \tag{11.375}$$

qui vaut bien le produit annoncé. □

Corollaire 11.182.
Si $A \in \mathbb{M}(n, \mathbb{C})$ et $k \in \mathbb{N}$ alors

$$\mathrm{Spec}(A^k) = \{\lambda^k \text{ tel que } \lambda \in \mathrm{Spec}(A)\}. \tag{11.376}$$

Démonstration. Par le lemme 11.176 nous avons une matrice unitaire U et une triangulaire T telles que $A = UTU^{-1}$. En passant à a puissance k nous avons aussi

$$A^k = UT^kU^{-1}. \tag{11.377}$$

Donc le spectre de A^k est celui de T^k (lemme 11.177 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. □

53. La proposition 11.174 montre cela, et le lemme de Schur complexe 11.176 va un peu plus loin et précise que la trigonalisation peut être faite par une matrice unitaire.
54. Parce que le polynôme caractéristique est scindé, voir la proposition 11.174..
55. Définition 11.146.

11.9.7 Diagonalisation : cas complexe, ce qu'on a

Lemme 11.183 (Théorème spectral hermitien)**.**
Pour un opérateur hermitien[56]*,*

(1) le spectre est réel,

(2) deux vecteurs propres pour des valeurs propres distinctes sont orthogonales[57]*.*

Démonstration. Soit v un vecteur de valeur propre λ. Nous avons d'une part

$$\langle Av, v\rangle = \lambda\langle v, v\rangle = \lambda\|v\|^2, \tag{11.378}$$

et d'autre part, en utilisant le fait que A est hermitien,

$$\langle Av, v\rangle = \langle v, A^*v\rangle = \langle v, Av\rangle = \bar{\lambda}\|v\|^2, \tag{11.379}$$

par conséquent $\lambda = \bar{\lambda}$ parce que $v \neq 0$.

Soient λ_i et v_i $(i = 1, 2)$ deux valeurs propres de A avec leurs vecteurs propres correspondants. Alors d'une part

$$\langle Av_1, v_2\rangle = \lambda_1\langle v_1, v_2\rangle, \tag{11.380}$$

et d'autre part

$$\langle Av_1, v_2\rangle = \langle v_1, Av_2\rangle = \lambda_2\langle v_1, v_2\rangle. \tag{11.381}$$

Nous avons utilisé le fait que λ_2 était réel. Par conséquent, soit $\lambda_1 = \lambda_2$, soit $\langle v_1, v_2\rangle = 0$. □

Remarque 11.184.
Un opérateur de la forme A^*A est évidemment hermitien. De plus ses valeurs propres sont toutes positives parce que si $A^*Ax = \lambda v$ alors

$$0 \leqslant \langle Av, Av\rangle = \langle A^*Av, v\rangle = \lambda\langle v, v\rangle. \tag{11.382}$$

Donc $\lambda \geqslant 0$.

Définition 11.185.
Un endomorphisme est ***normal*** *s'il commute avec son adjoint.*

Les opérateurs normaux comprennent évidemment les opérateurs hermitiens, mais également les anti-hermitiens, et ça c'est bien parce que c'est le cas de l'algèbre associée à SU(2).

Théorème 11.186 (Théorème spectral pour les matrices normales[58][153, 154, 155])**.**
Soit $A \in \mathbb{M}(n, \mathbb{C})$ une matrice de valeurs propres $\lambda_1, \ldots, \lambda_n$ (non spécialement distinctes). Alors les conditions suivantes sont équivalentes :

(1) A est normale,

(2) A se diagonalise par une matrice unitaire,

(3) $\sum_{i,j=1}^n |A_{ij}|^2 = \sum_{j=1}^n |\lambda_j|^2$,

(4) il existe une base orthonormale de vecteurs propres de A.

Démonstration. Nous allons nous contenter de prouver (1)⇔(2).

Soit Q la matrice unitaire donnée par la décomposition de Schur (lemme 11.176) : $A = QTQ^{-1}$. Étant donné que A est normale nous avons

$$QTT^*Q^{-1} = QT^*TQ^{-1}, \tag{11.383}$$

56. Définition 11.76.
57. Pour la forme (11.7).
58. Définition 11.185

ce qui montre que T est également normale. Or une matrice triangulaire supérieure normale est diagonale. En effet nous avons $T_{ij} = 0$ lorsque $i > j$ et

$$(TT^*)_{ii} = (T^*T)_{ii} = \sum_{k=1}^{n} |T_{ki}|^2 = \sum_{k=1}^{n} |T_{ik}|^2. \tag{11.384}$$

Écrivons cela pour $i = 1$ en tenant compte de $|T_{k1}|^2 = 0$ pour $k = 2, \dots, n$,

$$|T_{11}|^2 = |T_{11}|^2 + |T_{12}|^2 + \cdots + |T_{1n}|^2, \tag{11.385}$$

ce qui implique que T_{11} est le seul non nul parmi les T_{1k}. En continuant de la sorte avec $i = 2, \dots, n$ nous trouvons que T est diagonale.

Dans l'autre sens, si A se diagonalise par une matrice unitaire, $UAU^* = D$, nous avons

$$DD^* = UAA^*U^* \tag{11.386}$$

et

$$D^*D = UA^*AU^*, \tag{11.387}$$

qui ce prouve que A est normale. □

Tant que nous en sommes à parler de spectre de matrices hermitiennes... Soit une matrice inversible $A \in \mathrm{GL}(n, \mathbb{C})$. La matrice A^*A est hermitienne [59] et le théorème 11.183 nous assure que ses valeurs propres sont réelles. Par la remarque 11.184, ses valeurs propres sont même positives.

Lemme 11.187 ([156]).
Si A est une matrice carrée et inversible,

$$\mathrm{Spec}(A^*A) = \mathrm{Spec}(AA^*) \tag{11.388}$$

Démonstration. Nous allons montrer l'égalité des polynômes caractéristiques. D'abord une simple multiplication montre que

$$(A^*A - \lambda\mathbb{1})A^{-1} = A^{-1}(AA^* - \lambda\mathbb{1}). \tag{11.389}$$

Nous prenons le déterminant de cette égalité en utilisant les propriétés 11.52(1) et (3) :

$$\det(A^*A - \lambda\mathbb{1})\det(A^{-1}) = \det(A^{-1})\det(AA^* - \lambda\mathbb{1}). \tag{11.390}$$

En simplifiant par $\det(A^{-1})$ (qui est non nul parce que A est inversible) nous obtenons l'égalité des polynômes caractéristiques et donc l'égalité des spectres. □

11.9.8 Diagonalisation : cas réel

Lemme 11.188 (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

$$QAQ^{-1} = \begin{pmatrix} \lambda_1 & * & * & * & * \\ 0 & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \lambda_r & * & * \\ 0 & 0 & 0 & \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} & * \\ 0 & 0 & 0 & 0 & \begin{pmatrix} a_s & b_s \\ c_s & d_s \end{pmatrix} \end{pmatrix}. \tag{11.391}$$

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.

59. Définition 11.76.

Démonstration. Si la matrice A a des valeurs propres réelles, nous procédons comme dans le cas complexe. Cela nous fournit le 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

$$Au + iAv = A(u + iv) = (\alpha + i\beta)(u + iv) = \alpha u - \beta v + i(\alpha v + \beta v), \tag{11.392}$$

et en égalisant les parties réelles et imaginaires,

$$Au = \alpha u - \beta v \tag{11.393a}$$
$$Av = \alpha v + \beta u. \tag{11.393b}$$

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 avions 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

$$Q^{-1}AQe_1 = Q^{-1}Aq_1 = Q^{-1}(aq_1 + bq_2) = ae_1 + be_2. \tag{11.394}$$

La matrice $Q^{-1}AQ$ est donc de la forme

$$Q^{-1}AQ = \begin{pmatrix} \begin{pmatrix} \cdot & \cdot \\ \cdot & \cdot \end{pmatrix} & C_1 \\ 0 & A_1 \end{pmatrix} \tag{11.395}$$

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 (11.391) que les valeurs propres sont celles des blocs diagonaux. Étant donné que QAQ^{-1} et A ont même polynôme caractéristique, ce sont les valeurs propres de A. □

Théorème 11.189 (Théorème spectral, matrice symétrique[43])**.**
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 11.188 donne une matrice orthogonale qui trigonalise A. Les valeurs propres étant toutes réelles, la matrice QAQ^{-1} est même triangulaire (il n'y a pas de blocs dans la forme (11.391)). Prouvons que QAQ^{-1} est symétrique :

$$(QAQ^{-1})^t = (Q^{-1})^t A^t Q^t = QA^tQ^{-1} = QAQ^{-1} \tag{11.396}$$

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 e telle que $A = Q^tDQ$ avec D diagonale. Nous posons $f_i = Q^te_i$ et en tenant compte du fait que $Q^t = Q^{-1}$ nous avons $Af_i = Q^tDQQ^te_i = Q^t\lambda_i e_i = \lambda_i f_i$. Donc les f_i sont des vecteurs propres de A. De plus ils sont orthonormés parce que

$$\langle f_i, f_j\rangle = \langle Q^te_i, Q^te_j\rangle = \langle e_i, Q^tQe_j\rangle = \langle e_i, e_j\rangle = \delta_{ij}. \tag{11.397}$$

□

Le théorème spectral pour les opérateurs autoadjoints sera traité plus bas parce qu'il a besoin de choses sur les formes bilinéaires, théorème 11.287.

Remarque 11.190.
Une matrice symétrique est diagonalisable par une matrice orthogonale. Nous pouvons en réalité nous arranger pour diagonaliser par une matrice de $\mathrm{SO}(n)$. Plus généralement si A est une matrice diagonalisable par une matrice $P \in \mathrm{GL}^+(n,\mathbb{R})$ alors elle est diagonalisable par une matrice de $\mathrm{GL}^-(n,\mathbb{R})$ en changeant le signe de la première ligne de P. Et inversement.

En effet, si nous avons $P^tDP = A$, alors en notant $*$ les quantités qui ne dépendent pas de a, b ou c,

$$\begin{aligned}\begin{pmatrix} a & * & * \\ b & * & * \\ c & * & * \end{pmatrix}\begin{pmatrix} \lambda_1 & & \\ & \lambda_2 & \\ & & \lambda_3 \end{pmatrix}\begin{pmatrix} a & b & c \\ * & * & * \\ * & * & * \end{pmatrix} &= \begin{pmatrix} a & * & * \\ b & * & * \\ c & * & * \end{pmatrix}\begin{pmatrix} \lambda_1 a & \lambda_1 b & \lambda_1 c \\ * & * & * \\ * & * & * \end{pmatrix} \\ &= \begin{pmatrix} \lambda_1 a^2 + * & \lambda_1 ab + * & \lambda_1 ac + * \\ \dots & \dots & \dots \\ \dots & \dots & \dots \end{pmatrix}.\end{aligned} \tag{11.398}$$

Nous voyons donc que si nous changeons les signes de a, b et c en même temps, le résultat ne change pas.

Définition 11.191 (Matrice définie positive, opérateur définit positif)**.**
Un opérateur sur un espace vectoriel sur $\mathbb{C}$ ou $\mathbb{R}$ est ***définit positif*** *si toutes ses valeurs propres sont réelles et strictement positives. Il est* ***semi-définie positive*** *si ses valeurs propres sont réelles positives ou nulles.*

Afin d'éviter l'une ou l'autre confusion, nous disons souvent *strictement* définie positive pour positive.

11.192.
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 11.193.
Nous ne définissons pas la notion de matrice définie positive pour une matrice non symétrique.

Proposition 11.194.
Soit M, une matrice symétrique. Nous avons

(1) $\det M > 0$ *et* $\mathrm{Tr}(M) > 0$ *implique M définie positive*[60]*,*

(2) $\det M > 0$ *et* $\mathrm{Tr}(M) < 0$ *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.*

Proposition 11.195.
Une application linéaire est définie positive[61] *si et seulement si sa matrice associée l'est.*

60. Défintion 11.191.
61. Définition 11.191.

Lorsqu'un énoncé parle d'une matrice symétrique, le premier réflexe est de la diagonaliser : considérer une matrice orthogonale T telle que $T^tMT = D$ 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 11.196.
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 $\langle x, Mx\rangle \geqslant 0$ pour tout x non nul dans $\mathbb{R}^n$.

(3) Si elle est seulement définie positive, alors $\langle x, Mx\rangle \geqslant \lambda\|x\|^2$ dès que $\lambda \geqslant 0$ 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 11.189. Nous nommons x_i les coordonnées de x dans cette base. Alors,

$$\langle x, Mx\rangle = \sum_{i,j} x_i\langle e_i, x_jMe_j\rangle = \sum_{i,j} x_ix_j\langle e_i, \lambda_je_j\rangle = \sum_{ij} x_ix_j\lambda_j\delta_{ij} = \sum_i \lambda_ix_i^2 \tag{11.399}$$

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

$$\langle x, Mx\rangle = \sum_i \lambda_ix_i^2. \tag{11.400}$$

Cela est plus grand ou égal à zéro si et seulement si tous les λ_i sont plus grands ou égaux à zéro.

(3) Soit une matrice orthogonale T diagonalisant M, c'est-à-dire telle que $T^tMT = D$ avec D diagonale. Nous allons vérifier que

$$\langle Tx, Mtx\rangle \geqslant \lambda\|Tx\|^2 \tag{11.401}$$

pour tout x. Vu que T est une bijection [62], 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

$$\begin{aligned}
\langle Tx, MTx\rangle &= \langle x, T^tMTx\rangle && \text{(11.402a)}\\
&= \langle x, Dx\rangle && \text{(11.402b)}\\
&= \sum_k \langle x, x_kDe_k\rangle && \text{(11.402c)}\\
&= \sum_k \lambda_kx_k\underbrace{\langle x, e_k\rangle}_{=x_k} && \text{(11.402d)}\\
&\geqslant \sum_k \lambda|x_k|^2 && \text{(11.402e)}\\
&= \lambda\|x\|^2 && \text{(11.402f)}\\
&= \lambda\|Tx\|^2. && \text{(11.402g)}
\end{aligned}$$

Au dernier passage nous avons utilisé le fait que T est une isométrie (proposition 11.83).

□

62. Une matrice orthogonale a un déterminant ± 1.

Les personnes qui aiment les vecteurs lignes et colonnes écriront des inégalités comme

$$x^t M x \geqslant x^t x. \tag{11.403}$$

Tout à l'autre bout du spectre des personnes névrosées des notations, on trouvera des inégalités comme

$$M(x \otimes x) \geqslant x \cdot x. \tag{11.404}$$

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 12.8.6 et en particulier ce qui suit (12.295).

La notation adoptée ici avec le produit scalaire $\langle x, Mx\rangle$ 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.

Corollaire 11.197.
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 11.196. □

Lemme 11.198.
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 11.196. Si A est définie positive et que $\{e_i\}$ est une base, alors

$$A_{ii} = \langle Ae_i, e_i\rangle \geqslant \lambda \|e_i\|^2 = \lambda \geqslant 0. \tag{11.405}$$

Si A est strictement définie positive, alors λ peut être choisi strictement positif. □

11.10 Formes bilinéaires et quadratiques

Plus à propos de formes bilinéaires dans le thème 47.

11.10.1 Généralités

Définition 11.199 ([157]).
*Soit un espace vectoriel E et $\mathbb{F}$ un corps de caractéristique différente de 2. Une **forme quadratique** sur E est une application $q\colon E \to \mathbb{F}$ pour laquelle il existe une forme bilinéaire symétrique $b\colon E \times E \to \mathbb{F}$ satisfaisant $q(x) = b(x, x)$ pour tout $x \in E$.*

L'ensemble des formes quadratiques réelles sur E est noté $Q(E)$.

Lemme 11.200.
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** :

$$b(x, y) = \frac{1}{2}\big(q(x) + q(y) - q(x - y)\big). \tag{11.406}$$

Elle est donc déterminée par q. □

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.

11.10.2 Matrice associée à une forme bilinéaire

Soit une forme bilinéaire $b\colon E\times E\to\mathbb{K}$ et une base $\{f_\alpha\}$ de E, pas spécialement orthonormée. Nous définissons les nombres

$$B_{\alpha\beta}=b(f_\alpha,f_\beta),\tag{11.407}$$

qui forment une matrice symétrique dans $\mathbb{M}(n,\mathbb{K})$. Alors nous avons aussi, si $y=\sum_\alpha y_\alpha f_\alpha$ et $y'=\sum_\beta y'_\beta f_\beta$:

$$b(y,y')=\sum_{\alpha\beta}q(f_\alpha,f_\beta)=\sum_{\alpha\beta}B_{\alpha\beta}y_\alpha y'_\beta.\tag{11.408}$$

La matrice B est la matrice de b dans la base $\{f_\alpha\}$ de V.

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.

11.10.3 Diagonalisation

Proposition 11.201.
Soit une forme bilinéaire symétrique b sur un espace vectoriel E de dimension finie. Il existe une matrice orthogonale Q telle que

(1) $D=Q^tbQ$ est diagonale

(2) $D(x,y)=b(Qx,Qy)$ pour tout $x,y\in E$.

Dans cet énoncé, nous mélangeons sans vergogne les formes et les matrices, en supposant qu'une base soit fixée[63]*. Par exemple*

$$D(x,y)=\sum_{ij}D_{ij}x_iy_j.\tag{11.409}$$

Démonstration. Pour la matrice diagonale, c'est le théorème spectral 11.189(2) qui joue parce que la matrice d'une forme bilinéaire symétrique est symétrique (c'est vu de la définition (11.407)).

Pour le reste c'est un calcul :

$$\begin{aligned}D(x,y)&=\sum_{ijkl}Q^t_{ik}b_{kl}Q_{lj}x_iy_j&(11.410a)\\&=\sum_{ijkl}b_{kl}(Q_{ki}x_i)(Q_{lj}y_j)&(11.410b)\\&=\sum_{kl}b_{kl}(Qx)_k(Qy)_l&(11.410c)\\&=b(Qx,Qy).&(11.410d)\end{aligned}$$

Nous avons utilisé le produit matrice fois vecteur donné par (4.72). □

11.10.4 Isométrie, forme quadratique et bilinéaire

Exemple 11.202
La forme quadratique $q(x)=x_1^2+x_2^2$ donne la norme euclidienne. La forme bilinéaire associée est $b(x,y)=x_1y_1+x_2y_2$, qui est le produit scalaire usuel. △

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.

63. 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 11.203.
*Une **isométrie** pour la forme quadratique q est une application bijective $f\colon V \to V$ telle que*

$$q(x-y) = q\big(f(x) - f(y)\big). \tag{11.411}$$

Dans les cas où q donne une distance, alors c'est une isométrie au sens usuel.

Définition 11.204 (Thème 64)**.**
*Soit un espace vectoriel E muni d'une forme bilinéaire b. Une **isométrie** pour b est une bijection $f\colon E \to E$ telle que*

$$b\big(f(x), f(y)\big) = b(x,y) \tag{11.412}$$

pour tout $x, y \in E$.

Lemme 11.205.
Soient q une forme quadratique et b la forme bilinéaire associée par le lemme 11.200. Une application $f\colon E \to E$ 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 $f\colon E \to E$ telle que $f(0) = 0$, nous devons prouver l'équivalence des propriétés suivantes :

(1) $b\big(f(x), f(y)\big) = b(x,y)$ pour tout $x, y \in E$;
(2) $q\big(f(x) - f(y)\big) = q(x-y)$ 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,

$$\begin{aligned} q\big(f(x) - f(y)\big) &= b\big(f(x) - f(y), f(x) - f(y)\big) && \text{(11.413a)}\\ &= q\big(f(x)\big) - 2b\big(f(x), f(y)\big) + q\big(f(y)\big) && \text{(11.413b)}\\ &= q(x) + q(y) - 2b(x,y) && \text{(11.413c)}\\ &= q(x-y). && \text{(11.413d)} \end{aligned}$$

Dans l'autre sens, nous commençons par remarquer que l'hypothèse $f(0) = 0$ donne $q(x) = q\big(f(x)\big)$. Ensuite nous utilisons l'identité de polarisation (11.406) :

$$\begin{aligned} b\big(f(x), f(y)\big) &= \frac{1}{2}\big[q\big(f(x)\big) + q\big(f(y)\big) - q\big(f(x-y)\big)\big] && \text{(11.414a)}\\ &= \frac{1}{2}\big[q(x) + q(y) - q(x-y)\big] && \text{(11.414b)}\\ &= b(x,y). && \text{(11.414c)} \end{aligned}$$

□

11.11 Conventions et notations sur les matrices et changement de bases

Nous nous proposons à présent de fixer toutes les notations concernant le calcul matriciel et les changements de bases[64]. Nous considérons des espaces vectoriels V et W respectivement munis de bases $\{e_i\}$ et $\{f_\alpha\}$. Ils sont tous deux sur le corps commutatif $\mathbb{K}$. Si $T\colon V \to W$ est une application linéaire, alors sa matrice est définie en la définition 4.61 (et les résultats qui montrent que le ψ est une bijection comme il faut). Ici nous prenons une notation plus détendue en notant T l'apllication linéaire et sa matrice.

En premier lieu nous avons

$$T_{\alpha i} = T(e_i)_\alpha. \tag{11.415}$$

64. Concernant la matrice d'une différentielle, c'est la proposition 13.187. Nous n'en parlerons pas ici parce que c'est pour plus tard.

Donc aussi

$$T(e_i) = \sum_\alpha T_{\alpha i} f_\alpha. \tag{11.416}$$

À ce point, nous avons l'impression de prendre une convention qui donne la matrice à l'envers par rapport à ce que l'on voudrait pour que les indices identiques se suivent. La raison est que la formule (11.418) de l'action d'une application linéaire sur un vecteur sera, elle, plus jolie.

En ce qui concerne l'application d'une matrice à un vecteur, c'est définit en (4.72) ; nous avons alors, pour $x = \sum_i x_i e_i$:

$$T(x) = \sum_i T(e_i) = \sum_{i\alpha} T_{\alpha i} x_i f_\alpha \tag{11.417}$$

ou encore, en pour les composantes :

$$T(x)_\alpha = \sum_i T_{\alpha i} x_i. \tag{11.418}$$

Lorsque nous avons une base orthonormée nous avons aussi

$$A_{ij} = \langle Ae_j, e_i \rangle. \tag{11.419}$$

Ici t est une application $V \to V$ et $A \in \mathbb{M}(n, \mathbb{K})$ est simplement un tableau de nombres sans prétentions d'être une application linéaire. Cependant, A peut être vu comme application linéaire $\mathbb{K} \to \mathbb{K}$, et l'ensemble de nombres $\{x_i\}_{i=1,\dots,n}$ peut être vu comme vecteur de $\mathbb{K}^n$. Dans ce contexte nous pouvons écrire

$$t(x)_i = (Ax)_i. \tag{11.420}$$

Cela signifie que si on identifie un vecteur au vecteur de ses composantes, l'application linéaire se réduit au produit « matrice fois vecteur » sur le corps de base.

Tant que nous y sommes, nous avons aussi la formule suivante dans $\mathbb{R}^n$ muni du produit scalaire usuel :

$$x \cdot Ay = \sum_k x_k (Ay)_k = \sum_{kl} x_k A_{kl} y_l = \sum_{kl} A_{kl} x_k y_l. \tag{11.421}$$

En voila au moins une pour laquelle les indices tombent au bons endroits.

11.11.1 Le changement de base

Soit un espace vectoriel V muni de deux bases $\{e_i\}_{i=1,\dots,n}$ et $\{f_\alpha\}_{\alpha=1,\dots,n}$. Les deux bases sont liées entre elles par

$$f_\alpha = \sum_i Q_{i\alpha} e_i. \tag{11.422}$$

Ici Q n'est pas une application linéaire $V \to V$: 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 $\mathbb{K}^n \to \mathbb{K}^n$.

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.

Lemme 11.206.
Soient des matrices $A, B \in \mathbb{M}(n, \mathbb{K})$. Si pour tout $x, y \in \mathbb{K}^n$ nous avons

$$\sum_{ij} A_{ij} x_i y_j = \sum_{ij} B_{ij} x_i y_j \tag{11.423}$$

alors $A = B$.

Démonstration. Il suffit de choisir $x_i = \delta_{ik}$ et $y_j = \delta_{jl}$, et d'effectuer les sommes ; par exemple

$$\sum_{ij} A_{ij} \delta_{ik} y_j = \sum_j A_{kj} y_j. \tag{11.424}$$

Après avoir effectué toutes les sommes nous nous retrouvons avec $A_{kl} = B_{kl}$, ce qui signifie $A = B$. □

11.11.2 Changement de base : vecteurs de base

Nous multiplions l'égalité (11.422) par $Q^{-1}_{\alpha j}$ [65] et nous sommons sur α :

$$\sum_{\alpha} Q^{-1}_{\alpha j} f_\alpha = \sum_{i\alpha} (A_{i\alpha} Q^{-1}_{\alpha j}) e_i = e_j. \tag{11.425}$$

Donc :

$$e_i = \sum_{\alpha} Q^{-1}_{\alpha i} f_\alpha. \tag{11.426}$$

11.11.3 Changement de base : coordonnées

Soit un vecteur $x \in V$. Il peut être écrit dans les deux bases :

$$x = \sum_i x_i e_i = \sum_\alpha y_\alpha f_\alpha. \tag{11.427}$$

En remplaçant e_i par sa valeur (11.426) nous avons l'égalité

$$\sum_{i\alpha} x_i Q^{-1}_{\alpha i} f_\alpha = \sum_\alpha y_\alpha f_\alpha. \tag{11.428}$$

Vu que les f_α sont linéairement indépendants, l'égalité des sommes donne l'égalité de chacun de termes :

$$y_\alpha = \sum_i x_i Q^{-1}_{\alpha i}. \tag{11.429}$$

En identifiant $x \in V$ au vecteur dans $\mathbb{K}^n$ de ses coordonnées dans la base $\{e_i\}$ nous pouvons écrire

$$y_\alpha = (Q^{-1}x)_\alpha, \tag{11.430}$$

ou pire :

$$y = Q^{-1}x. \tag{11.431}$$

Cette dernière égalité repose 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 $\mathbb{K}^n$.

Une chose agréable avec cette façon d'écrire est que nous trouvons tout de suite la transformation inverse $x = Qy$ qui peut être écrire de différentes manières :

$$x = Qy \tag{11.432a}$$
$$x_i = (Qy)_i \tag{11.432b}$$
$$x_i = \sum_\alpha Q_{i\alpha} y_\alpha \tag{11.432c}$$

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.

11.11.4 Changement de base : matrice d'une application linéaire

Proposition 11.207.
Soit une application linéaire $t\colon V \to V$ de matrices A et B dans les bases $\{e_i\}$ et $\{f_\alpha\}$. Si les bases sont liées par

$$f_\alpha = \sum_i Q_{i\alpha} e_i, \tag{11.433}$$

alors les matrices A et B sont liées par

$$B = Q^{-1}AQ. \tag{11.434}$$

65. 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.

Démonstration. L'hypothèse sur le fait que A et B sont les matrices de t signifie que pour tout $x \in V$,

$$t(x) = \sum_{ij} A_{ji} x_i e_j = \sum_{\alpha\beta} B_{\alpha\beta} y_\beta f_\alpha. \tag{11.435}$$

En remplaçant e_j par son expression (11.426) en termes des f_α et x_i par son expression (11.432b), nous avons

$$(By)_\alpha = \sum_{ij\alpha} A_{ji} (Qy)_i Q^{-1}_{\alpha j} f_\alpha \tag{11.436a}$$

$$= \sum_{i\alpha} (Q^{-1}A)_{\alpha i} (Qy)_i f_\alpha \tag{11.436b}$$

$$= \sum_{\alpha} (Q^{-1}AQy)_\alpha f_\alpha. \tag{11.436c}$$

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

$$B = Q^{-1}AQ. \tag{11.437}$$

□

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.

11.11.5 Changement de base : matrice d'une forme bilinéaire

Soit une forme bilinéaire[66] $q\colon V \times V \to \mathbb{K}$ dont la matrice[67] dans la base $\{e_i\}$ est A et celle dans la base $\{f_\alpha\}$ est B.

Rien n'indique pour l'instant que A et B sont les mêmes qu'avant. Au contraire, nous allons voir qu'elles ne sont en général pas les mêmes.

Soit $x, x' \in V$ de coordonnées (x_i) et (x'_i) dans la base $\{e_i\}$ et (y_α), (y'_α) dans la base $\{f_\alpha\}$. Par définition de la matrice associée à une forme bilinéaire,

$$q(x, x') = \sum_{ij} A_{ij} x_i x'_j = \sum_{\alpha\beta} B_{\alpha\beta} y_\alpha y'_\beta. \tag{11.438}$$

En remplaçant les x_i et x'_i par leurs valeurs en fonction de y_α et y'_β,

$$q(x, x') = \sum_{ij\alpha\beta} A_{ij} Q_{i\alpha} y_\alpha Q_{j\beta} y'_\beta \tag{11.439a}$$

$$= \sum_{\alpha\beta} (Q^t AQ)_{\alpha\beta} y_\alpha y'_\beta \tag{11.439b}$$

où Q^t désigne la transposée de la matrice Q : $Q^t_{ij} = Q_{ji}$. Vu que les nombres y_α et y'_β sont arbitraires nous déduisons[68]

$$B = Q^t AQ. \tag{11.440}$$

Remarque 11.208.
Notons que cette « loi de transformation » n'est pas la même que celle pour une application linéaire. Ici nous avons Q^t alors que pour les applications linéaires nous avions Q^{-1}.

Pour cette raison, tant que nous travaillons avec des bases orthonormées, c'est-à-dire tant que Q est orthogonale[69], nous pouvons confondre une application linéaire avec une application bilinéaire

66. Définition 11.1
67. Définition 11.407.
68. Lemme 11.206.
69. Définition 4.90.

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 (corollaire 11.274) est un résultat de réduction de forme bilinéaire et non d'endomorphismes.

11.11.6 Invariance de la trace

Proposition 11.209 ([1]).
Soit une application linéaire f. Si la matrice de f dans une base est A et est B dans une autre base, alors

$$\mathrm{Tr}(A) = \mathrm{Tr}(B). \tag{11.441}$$

Démonstration. Les matrices A et B sont liées par la proposition 11.207 : $B = Q^{-1}AQ$ où Q est la matrice qui lie les vecteurs des deux bases. L'invariance cyclique de la trace donnée en le lemme 4.59 implique que

$$\mathrm{Tr}(B) = \mathrm{Tr}(Q^{-1}AQ) = \mathrm{Tr}(QQ^{-1}A) = \mathrm{Tr}(A). \tag{11.442}$$

□

11.12 Fonctions

Soient $(V, \|.\|_V)$ et $(W, \|.\|_W)$ 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 caractérisation suivante est un recopiage de la définition 7.66 lorsque la topologie est donnée par des boules.

Proposition 11.210.
Soit $f\colon V \to W$ une fonction de domaine $\mathrm{Dom}(f) \subset V$ et soit a un point d'accumulation de $\mathrm{Dom}(f)$. 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 $x \in \mathrm{Dom}(f)$,

$$0 < \|x - a\|_V < \delta \Rightarrow \|f(x) - \ell\|_W < \varepsilon. \tag{11.443}$$

*Dans ce cas, nous écrivons $\lim_{x\to a} f(x) = \ell$ et nous disons que ℓ est la **limite** de f lorsque x tend vers a.*

Remarque 11.211.
Le fait que nous limitions la formule (11.443) aux x dans le domaine de f n'est pas anodin. Considérons la fonction $f(x) = \sqrt{x^2 - 4}$, de domaine $|x| \geqslant 2$. Nous avons

$$\lim_{x\to 2} \sqrt{x^2 - 4} = 0. \tag{11.444}$$

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 dons 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 $[2, \infty[$.

11.13 Sous espaces caractéristiques

Lorsqu'un opérateur n'est pas diagonalisable, les valeurs propres jouent quand même un rôle important.

Définition 11.212.
Soit E un $\mathbb{K}$-espace vectoriel $f \in \mathrm{End}(E)$. Pour $\lambda \in \mathbb{K}$ nous définissons

$$F_\lambda(f) = \{v \in E \text{ tel que } (f - \lambda\mathbb{1})^n v = 0, n \in \mathbb{N}\} \tag{11.445}$$

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 11.213.
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

$$(f - \lambda\mathbb{1})^n f(x) = f\big((f - \lambda\mathbb{1})^n x\big) = 0, \tag{11.446}$$

par conséquent $f(x) \in F_\lambda(f)$. □

Remarque 11.214.
Toute matrice sur $\mathbb{C}$ n'est pas diagonalisable : nous en avons déjà donné une exemple simple en 11.263. Nous en voyons maintenant un moins simple. Considérons en effet l'endomorphisme f donné par la matrice

$$\begin{pmatrix} a & \alpha & \beta \\ 0 & a & \gamma \\ 0 & 0 & b \end{pmatrix} \tag{11.447}$$

où $a \neq b$, $\alpha \neq 0$, β et γ sont des nombres complexes quelconques. Son polynôme caractéristique est

$$\chi_f(\lambda) = (a - \lambda)^2 (b - \lambda), \tag{11.448}$$

et les valeurs propres sont donc a et b. Nous trouvons les vecteurs propres pour la valeur a en résolvant

$$\begin{pmatrix} a & \alpha & \beta \\ 0 & a & \gamma \\ 0 & 0 & b \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} ax \\ ay \\ az \end{pmatrix}. \tag{11.449}$$

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

$$\begin{pmatrix} \frac{1}{b-a}\left(\beta + \frac{\alpha\gamma}{b-a}\right) \\ \frac{\gamma}{b-a} \\ 1 \end{pmatrix}. \tag{11.450}$$

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

$$(f - \alpha\mathbb{1})^2 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a & \alpha & \beta \\ 0 & a & \gamma \\ 0 & 0 & b \end{pmatrix} \begin{pmatrix} \alpha \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} a\alpha \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \tag{11.451}$$

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.

11.13.1 Théorèmes de décomposition

Théorème 11.215 (Théorème spectral, décomposition primaire)**.**
Soit E espace vectoriel de dimension finie sur le corps algébriquement clos $\mathbb{K}$ et $f \in \mathrm{End}(E)$. Alors

$$E = F_{\lambda_1}(f) \oplus \dots \oplus F_{\lambda_k}(f) \tag{11.452}$$

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

$$P = (f - \lambda_1)^{\alpha_1} \dots (f - \lambda_r)^{\alpha_r} \tag{11.453}$$

en facteurs irréductibles. La le théorème de noyaux (11.127) nous avons

$$E = \ker(f - \lambda_1)^{\alpha_1} \oplus \dots \oplus \ker(f - \lambda_r)^{\alpha_r}. \tag{11.454}$$

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

$$\ker(f - \lambda_i)^{\alpha_i} \subset F_{\lambda_i}(f) \tag{11.455}$$

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

$$\begin{cases} (f - \lambda_i)w = 0 & \text{(11.456a)} \\ (f - \lambda_j)w = 0. & \text{(11.456b)} \end{cases}$$

Ce w serait donc un vecteur propre simultané 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

$$\sum_i \dim F_{\lambda_i}(f) \leqslant \dim E. \tag{11.457}$$

En tenant compte de l'inclusion (11.455) nous avons même

$$\dim E = \sum_i \dim \ker(f - \lambda_i)^{\alpha_i} \leqslant \sum_i F_{\lambda_i}(f) \leqslant \dim E. \tag{11.458}$$

Par conséquent nous avons $\dim \ker(f - \lambda_i)^{\alpha_i} = \dim F_{\lambda_i}(f)$ et l'égalité des deux espaces. □

Problèmes et choses à faire

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-simples [70] sont les endomorphismes diagonaux.

Théorème 11.216 (Décomposition de Dunford)**.**
Soit E un espace vectoriel sur le corps algébriquement clos $\mathbb{K}$ et $u \in \mathrm{End}(E)$ un endomorphisme de E.

(1) L'endomorphisme u se décompose de façon unique sous la forme

$$u = s + n \tag{11.459}$$

où s est diagonalisable, n est nilpotent et $[s, n] = 0$.

70. Définition 11.141.

(2) *Les endomorphismes s et n sont des polynômes en u et commutent avec u.*

(3) *Les parties s et n sont données par*

$$s = \sum_i \lambda_i p_i \tag{11.460a}$$

$$n = \sum_i (s - \lambda_i \mathbb{1}) p_i \tag{11.460b}$$

où les sommes sont sur les valeurs propres distinctes[71] *de f et où $p_i : E \to F_{\lambda_i}(u)$ est la projection de E sur $F_{\lambda_i}(u)$.*

Démonstration. Le théorème spectral 11.215 nous indique que

$$E = \bigoplus_i F_{\lambda_i}(f). \tag{11.461}$$

Nous considérons l'endomorphisme s de E qui consiste à dilater d'un facteur λ l'espace caractéristique $F_\lambda(f)$:

$$s = \sum_i \lambda_i p_i \tag{11.462}$$

où $p_i : E \to F_{\lambda_i}(u)$ 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

$$f - s : F_\lambda(f) \to F_\lambda(f). \tag{11.463}$$

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

$$s'u = s'^2 + s'n' = s'^2 + n's' = (s' + n')s' = us', \tag{11.464}$$

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 diagonalisibilité.

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 11.170, 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,

$$(A + B)^n = \sum_{k=0}^{n} \binom{k}{n} A^k B^{n-k}. \tag{11.465}$$

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 $s = s'$.

□

71. C'est-à-dire sur les sous-espaces caractéristiques.

11.13.2 Diverses conséquences

Théorème 11.217.
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 11.216) : il existe une matrice inversible P telle que

$$A = P^{-1}(D + N)P \tag{11.466}$$

où D est diagonale, N est nilpotente et $[D, N] = 0$. Étant donné que $D + N$ est triangulaire, son polynôme caractéristique que

$$\chi_{D+N}(\lambda) = \prod_i D_{ii} - \lambda. \tag{11.467}$$

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

$$A^k = P^{-1}(D + N)^k P \tag{11.468a}$$

$$= P^{-1} \sum_{j=0}^{k} \binom{j}{k} D^{j-k} N^j P \tag{11.468b}$$

$$= P^{-1} \sum_{j=0}^{n-1} \binom{j}{k} D^{j-k} N^j P \tag{11.468c}$$

où nous avons utilité 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

$$\|(D + N)^k\| \leqslant \sum_{j=0}^{k} \binom{j}{k} \rho(D)^{k-j} \|N\|^j. \tag{11.469}$$

Du coup si $\rho(D) < 1$ alors $\|(D + N)^k\| \to 0$ (et c'est même un si et seulement si). □

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 16.115 une formule pour le logarithme sous forme d'une série ; ce logarithme sera réel.

11.13.3 Valeurs singulières

Définition 11.218.
*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*

$$Mv = \sigma u \tag{11.470a}$$

$$M^* u = \sigma v. \tag{11.470b}$$

Théorème 11.219 (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

$$M = ADB \tag{11.471}$$

où il existe deux matrices unitaires $A \in \mathrm{U}(m \times m)$, $B \in \mathrm{U}(n \times n)$ et une matrice (pseudo)diagonale $D \in \mathbb{M}(m \times n)$ tels que

(1) $A \in \mathrm{U}(m \times m)$, $B \in \mathrm{U}(n \times n)$ *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 rang*[72] *de* M*.*

Corollaire 11.220.
Soit $M \in \mathbb{M}(n, \mathbb{C})$*. Il existe un isomorphisme* $f : \mathbb{C}^n \to \mathbb{C}^n$ *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. □

11.14 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 sections 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 sujet[73]. 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.

11.14.1 Extension des applications linéaires

Définition 11.221 ([158])**.**
L'espace vectoriel obtenu par ***extension du corps de base*** *de* E *est l'espace vectoriel*

$$E_{\mathbb{L}} = \mathbb{L} \otimes_{\mathbb{K}} E. \tag{11.472}$$

Ce dernier est le quotient $\mathbb{L} \otimes_{\mathbb{K}} E = (\mathbb{L} \times E)/\sim$ *par la relation d'équivalence*

$$(\lambda, v) \sim \left(a\lambda, \frac{1}{a} v\right) \tag{11.473}$$

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 $f : E \to F$ est une applications linéaire nous définissons

$$\begin{aligned} f_{\mathbb{L}} : E_{\mathbb{L}} &\to F_{\mathbb{L}} \\ [\lambda, v] &\mapsto [\lambda, f(v)]. \end{aligned} \tag{11.474}$$

Remarque 11.222.
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

$$\begin{aligned} \iota : E &\to E_{\mathbb{L}} \\ v &\mapsto [1, v]. \end{aligned} \tag{11.475}$$

Proposition 11.223 ([66])**.**
Injectivité et surjectivité respectées.

(1) L'application $f_{\mathbb{L}}$ *est injective si et seulement si* f *est injective.*

72. Définition 4.38.
73. 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

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ {\scriptstyle\tau}\downarrow & & \downarrow{\scriptstyle\tau} \\ E_{\mathbb{L}} & \xrightarrow[f_{\mathbb{L}}]{} & F_{\mathbb{L}} \end{array} \tag{11.476}$$

est un diagramme commutatif. En effet

$$(\tau \circ f)(v) = [1, f(v)] \tag{11.477}$$

tandis que

$$(f_{\mathbb{L}\circ\tau})(v) = f_{\mathbb{L}}[1, v] = [1, f(v)]. \tag{11.478}$$

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 4.50(1), nous savons qu'il existe $g\colon F \to E$ telle que $f \circ g = \mathrm{Id}\,|_F$. Nous en déduisons que $f_{\mathbb{L}} \circ g_{\mathbb{L}} = \mathrm{Id}\,|_{F_{\mathbb{L}}}$ parce que si $[\lambda, v] \in F_{\mathbb{L}}$ alors

$$(f_{\mathbb{L}} \circ g_{\mathbb{L}})[\lambda, v] = f_{\mathbb{L}}[\lambda, g(v)] = [\lambda, (f \circ g)(v)] = [\lambda, v]. \tag{11.479}$$

Notons que g est injective, donc $g_{\mathbb{L}}$ est injective et l'égalité $f_{\mathbb{L}} \circ g_{\mathbb{L}} = \mathrm{Id}\,|_{F_{\mathbb{L}}}$ implique que $f_{\mathbb{L}}$ est également injective. □

Proposition 11.224 ([1, 159])**.**
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

$$\lambda \otimes ke_i = \frac{\lambda}{k} \otimes e_i = \frac{\lambda}{k}(1 \otimes e_i). \tag{11.480}$$

Cela pour introduire que l'application

$$\begin{aligned} \psi\colon \mathbb{L} \otimes_{\mathbb{K}} E &\to \bigoplus_i \mathbb{L}(1 \otimes e_i) \\ \sum_k \lambda_k \otimes v_k &\mapsto \oplus_i \sum_k (\lambda_k v_{ik})(1 \otimes e_i) \end{aligned} \tag{11.481}$$

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

$$\sum_i \sum_k (\lambda_k v_{ik})(1 \otimes e_i) = 0 \tag{11.482}$$

alors les choses suivantes sont nulles également :

$$\sum_i \sum_k (\lambda_k v_{ik})(1 \otimes e_i) = \sum_{ik} (\lambda_k \otimes v_{ik}e_i) = \sum_k (\lambda_k \otimes \sum_i v_{ik}e_i) = \sum_k (\lambda_k \otimes v_k). \tag{11.483}$$

Le dernier est l'argument de ψ. Le fait que ce soit nul implique que ψ est injective. □

Remarque 11.225.
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.

Corollaire 11.226.
La $\mathbb{L}$-dimension de $E_{\mathbb{L}}$ est égale à la $\mathbb{K}$-dimension de E.

11.14.2 Projections

Problèmes et choses à faire

Nous allons définir $\texttt{proj}\colon \mathcal{L}(E_{\mathbb{L}}, F_{\mathbb{L}}) \to \mathcal{L}(E, F)$ en faisant appel à des bases et en prouvant que les choses définies ne dépendent pas des bases choisies. Il y a surement 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 6.54). 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

$$\mathbb{L} = \mathbb{K} \oplus V. \tag{11.484}$$

Nous avons alors naturellement une projection $\texttt{proj}\colon \mathbb{L} \to \mathbb{K}$.

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 11.224, ce sont des bases de $E_{\mathbb{L}}$ et $F_{\mathbb{L}}$. Si la fonction $f\colon E_{\mathbb{L}} \to F_{\mathbb{L}}$ s'écrit dans ce ces bases comme

$$f(e_i) = \sum_a f_{ai} e_a \tag{11.485}$$

alors nous définissons $\texttt{proj}(f)$ par

$$(\texttt{proj}\, f)e_i = \sum_a \texttt{proj}(f_{ai}) e_a. \tag{11.486}$$

Proposition 11.227 ([1]).
L'application `proj` *définie en* (11.486) *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 $\texttt{proj}$. La première est la projection $\texttt{proj}\colon \mathbb{L} \to \mathbb{K}$ qui ne dépend que d'un choix de supplémentaire et que nous supposons fixée ici. D'autre part il y a $\texttt{proj}\colon E_{\mathbb{L}} \to E$ qui dépend a priori des bases choisies.

Nous choisissons de nouvelles bases qui sont liées aux anciennes bases par

$$\begin{cases} e'_b = \sum_a B_{ab} e_a & \text{(11.487a)} \\ e'_i = \sum_j A_{ji} e_j. & \text{(11.487b)} \end{cases}$$

Les matrices A et B sont dans $\mathrm{GL}(\mathbb{K})$. Nous allons écrire l'opérateur $\texttt{proj}'$ qui correspond à ces bases et montrer que pour toute application linéaire $f\colon E_{\mathbb{L}} \to F_{\mathbb{L}}$ nous avons $\texttt{proj}(f) = \texttt{proj}'(f)$. Nous avons :

$$\begin{aligned} f(e'_j) &= \sum_i A_{ji} f(e_i) && \text{(11.488a)} \\ &= \sum_a \sum_b \sum_i A_{ji} f_{ai} (B^{-1})_{ba} e'b && \text{(11.488b)} \\ &= \sum_b \Big(\sum_{ai} A_{ji} f_{ai} (B^{-1})_{ba} \Big) e'b, && \text{(11.488c)} \end{aligned}$$

ce qui fait que

$$(\texttt{proj}'\, f)e'_j = \sum_b \Big(\texttt{proj}\left(A_{ji} f_{ai} (B^{-1})_{ba} \right) \Big) e'_b. \tag{11.489}$$

Nous calculons maintenant $(\texttt{proj}'\, f)e_j$ en substituant $e_j = \sum_l (A^{-1})_{lj} e'_l$ et en utilisant (11.489) et la linéarité de $\texttt{proj}'$ et la $\mathbb{K}$-linéarité de $\texttt{proj}\colon \mathbb{L} \to \mathbb{K}$:

$$\begin{aligned} (\texttt{proj}'\, f)\Big(\sum_l (A^{-1})_{lj} e'_l \Big) &= \sum_l (A^{-1})_{lj} \sum_b \sum_{ai} \texttt{proj}\left(A_{li} f_{ai} (B^{-1})_{ba} \right) e_b && \text{(11.490a)} \\ &= \sum_a \texttt{proj}(f_{aj}) e_a && \text{(11.490b)} \\ &= (\texttt{proj}\, f)e_j. && \text{(11.490c)} \end{aligned}$$

Donc $\texttt{proj} = \texttt{proj}'$. □

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 11.228 ([1])**.**
L'opération $\texttt{proj}\colon \mathcal{L}(E_{\mathbb{L}}, F_{\mathbb{L}}) \to \mathcal{L}(E, F)$ ne dépend pas des bases choisies un peu partout. Mais elle dépend de l'application $pr\colon \mathbb{L} \to \mathbb{K}$ déjà construite. Et celle-là dépend du choix d'un supplémentaire V qui fournit $\mathbb{L} = \mathbb{K} \oplus V$.

Si $\texttt{proj}(\lambda) = 0$ pour un de ces choix, cela n'implique nullement que $\lambda = 0$. Penser à $i \in \mathbb{C}$ si la projection $\texttt{proj}\colon \mathbb{C} \to \mathbb{R}$ est l'application $(x + iy) \mapsto x$ parallèle à l'axe des imaginaires.

Par contre si $\texttt{proj}(\lambda) = 0$ pour tout choix de V, alors nous avons bien $\lambda = 0$. Dans la suit nous « fixons » un choix de V générique, et lorsque nous rencontrerons l'égalité $\texttt{proj}(\lambda) = 0$ nous en déduirons $\lambda = 0$.

Proposition 11.229.
Si $f\colon E \to F$ 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) $\texttt{proj}\, f_{\mathbb{L}} = f$,

(2) $(f_{\mathbb{L}})_{ja} = f_{ja} \in \mathbb{K}$.

Démonstration. Nous avons

$$f_{\mathbb{L}}(e_i) = \sum_a f_{ai}(1 \otimes e_a) = \sum_a f_{ai}\tau(e_a), \tag{11.491}$$

donc

$$(\texttt{proj}\, f_{\mathbb{L}})e_i = \sum_a \texttt{proj}(f_{ai})e_a = \sum_a f_{ai}e_a = f(e_i). \tag{11.492}$$

Cela prouve que $\texttt{proj}\, f_{\mathbb{L}} = f$.

Par ailleurs,

$$f_{\mathbb{L}}(\tau e_i) = f_{\mathbb{L}}(1 \otimes e_i) = 1 \otimes f(e_i) = \tau\big(f(e_i)\big) = \sum_a f_{ai}\tau(e_a) \tag{11.493}$$

alors que par définition,

$$f_{\mathbb{L}}(\tau e_i) = \sum_a (f_{\mathbb{L}})_{ai}\tau(e_a). \tag{11.494}$$

Les éléments $\tau(e_a)$ formant une base[74], la comparaison de (11.493) avec (11.494) donne $(f_{\mathbb{L}})_{ai} = f_{ai} \in \mathbb{K}$. □

Lemme 11.230.
Soient

(1) Une base $\{e_i\}$ de E et une application linéaire $f\colon E \to F$;

(2) une base $\{e_a\}$ de F et une application linéaire $g\colon G \to F$;

(3) une base $\{e_\alpha\}$ de G et une application linéaire $\tilde{h}\colon G_{\mathbb{L}} \to E_{\mathbb{L}}$.

Alors nous avons

$$\texttt{proj}(f_{\mathbb{L}} \circ \tilde{h}) = \texttt{proj}(f_{\mathbb{L}}) \circ \texttt{proj}(\tilde{h}). \tag{11.495}$$

Démonstration. Pour écrire $\texttt{proj}(f_{\mathbb{L}} \circ \tilde{h})$ à partir de la définition (11.486) nous commençons par écrire

$$(f_{\mathbb{L}} \circ \tilde{h})e_\alpha = \sum_a (f_{\mathbb{L}} \circ \tilde{h})_{a\alpha}e_a = \sum_{ai} (f_{\mathbb{L}})_{ai}(\tilde{h})_{i\alpha}e_a = \sum_a \Big(\sum_i f_{ai}(\tilde{h})_{i\alpha}\Big)e_a \tag{11.496}$$

où nous avons utilisé le fait que $(f_{\mathbb{L}})_{ai} = f_{ai}$. Donc, en utilisant la $\mathbb{K}$-linéarité de $\texttt{proj}$,

$$\texttt{proj}(f_{\mathbb{L}} \circ \tilde{h})e_\alpha = \sum_a \sum_i \texttt{proj}\Big(f_{ai}(\tilde{h})_{i\alpha}\Big)e_a = \sum_a \sum_i f_{ai}\,\texttt{proj}\Big((\tilde{h})_{i\alpha}\Big)e_a. \tag{11.497}$$

74. Encore la proposition 11.224.

D'autre part,

$$\begin{aligned}\texttt{proj}(f_{\mathbb{L}})\circ\texttt{proj}(\tilde{h})e_\alpha &= \texttt{proj}(f_{\mathbb{L}})\sum_i \texttt{proj}\Big((\tilde{h})_{i\alpha}\Big)e_i\\ &= \sum_i \texttt{proj}\Big((\tilde{h})_{i\alpha}\Big)\sum_a f_{ai}e_a\\ &= \sum_{ai}\texttt{proj}\Big((\tilde{h})_{i\alpha}\Big)f_{ai}e_a,\end{aligned} \tag{11.498}$$

et c'est égal à (11.497). □

Remarque 11.231.
Nous n'avons en général pas $\texttt{proj}(xy) = \texttt{proj}(x)\,\texttt{proj}(y)$ pour tout $x, y \in \mathbb{L}$. Par exemple si $\mathbb{K} = \mathbb{R}$ et $\mathbb{L} = \mathbb{C}$ avec la projection canonique,

$$\texttt{proj}(i \cdot i) = \texttt{proj}(-1) = -1 \tag{11.499}$$

alors que $\texttt{proj}(i) = 0$.

Proposition 11.232.
Soient $f \in \mathcal{L}(E, F)$ et $g \in \mathcal{L}(F, E)$. Alors il existe $h\colon G \to E$ tel que $f \circ h = g$ si et seulement s'il existe $\tilde{g}\colon G_{\mathbb{L}} \to E_{\mathbb{L}}$ 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 $\tilde{h}\colon G_{\mathbb{L}} \to E_{\mathbb{L}}$ tel que $f_{\mathbb{L}} \circ \tilde{h} = g_{\mathbb{L}}$ alors en appliquant $\texttt{proj}$ des deux côtés et en utilisant le lemme 11.230,

$$\texttt{proj}(f_{\mathbb{L}}) \circ \texttt{proj}(\tilde{h}) = \texttt{proj}(g_{\mathbb{L}}) \tag{11.500}$$

c'est-à-dire

$$f \circ \texttt{proj}(\tilde{h}) = g, \tag{11.501}$$

c'est-à-dire que l'application $\texttt{proj}\,\tilde{h}\colon G \to E$ est la réponse à la proposition. □

11.14.3 Rang, polynôme minimal, polynôme caractéristique

Proposition 11.233 (Stabilité du rang par extension des scalaires[66])**.**
Si $f\colon E \to F$ est linéaire alors nous avons

$$\operatorname{rang}(f) = \operatorname{rang}(f_{\mathbb{L}}). \tag{11.502}$$

où à droite nous considérons le rang de l'application $\mathbb{L}$-linéaire $f_{\mathbb{L}}\colon E_{\mathbb{L}} \to F_{\mathbb{L}}$.

Démonstration. Il existe un supplémentaire V tel que $E = \ker(f) \oplus V$ avec $\dim(V) = \operatorname{rang}(f)$. Nous pouvons factoriser f en

$$f = f_2 \circ f_1 \tag{11.503}$$

avec $f_1\colon E \to V$ est la projection parallèle à $\ker(f)$ et est surjective (vers V) parce que $\dim(V) = \operatorname{rang}(f) = \dim\big(\text{Image}(f)\big)$. De plus $f_2\colon V \to F$ est injective parce que si $v \in V$ est tel que $f_2(v) = 0$ alors on aurait

$$f(v) = (f_2 \circ f_1)(v) = f_2(v) = 0. \tag{11.504}$$

Cela donne $v \in \ker(f) \cap V = \{0\}$. Par la proposition 11.223, les applications $(f_1)_{\mathbb{L}}$ et $(f_2)_{\mathbb{L}}$ sont respectivement surjective et injective.

L'application $(f_2)_{\mathbb{L}}\colon V_{\mathbb{L}} \to F_{\mathbb{L}}$ est forcément surjective sur son image, donc

$$(f_2)_{\mathbb{L}}\colon V_{\mathbb{L}} \to \text{Image}(f_{\mathbb{L}}) \tag{11.505}$$

est un isomorphisme de $\mathbb{L}$-espaces vectoriels. Nous avons alors les égalités

$$\dim_{\mathbb{L}}(V_{\mathbb{L}}) = \dim_{\mathbb{L}}\big(\text{Image}(f_{\mathbb{L}})\big) = \operatorname{rang}(f_{\mathbb{L}}). \tag{11.506}$$

Mais aussi, par les définitions posées plus haut,

$$\dim(V) = \operatorname{rang}(f) = \dim\big(\text{Image}(f)\big). \tag{11.507}$$

Mais le corollaire 11.226 nous dit que $\dim_{\mathbb{L}}(V_{\mathbb{L}}) = \dim_{\mathbb{K}}(V)$. Donc il y a égalité des deux lignes (11.506) et (11.507) donne $\operatorname{rang}(f) = \operatorname{rang}(f_{\mathbb{L}})$. □

Proposition 11.234.
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 11.229(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 11.146) : 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 $\mathbb{K}$. □

La situation est très différente avec le polynôme minimal[75]. 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 11.235 ([66, 1])**.**
Soit $\mathbb{L}$ une extension du corps $\mathbb{K}$ et une application linéaire $f\colon E \to F$ entre deux $\mathbb{K}$-espaces vectoriels. Alors $\mu_f = \mu_{f_{\mathbb{L}}}$.

Démonstration. Nous allons montrer que l'application

$$\begin{aligned} \tilde{g}\colon \frac{\mathbb{L}[X]}{(\mu)} &\to \operatorname{End}(E_{\mathbb{L}}) \\ \bar{P} &\mapsto P(f_{\mathbb{L}}) \end{aligned} \tag{11.508}$$

est bien définie et injective. La proposition 11.136 nous dira alors que μ est le polynôme minimal de $f_{\mathbb{L}}$.

Pour prouver que l'application $\tilde{g}$ est bien définie, nous commençons par prouver que $P(f_{\mathbb{L}}) = P(f)_{\mathbb{L}}$:

$$\begin{aligned} P(f_{\mathbb{L}})\lambda \otimes v &= \sum_k a_k f_{\mathbb{L}}^k \lambda \otimes v && \text{(11.509a)} \\ &= \lambda \otimes \sum_k a_k f^k(v) && \text{(11.509b)} \\ &= \lambda \otimes P(f)v && \text{(11.509c)} \\ &= P(f)_{\mathbb{L}}\lambda \otimes v. && \text{(11.509d)} \end{aligned}$$

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 $\operatorname{End}(E_{\mathbb{L}})$ nous considérons une base qui commence[76] 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

$$\sum_k \texttt{proj}\left(\lambda_k f_{\mathbb{L}}^k\right) = 0. \tag{11.510}$$

75. Définition 6.60.
76. Théorème de la base incomplète 4.11(2).

Pour détailler ce que cela implique, nous calculons ceci :

$$(\lambda f_{\mathbb{L}})(\tau e_i) = \lambda f_{\mathbb{L}}(\tau e_i) = \sum_a \lambda f_{ia} e_a, \tag{11.511}$$

par conséquent $\texttt{proj}(\lambda f_{\mathbb{L}})e_i = \sum_a \texttt{proj}(\lambda f_{ia})e_a$, et comme $\texttt{proj}$ est $\mathbb{K}$-linéaire et que $f_{ai} \in \mathbb{K}$,

$$\texttt{proj}(\lambda f_{\mathbb{L}})e_i = \texttt{proj}(\lambda) \sum_a f_{ai} e_a = \texttt{proj}(\lambda)\,\texttt{proj}(f_{\mathbb{L}})e_i = \texttt{proj}(\lambda) f(e_i). \tag{11.512}$$

Appliquer la projection $\texttt{proj}$ à l'équation (11.510) donne alors $\sum_k \texttt{proj}(\lambda)_k f^k = 0$. Mais comme les f^k sont linéairement indépendantes sur $\mathbb{K}$ nous avons pour tout k : $\texttt{proj}(\lambda_k) = 0$ (égalité dans $\mathbb{K}$). En nous souvenant de la remarque 11.228 nous en déduisons $\lambda_k = 0$ dans $\mathbb{L}$.

Dans les choix de bases faits, l'application $\tilde{g}$ a la forme

$$\tilde{g} = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ * & * & * & \\ * & * & * & \\ * & * & * & \end{pmatrix}, \tag{11.513}$$

qui est injective.

Vu que $\tilde{g}$ est injective, μ est le polynôme minimal de $f_{\mathbb{L}}$ et donc $\mu = \mu_{\mathbb{L}}$. □

11.15 Frobenius et Jordan

11.15.1 Matrice compagnon

Définition 11.236.
*Soit le polynôme $P = X^n - a_{n-1}X^{n-1} - \ldots - a_1 X - a_0$ dans $\mathbb{K}[X]$. La **matrice compagnon** de P est la matrice donnée par*

$$C(P) = \begin{pmatrix} 0 & \cdots & \cdots & 0 & a_0 \\ 1 & 0 & & \vdots & a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & a_{n-2} \\ 0 & \cdots & 0 & 1 & a_{n-1} \end{pmatrix} \tag{11.514}$$

si $n \geqslant 2$ et par (a_0) si $n = 1$.

Une matrice est dite compagnon si elle a cette forme.

Proposition 11.237.
Si f est l'endomorphisme associé à la matrice $C(P)$ nous avons

$$f(e_i) = \begin{cases} e_{i+1} & \text{si } i < n \\ (a_0, \ldots, a_{n-1}) & \text{si } i = n. \end{cases} \tag{11.515}$$

De plus l'endomorphisme f vérifie $P(f)e_1 = 0$.

Lemme 11.238 ([160]).
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, $\big(f^i(e_1)\big)_{i=1,\dots,n-1}$ est libre, donc le polynôme minimal ponctuel en e_1 est de degré n au minimum. En reprenant les notations du théorème 6.36, 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. □

Remarque 11.239.
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.

11.15.2 Réduction de Frobenius

Lemme 11.240.
Soit un endomorphisme $f\colon E \to E$ 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 11.253 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 combinaisons 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 11.154), donc il est le polynôme minimal. □

Théorème 11.241 (Réduction de Frobenius [161, 162, 163])**.**
Soit E, un $\mathbb{K}$-espace vectoriel, et $f \in \mathrm{End}(E)$. 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

$$\chi_f = \prod_{i=1}^{r} \mu_i \tag{11.516a}$$

$$\mu_f = \mu_1 \tag{11.516b}$$

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 cycliques[77], leurs polynôme caractéristiques sont égaux à leurs polynômes minimaux (lemme 11.240). Cela prouve l'égalité (11.516a). Ensuite tous les μ_i doivent diviser le polynôme minimal, donc $\mathrm{ppcm}(\mu_1, \dots, \mu_r)$ 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 $\mathrm{ppcm}(\mu_1, \dots, \mu_r) = \mu_f$. Mais par ailleurs $\mu_1 = \mathrm{ppcm}(\mu_1, \dots, \mu_r)$ parce qu'on a supposé $\mu_{i+1} \mid \mu_i$, donc $\mu_1 = \mu_f$.

77. Définition 11.138.

Soit d, le degré du polynôme minimal de f et $y \in E$ tel que $\mu_f = \mu_{f,y}$ (voir lemme 11.137). Le plus petit espace stable sous f contenant y est

$$E_y = \text{Span}\{y, f(y), \dots, f^{d-1}(y)\}. \tag{11.517}$$

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'était pas linéairement indépendants, alors nous aurions des a_k tels que $\sum_k a_k e_k = 0$ et avec lesquels

$$\big(\sum_k a_k X^k\big)(f)y = 0, \tag{11.518}$$

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 étendre [78] $\{e_1, \dots, e_d\}$ en une base $\{e_1, \dots, e_n\}$ de E. Ensuite nous allons montrer que

$$E = E_y \oplus F \tag{11.519}$$

avec

$$F = \{x \in E \text{ tel que } e_d^*\big(f^k(x)\big) = 0 \forall k \in \mathbb{N}\}. \tag{11.520}$$

Par construction, F est invariant sous f. Montrons pour commencer que $E_y \cap F = \{0\}$. Un élément de E_y s'écrit

$$z = a_1 e_1 + \cdots + a_k e_k \tag{11.521}$$

avec $k \leqslant d$. Étant donné que f décale les vecteurs de base, nous avons $e_d^*\big(f^{d-k}(z)\big) = a_k$. Du coup $z \in F$ si et seulement si $a_1 = \ldots = a_d = 0$, c'est-à-dire que $E_y \cap F = \{0\}$.

Nous montrons maintenant que $\dim F = n - d$. Pour cela nous considérons l'application

$$\begin{aligned} T\colon \mathbb{K}[F] &\to E^* \\ g &\mapsto e_d^* \circ g. \end{aligned} \tag{11.522}$$

Cette application est injective. En effet un élément général de $\mathbb{K}[f]$ est

$$g = a_1 \,\text{Id} + a_2 f + \cdots + a_p f^{p-1} \tag{11.523}$$

avec $p \leqslant d$. Si $T(g) = 0$, alors nous avons en particulier

$$0 = T(g)e_{d-p+1} = e_d^*(a_1 e_{d-p+1} + a_2 e_{d-p+2} + \cdots + a_p e_d) = a_p. \tag{11.524}$$

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.

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 :

$$\begin{aligned} (\text{Image}(T))^\perp &= \{x \in E \text{ tel que } T(g)x = 0 \forall g \in \mathbb{K}[f]\} && \text{(11.525a)} \\ &= \{x \in E \text{ tel que } e_d^*\big(g(x)\big) = 0 \forall g \in \mathbb{K}[f]\} && \text{(11.525b)} \\ &= F. && \text{(11.525c)} \end{aligned}$$

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 $f|_{E_y j}$, alors par le lemme 11.139 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

78. Pour autant que j'aie compris, cette extension manque dans [161]. Corrigez moi si je me trompe.

(1) $E = \bigoplus_{i=1}^{r} F_i$,
(2) $f|_{F_i}$ est cyclique,
(3) $\mu_{f|_{F_{i+1}}}$ 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 (11.516). Nous supposons que $P_i = Q_i$ pour $i \leqslant 1 \leqslant j-1$ et nous tentons de montrer que $P_j = Q_j$.

Nous avons

$$P_j(f) = P_j(f)|_{F_1} \oplus \ldots \oplus P_j(f)|_{F_{j-1}}. \tag{11.526}$$

En effet étant donné que P_{j+k} divise P_j, nous avons [79] $P_j(f) = A(f) \circ P_{j+k}(f)$, mais $P_{j+k}(f)F_{j+k} = 0$, donc $P_j(f)F_{j+k} = 0$. Les espaces G_i n'ayant a priori aucun rapport avec les polynômes P_i, nous écrivons

$$P_j(f) = P_j(f)|_{G_1} \oplus \ldots \oplus P_j(f)|_{G_{j-1}} \oplus P_j(f)|_{G_j} \oplus \ldots \oplus P_j(f)|_{G_s}. \tag{11.527}$$

Pour $1 \leqslant i \leqslant j-1$, 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,

$$\dim P_j(f)F_i = \dim P_j(f)G_i. \tag{11.528}$$

En prenant les dimensions des images dans les égalités (11.526) et (11.527), nous trouvons que

$$P_j(f)|_{G_j} = \ldots = P_j(f)|_{G_s} = 0. \tag{11.529}$$

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 11.242.
Sous forme matricielle, ce théorème dit que toute matrice est semblable à une matrice de la forme bloc-diagonale

$$f = \begin{pmatrix} C_{\mu_1} & & \\ & \ddots & \\ & & C_{\mu_r} \end{pmatrix} \tag{11.530}$$

où les C_{μ_i} sont les matrices compagnon (définition 11.236).

En particulier, et ceci est très important, deux applications sont semblables si et seulement si elles ont même suite d'invariants de similitude.

Remarque 11.243.
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.

11.15.3 Forme normale de Jordan

Il existe une preuve directe de la réduction de Jordan ne nécessitant pas la réduction de Frobenius[153]. Cette dernière passe par les espaces caractéristiques [80] 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.

79. En vertu du lemme 11.126.
80. Aussi appelés « espaces propres généralisés ».

Théorème 11.244 (Réduction de Jordan)**.**
Soit E un espace vectoriel sur $\mathbb{K}$, et $f \in \mathrm{End}(E)$ un endomorphisme dont le polynôme caractéristique χ_f est scindé[81]*. Il existe une base de E dans laquelle la matrice de f s'écrit sous la forme*

$$M = \begin{pmatrix} J_{n_1}(\lambda_1) & & \\ & \ddots & \\ & & J_{n_k}(\lambda_k) \end{pmatrix} \tag{11.531}$$

où les λ_i sont les valeurs propres de f (avec éventuelle répétitions) et $J_n(\lambda)$ représente le bloc $n \times n$

$$J_n(\lambda) = \begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \lambda & & \\ & & & \ddots & 1 \\ & & & & \lambda \end{pmatrix}. \tag{11.532}$$

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 11.238 que (la matrice de) f est semblable à sa matrice compagnon. En l'occurrence pour f nous avons

$$C_{X^m} = \begin{pmatrix} 0 & & & 0 \\ 1 & \ddots & & \vdots \\ & \ddots & \ddots & \vdots \\ & & 1 & 0 \end{pmatrix}. \tag{11.533}$$

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

$$\chi_f = (X - \lambda_1)^{l_1} \dots (X - \lambda_m)^{l_m}. \tag{11.534}$$

Le lemme des noyaux (théorème 11.127) nous enseigne que

$$E = \bigoplus_{i=1}^{m} \underbrace{\ker(f - \mu_i \mathbb{1})^{l_i}}_{F_i}. \tag{11.535}$$

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

$$f|_{F_i} = (f - \lambda_i \mathbb{1})|_{F_i} + \lambda_i \mathbb{1}_{F_i}, \tag{11.536}$$

nous voyons que $f|_{F_i}$ s'écrit comme un bloc de Jordan avec λ_i sur la diagonale. □

Remarque 11.245.
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 $\mathbb{R}$.

81. C'est pour cette hypothèse que $\mathbb{K} = \mathbb{R}$ n'est pas le bon cadre.

11.16 Commutant et endomorphismes cycliques

11.16.1 Endomorphisme cyclique

Lemme 11.246.
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

$$E_{f,x} = \text{Span}\{f^k(x) \text{ tel que } k \in \mathbb{N}\}. \tag{11.537}$$

Définition 11.247.
*Soit E un espace vectoriel de dimension finie sur un corps $\mathbb{K}$ et un endomorphisme $f : E \to E$. Le **commutant** de f est l'ensemble des endomorphismes de E qui commutent avec f :*

$$\mathcal{C}(f) = \{g \in \mathcal{L}(E, E) \text{ tel que } g \circ f = f \circ g\}. \tag{11.538}$$

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.

11.16.2 Commutant : cas diagonalisable

Proposition 11.248 ([164]).
Si f est diagonalisable, alors

$$\dim\big(\mathcal{C}(f)\big) = \sum_{\lambda \in \text{Spec}(f)} \dim(E_\lambda)^2. \tag{11.539}$$

où les E_λ sont les espaces propres de f.

Démonstration. D'abord su $g \in \mathcal{C}(f)$ alors E_λ est stable par g. En effet si $v \in E_\lambda$ alors $f\big(g(v)\big) = g\big(f(v)\big) = g(\lambda v) = \lambda g(v)$, 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

$$\begin{aligned} \psi : \mathcal{C}(f) &\to \text{End}(E_1) \times \ldots \times \text{End}(E_r) \\ g &\mapsto g|_{E_1} \times \ldots \times g|_{E_r} \end{aligned} \tag{11.540}$$

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 propres [82] :

$$x = \sum_{\lambda \in \text{Spec}(f)} x_\lambda \tag{11.541}$$

avec $x_\lambda \in E_\lambda$. Nous avons alors

$$g(x) = \sum_\lambda g(x_\lambda) = \sum_\lambda \psi(g)_\lambda(x_\lambda). \tag{11.542}$$

Vu que nous avons $\psi(g)_\lambda = \psi(h)_\lambda$, nous avons aussi

$$g(x) = \sum_\lambda \psi(g)_\lambda(x_\lambda) = \sum_\lambda \psi(h)_\lambda(x_\lambda) = \sum_\lambda h(x_\lambda) = h(x). \tag{11.543}$$

Cela prouve $g = h$ et donc que ψ est injective.

82. Théorème 11.167(5).

ψ est surjective Si nous avons pour chaque $\lambda \in \mathrm{Spec}(f)$ un endomorphisme g_λ de E_λ alors en posant

$$g(x) = \sum_{\lambda \in \mathrm{Spec}(f)} g_\lambda(x_\lambda) \tag{11.544}$$

alors nous avons bien

$$\psi(g) = \big(g_{\lambda_1}, \dots, g_{\lambda_r}\big). \tag{11.545}$$

Nous pouvons donc conclure en écrivant

$$\dim\big(\mathcal{C}(f)\big) = \sum_{\lambda \in \mathrm{Spec}(f)} \dim\big(\mathrm{End}(E_\lambda)\big) = \sum_{\lambda \in \mathrm{Spec}(f)} \dim(E_\lambda)^2. \tag{11.546}$$

□

Remarque 11.249.
Nous avons alors immédiatement

$$\dim\big(\mathcal{C}(f)\big) \geqslant \dim(E) \tag{11.547}$$

lorsque f est diagonalisable.

En suivant la notation (11.269), un endomorphisme est cyclique lorsqu'il existe $x \in E$ tel que $E_x = E$.

Proposition 11.250 ([164]).
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) $\dim\big(\mathcal{C}(f)\big) = n$
(5) *L'endomorphisme f possède n valeurs propres distinctes.*
(6) $\dim\big(\mathbb{K}[f]\big) = n$

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 (11.539), les espaces propres de f ont dimension 1. Par conséquent f possède n valeurs propres distinctes.

(5) implique (6) Le théorème 11.167 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 11.145 nous avons $\dim\big(\mathbb{K}[f]\big) = \deg(\mu) = n$ par la proposition 6.37.

(6) implique (1) Par l'isomorphisme $\mathbb{K}[f] = \mathbb{K}[X]/(\mu)$ de la proposition 11.145 et la proposition 6.37 nous avons $n = \dim\big(\mathbb{K}[f]\big) = \deg(\mu)$. Vu que χ est un polynôme annulateur (Caley-Hamilton 11.154), 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 11.167 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 $v = e_1 + \cdots + e_n$ est cyclique. Nous avons

$$f^k(v) = \sum_{i=1}^{n} \lambda_i^k e_i. \tag{11.548}$$

Pour prouver que cette famille (avec $k = 0, \dots, n-1$) est libre[83] nous en prenons une combinaison linéaire nulle et nous prouvons que les coefficients sont tous nuls. Soit donc

$$0 = \sum_{l=0}^{n-1} a_l f^l(v) = \sum_{l=0}^{n-1} a_l \sum_{i=1}^{n} \lambda_i^l e_i = \sum_{i=1}^{n} \Big(\sum_{l=0}^{n-1} a_l \lambda_i^l \Big) e_i. \tag{11.549}$$

Vu que cela est nul, nous avons pour tout i :

$$\sum_{l=0}^{n-1} a_l \lambda_i^l = 0. \tag{11.550}$$

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

$$\det \begin{pmatrix} 1 & \lambda_1 & \lambda_1^2 & \cdots & \lambda_1^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \lambda_n & \lambda_n^2 & \cdots & \lambda_n^{n-1} \end{pmatrix}. \tag{11.551}$$

Il s'agit du déterminant de Vandermonde déjà étudié par la proposition 11.54. Nous avons $\det(A) = \prod_{1 \leqslant i < j \leqslant n} (\lambda_j - \lambda_i)$. 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

$$g(v) = \sum_{k=0}^{n-1} a_k f^k(v). \tag{11.552}$$

Cela donne une application linéaire

$$\begin{aligned} \psi \colon \mathcal{C}(f) &\to \mathbb{K}[f] \\ g &\mapsto P \text{ tel que } P(f)v = g(v). \end{aligned} \tag{11.553}$$

C'est une application injective parce que si $\psi(g) = 0$ alors $g(v) = 0$ et pour tout k nous avons $g\big(f^k(v)\big) = f^k\big(g(v)\big) = 0$. L'endomorphisme g s'annulant sur une base, est nul.

(3) implique (4) Si $n_1, \dots, n_r$ sont les dimensions des différents espaces propres de f, nous avons les inégalités

$$\dim\big(\mathbb{K}[f]\big) = \deg(\mu) \leqslant n = n_1 + \cdots + n_r \leqslant n_1^2 + \cdots + n_r^2 = \dim\big(\mathcal{C}(f)\big). \tag{11.554}$$

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 $\dim\big(\mathcal{C}(f)\big) = n$.

Nous avons fini de prouver toutes les équivalences demandées. □

Exemple 11.251

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. △

83. Ce sera alors une base parce que n vecteurs libres dans un espace de dimension n est toujours une base, proposition 4.16.

11.16.3 Commutant : cas général

Nous considérons encore un espace vectoriel E de dimension finie n et un endomorphisme $f\colon E\to E$. Nous notons μ sont polynôme minimal et μ_x le polynôme minimal ponctuel en x.

Lemme 11.252 ([165, 161, 66]).
Nous avons

$$\dim\big(\mathcal{C}(f)\big)\geqslant\dim(E) \tag{11.555}$$

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 supérieure. 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

$$(AX-XA)_{kk}=\sum_i\big(A_{ki}X_{ik}-X_{ki}A_{ik}\big)=\sum_{k\leqslant i\leqslant k}(A_{ki}X_{ik}-X_{ki}A_{ik})=0. \tag{11.556}$$

Nous avons donc au maximum

$$\frac{n(x+1)}{2}-n \tag{11.557}$$

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 11.241. 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 $\mathrm{End}(E_i)$. Mais en prolongeant par 0 sur E, ça reste libre en tant que partie de $\mathrm{End}(E)$.

Bien entendu les f_j^k et les f_i^k $(i\neq j)$ sont linéairement indépendants dans $\mathrm{End}(E)$ 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 $\mathrm{End}(E)$ composée d'endomorphismes qui commutent avec f. Il y en a en tout

$$\sum_{i=1}^r\deg(\mu_i)=\deg(\chi_f)=n. \tag{11.558}$$

Par conséquent $\dim\big(\mathcal{C}(f)\big)\geqslant\dim(E)$.

□

Théorème 11.253 ([147]).
Soit un endomorphisme $f\colon E\to E$ 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 11.240.

(1) implique (2) Conformément à ce que nous permet le lemme 11.137 nous choisissons[84] $a \in E$ de telle sorte à avoir $\mu_a = \mu$. De plus pour $x \in E$ nous considérons l'application

$$\begin{aligned}\varphi_x\colon \mathbb{K}[X] &\to E\\ P &\mapsto P(f)x.\end{aligned} \tag{11.559}$$

Nous avons $\varphi_a(P) = P(f)a$ et vu que E_a est engendré par les $f^k(a)$ nous avons $\varphi_a\big(\mathbb{K}[X]\big) = E_a$. 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

$$\bar{P} = \{P + Q\mu_a\}_{Q\in\mathbb{K}[X]}. \tag{11.560}$$

Nous considérons donc l'application

$$\varphi_a\colon \frac{\mathbb{K}[X]}{(\mu_a)} \to E_a \tag{11.561}$$

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 montrer que P est annulateur de a. Mais par définition 11.133 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 $\dim\big(\mathbb{K}[X]/P\big) = \deg(P)$ par la proposition 11.145. Au final nous avons $\dim(E_a) = \deg(\chi) = \dim(E)$. Et par conséquent $E_a = E$. Cela prouver que a est un vecteur cyclique pour 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

$$g(y) = g\big(Q(f)v\big) = Q(f)\big(g(v)\big) = Q(f)\big(P(f)v\big) = P(f)Q(f)v = P(f)y. \tag{11.562}$$

Donc $g = P(f)$.

(3) implique (1) Nous avons les inégalités :

$$n \leqslant \dim\big(\mathcal{C}(f)\big) = \dim\big(\mathbb{K}[f]\big) = \deg(\mu) \leqslant \deg(\chi) = n. \tag{11.563}$$

La première est le lemme 11.252. 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.

□

Corollaire 11.254 ([66]).
En suivant les notations sur les extensions de corps de base de la section 11.14, l'endomorphisme $f\colon E \to F$ est cyclique si et seulement si l'endomorphisme $f_{\mathbb{L}}\colon E_{\mathbb{L}} \to F_{\mathbb{L}}$ est cyclique.

84. Dans toute la suite,nous devrions écrire μ_f et $\mu_{f,a}$ mais nous omettons d'indiquer explicitement la dépendance en f.

Démonstration. Nous savons par le théorème 11.253 qu'un endomorphisme est cyclique si et seulement si son polynôme minimal est égal à son polynôme caractéristique. Or par les propositions 11.234 et 11.235, nous savons que ces polynômes sont identiques pour f et pour $f_{\mathbb{L}}$. □

Théorème 11.255 (Similitude et extension de corps[66]).
Les applications linéaires $f, g: E \to E$ 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 $m \in \mathrm{GL}(E)$ tel que $f = mgm^{-1}$ alors il suffit d'appliquer le lemme 11.230 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 11.241. 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 $f|_{E_i}: E_1 \to E_i$ est cyclique et de polynôme minimal μ.

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 (corollaire 11.254). 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 11.242 nous permet de conclure que f et g sont semblables si et seulement si $f_{\mathbb{L}}$ et $g_{\mathbb{L}}$ le sont. □

11.17 Hyperplans et formes linéaires

Définition 11.256.
*Si E est un espace vectoriel de dimension n, un **hyperplan** de E est un sous-espace vectoriel de dimension $n - 1$.*

Proposition 11.257 ([166]).
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 :

$$H = \ker(\varphi). \tag{11.564}$$

Démonstration. En deux parties.

(1) Soit un supplémentaire A de H. Nous considérons la restriction $\varphi_A: A \to \mathbb{K}$. 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 corollaire 4.37 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 $\mathrm{Span}\{e_1, \dots, e_{n-1}\} = H$. Nous pouvons alors considérer la forme linéaire définie par

$$\varphi(e_i) = \begin{cases} 0 & \text{si } i = 1, \dots, n-1 \\ 1 & \text{si } i = n. \end{cases} \tag{11.565}$$

Cette forme vérifie $\ker(\varphi) = H$.

□

Proposition 11.258 ([65]).
Soit un espace vectoriel E de dimension finie $n \geqslant 2$. 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 complétons[85] en une base de E : si $x = \sum_{i=1}^{n} x_i e_i$, nous avons $x \in V$ si et seulement si $x_{s+1} = \ldots = x_n = 0$. Nous considérons les formes linéaires

$$\begin{aligned} \varphi_i \colon E &\to \mathbb{R} \\ x &\mapsto x_i, \end{aligned} \tag{11.566}$$

et nous considérons les parties $H_i = \ker(\varphi_i)$ qui sont de hyperplans par la proposition 11.257. Les H_i avec $s+1 \leqslant i \leqslant n$ sont une famille de $n-s$ hyperplans qui vérifient

$$V = \bigcap_{i=s+1}^{n} \ker(\varphi_i) \tag{11.567}$$

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 11.259 ([65]).
Soit un $\mathbb{K}$-espace vectoriel E de dimension finie $n \geqslant 2$. Si H_i sont des hyperplans de E, alors

$$\dim\left(\bigcup_{i=1}^{m} H_i\right) \geqslant n - m. \tag{11.568}$$

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 4.40 que

$$\dim(H_1 \cap H_2) = \dim(H_1) + \dim(H_2) - \dim(H_1 \cap H_2). \tag{11.569}$$

De plus $\dim(H_1 + H_2) \leqslant n$. En remplaçant, par les valeurs,

$$\begin{aligned} \dim(H_1 \cap H_2) &= \dim(H_1) + \dim(H_2) - \dim(H_1 \cap H_2) && \text{(11.570a)} \\ &= n - 1 + n - 1 - \dim(H_1 + H_2) && \text{(11.570b)} \\ &\geqslant 2n - 2 - n && \text{(11.570c)} \\ &= n - 2. && \text{(11.570d)} \end{aligned}$$

Donc $\dim(H_1 \cap H_2) \geqslant n - 2$.

La récurrence Nous calculons $\dim(H_1 \cap \ldots \cap H_m \cap H_{m+1})$ en commençant encore par la proposition 4.40 :

$$\begin{aligned} \dim(H_1 \cap \ldots \cap H_m \cap H_{m+1}) &= \underbrace{\dim(H_1 \cap \ldots \cap H_m)}_{\leqslant n-m} + \dim(H_{m+1}) && \text{(11.571a)} \\ &\quad - \underbrace{\dim\big((H_1 \cap \ldots H_m) + H_{m+1}\big)}_{\leqslant n} && \text{(11.571b)} \\ &\geqslant n - m + (n-1) - n && \text{(11.571c)} \\ &= n - m - 1. && \text{(11.571d)} \end{aligned}$$

C'est bon pour la récurrence.

□

11.17.1 Trouver la matrice d'une symétrie donnée

Les notions de déterminants, produit scalaire et vectoriels[86] donnent une bonne intuition géométrique des matrices. Nous pouvons alors chercher les matrices de quelques symétriques dans $\mathbb{R}^2$ ou $\mathbb{R}^3$.

85. Théorème de la base incomplète, 4.11(4).
86. Définitions 11.50, 11.5 et 11.28.

11.17.1.1 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

$$A = \begin{pmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & -1\end{pmatrix}. \tag{11.572}$$

Pour écrire cela, nous avons juste mit 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 plan [87], 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

$$f_1 = \begin{pmatrix}0\\1\\0\end{pmatrix}, \quad f_2 = \begin{pmatrix}1\\0\\-1\end{pmatrix}. \tag{11.573}$$

Nous avons

$$\begin{aligned} Af_1 &= f_1\\ Af_2 &= f_2. \end{aligned} \tag{11.574}$$

Afin de trouver un vecteur perpendiculaire au plan, calculons le produit vectoriel :

$$f_3 = f_1 \times f_2 = \begin{vmatrix} e_1 & e_2 & e_3\\ 0 & 1 & 0\\ 1 & 0 & -1 \end{vmatrix} = -e_1 - e_3 = \begin{pmatrix}-1\\0\\-1\end{pmatrix}. \tag{11.575}$$

Nous avons

$$Af_3 = -f_3. \tag{11.576}$$

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 (11.573) dit que

$$f_1 = e_2. \tag{11.577}$$

Ensuite, nous avons

$$\begin{aligned} f_2 &= e_1 - e_3\\ f_3 &= -e_1 - e_3. \end{aligned} \tag{11.578}$$

87. Pour le trouver, penser au produit vectoriel.

La somme de ces deux équations donne $-2e_3 = f_2 + f_3$, c'est-à-dire

$$e_3 = -\frac{f_2 + f_3}{2} \tag{11.579}$$

Et enfin, nous avons

$$e_1 = \frac{f_2 - f_3}{2}. \tag{11.580}$$

Maintenant nous pouvons calculer les images de e_1, e_2 et e_3 en faisant

$$\begin{aligned} Ae_1 &= \frac{Af_2 - Af_3}{2} = \frac{1}{2}\begin{pmatrix} 0 \\ 0 \\ -2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix}, \\ Ae_2 &= Af_1 = f_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \\ Ae_3 &= -\frac{f_2 - f_3}{2} = -\frac{1}{2}\begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix}. \end{aligned} \tag{11.581}$$

La matrice A s'écrit maintenant en mettant les trois images trouvées en colonnes :

$$A = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}. \tag{11.582}$$

11.17.1.2 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

$$f_2 = \begin{pmatrix} 1 \\ 0 \\ x \end{pmatrix}, \tag{11.583}$$

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.

11.17.1.3 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.

11.18 Théorème de Burnside

Lemme 11.260.
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 11.261.
Toute représentation[88] *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 11.260 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 11.167). 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

$$\begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}. \tag{11.584}$$

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. □

Théorème 11.262 (Burnside[57, 167])**.**
Un sous-groupe de $\mathrm{GL}(n, \mathbb{C})$ est fini si et seulement s'il est d'exposant[89] *fini.*

Démonstration. Soit G un sous-groupe de $\mathrm{GL}(n, \mathbb{C})$. Si G est fini, l'ordre de ses éléments divise $|G|$ (corollaire 2.32 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.

Générateurs Le groupe G est une partie de $\mathbb{M}(n, \mathbb{C})$ dont nous considérons l'algèbre engendrée[90] $\mathcal{G}$. Soit $C_1, \dots, C_r$ une famille génératrice de $\mathcal{G}$ constituée d'éléments de G et la fonction

$$\begin{aligned} \tau\colon G &\to \mathbb{C}^r \\ A &\mapsto \big(\mathrm{Tr}(AC_1), \dots, \mathrm{Tr}(AC_r)\big). \end{aligned} \tag{11.585}$$

τ est injective Soient $A, B \in G$ tels que $\tau(A) = \tau(B)$. Si C_i est un générateur de G, nous avons $\mathrm{Tr}(AC_i) = \mathrm{Tr}(BC_i)$ et par la linéarité de la trace, nous avons

$$\mathrm{Tr}(AM) = \mathrm{Tr}(BM) \tag{11.586}$$

pour tout $M \in G$. Notons par ailleurs

$$N = AB^{-1} - \mathbb{1}, \tag{11.587}$$

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 $P\big(AB^{-1} - \mathbb{1}\big)P^{-1} = D - \mathbb{1}$ qui est encore diagonale. Donc N est diagonalisable.

88. Définition 4.128.
89. Définition 2.17.
90. Définition 3.73.

Par ailleurs nous avons

$$\begin{aligned}\mathrm{Tr}\left((AB^{-1})^p\right) &= \mathrm{Tr}\left(AB^{-1}(AB^{-1})^{p-1}\right) && (11.588a)\\ &= \mathrm{Tr}\left(BB^{-1}(AB^{-1})^{p-1}\right) \qquad (11.586) && (11.588b)\\ &= \mathrm{Tr}\left((AB^{-1})^{p-1}\right). && (11.588c)\end{aligned}$$

En continuant nous obtenons

$$\mathrm{Tr}\left((AB^{-1})^p\right) = \mathrm{Tr}(\mathbb{1}) = n. \tag{11.589}$$

D'autre part,

$$N^k = (AB^{-1} - \mathbb{1})^k = \sum_{p=0}^{k} \binom{p}{k} (-1)^{k-p}(AB^{-1})^p \tag{11.590}$$

En prenant la trace, et en tenant compte du fait que $\mathrm{Tr}\left((AB^{-1})^p\right) = n$,

$$\mathrm{Tr}(N^k) = \sum_{p=0}^{k} \binom{p}{k} (-1)^{k-p} n = n(1-1)^k = 0. \tag{11.591}$$

Donc la trace de N^k est nulle et le lemme 11.160 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. Dons le polynôme minimal d'un élément de G est (a fortiori) scindé à racines simples et le théorème 11.167 nous assure alors que ces éléments sont diagonalisables. Du coup les valeurs propres des matrices de G sont des racines $e$ièmes 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 $e$ièmes de l'unité. Mais vu que les C_i sont dans G, nous avons

$$\mathrm{Image}(\tau) = \{\mathrm{Tr}(A) \text{ tel que } A \in G\}^r, \tag{11.592}$$

qui est un ensemble fini. Par conséquent G est fini parce que τ est injective.

□

11.18.1 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 11.263
Le théorème 11.167 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

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \tag{11.593}$$

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

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \tag{11.594}$$

qui revient au système

$$\begin{cases} x + y = x & (11.595a)\\ y = y. & (11.595b)\end{cases}$$

La première équation donne directement $y = 0$. Le seul espace propre est de dimension 1 et est engendré par $\begin{pmatrix}1\\0\end{pmatrix}$. △

La remarque 11.214 donne un exemple un peu plus avancé, qui montre la multiplicité algébrique et géométrique d'une racine d'un polynôme caractéristique.

Lemme 11.264 (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 11.174 : 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 11.215 nous donne la somme directe d'espaces caractéristiques [91]

$$E = F_{\lambda_1}(A_0)\oplus\dots\oplus F_{\lambda_r}(A_0). \tag{11.596}$$

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 11.216(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. □

Théorème 11.265 (Lie-Kolchin[168])**.**
Tout sous-groupe connexe et résoluble de $\mathrm{GL}(n,\mathbb{C})$ *est conjugué à un groupe de matrices triangulaires.*

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,

$$\begin{pmatrix}g_1 & *\\ 0 & g_2\end{pmatrix}. \tag{11.597}$$

Les matrices g_1 et g_2 sont carrés. Nous considérons alors l'application ψ définie par

$$\begin{aligned}\psi\colon G &\to \mathrm{GL}(V)\\ g &\mapsto g_1.\end{aligned} \tag{11.598}$$

Cela est un morphisme de groupes parce que

$$\begin{pmatrix}g_1 & *\\ 0 & g_2\end{pmatrix}\begin{pmatrix}h_1 & *\\ 0 & h_2\end{pmatrix} = \begin{pmatrix}g_1h_1 & *\\ 0 & g_2h_2\end{pmatrix}, \tag{11.599}$$

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 7.84). Et il est résoluble en tant qu'image

91. Définition 11.212.

d'un groupe résoluble par un homomorphisme par la proposition 2.42. Vu que $\psi(G)$ est un sous-groupe résoluble et connexe de $\mathrm{GL}(V)$ et que la dimension de V est strictement plis 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 (11.597) (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 et résoluble et que sa suite dérivée termine sur e (proposition 2.41).

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 11.264). 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 11.264 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 $g \in G$:

$$h\big(g(v)\big) = g\underbrace{g^{-1}hg}_{\in H}(v) = g(\lambda v) = \lambda g(v) \tag{11.600}$$

parce que v est vecteur propre de $g^{-1}hg$. Ce que le calcul (11.600) 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

$$(ghg^{-1})(v) = \lambda v \tag{11.601a}$$
$$h\big(g^{-1}v\big) = \lambda\big(g^{-1}v\big), \tag{11.601b}$$

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,

$$hg(w) = g(hw) = \lambda g(w), \tag{11.602}$$

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.

□

11.19 Retour sur les formes bilinéaires et quadratiques

11.19.1 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 11.266.
Une forme bilinéaire est ***non dégénérée*** $b(x, z) = 0$ *pour tout z implique $x = 0$.*

Lemme 11.267.
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

$$b(x - y, z) = 0 \tag{11.603}$$

pour tout z, ce qui implique $x - y = 0$. □

Proposition 11.268.
Une forme bilinéaire est non-dénénérée[92] *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 11.189). 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 $(e_k)_j = \delta_{kj}$:

$$b(x, e_k) = \sum_{ij} x_i (e_k)_j = \sum_i b_{ik} x_i = b_{kk} x_k. \tag{11.604}$$

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. □

92. Définition 11.266.

11.19.2 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 Lorentz [93], beaucoup oublient de justifier pourquoi elles devraient être linéaires.

Théorème 11.269 ([169]).
Une isométrie d'une forme bilinéaire[94] *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

$$\begin{aligned} b\big(f(x+y),z\big) &= b\big(f(x+y),f(f^{-1}(z))\big) && \text{(11.605a)}\\ &= b(x+y,f^{-1}(z)) && \text{(11.605b)}\\ &= b(x,f^{-1}(z))+b(y,f^{-1}(z)) && \text{(11.605c)}\\ &= b(f(x),z)+b(f(y),z) && \text{(11.605d)}\\ &= b\big(f(x)+f(y),z\big), && \text{(11.605e)} \end{aligned}$$

donc $f(x+y)=f(x)+f(y)$ par le lemme 11.267.

De la même façon on trouve $b\big(f(\lambda x),z\big)=b\big(\lambda f(x),z\big)$ qui prouve que $f(\lambda x)=\lambda f(x)$ et donc que f est linéaire. □

Exemple 11.270
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

$$b\big((a,b),(x,y)\big)=ax, \tag{11.606}$$

nous pouvons faire

$$f(x,y)=\begin{pmatrix} x\\ \lambda(x,y)\end{pmatrix} \tag{11.607}$$

où λ est n'importe quoi. △

Théorème 11.271.
Soit un espace vectoriel E muni d'une forme quadratique q. Soit une isométrie $f\colon E\to E$ pour q. Alors

(1) si $f(0)=0$, alors f est linéaire ;

(2) si $f(0)\neq 0$ alors f est affine[95].

Démonstration. Nous considérons la forme bilinéaire associée b. Si $f(0)=0$, nous savons par le lemme 11.205 que $b\big(f(x),f(y)\big)=b(x,y)$. La proposition 11.269 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

$$q\big(g(x)-g(y)\big)=q\big(f(x)-f(0)-f(y)+f(0)\big)=q(x-y). \tag{11.608}$$

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 10.53 des fonctions affines. □

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.

93. Théorème 19.15.
94. Définition 11.204.
95. Définition 10.8.

Lemme 11.272 ([170]).
Une isométrie d'un espace vectoriel normé de dimension finie est bijective.

Démonstration. Si $f : E \to E$ est une isométrie, elle est linéaire par le théorème 11.269. 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 corollaire 4.41 du théorème du rang. □

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

$$\begin{aligned}\tau_v : \mathbb{R}^n &\to \mathbb{R}^n \\ x &\mapsto x + v.\end{aligned} \tag{11.609}$$

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 11.273.
Soit une forme bilinéaire b sur $\mathbb{R}^n$ de matrice symétrique η. Si A est la matrice d'une application linéaire $\mathbb{R}^n \to \mathbb{R}^n$ telle que

$$b(Ax, Ay) = b(x, y) \tag{11.610}$$

pour tout $x, y \in \mathbb{R}^n$, alors

$$A^t \eta A = \eta. \tag{11.611}$$

Démonstration. En suivant la formule générale (11.408),

$$b(Ax, Ay) = \sum_{ij} \eta_{ij}(Ax)_i(Ay)_j = \sum_{ijkl} \eta_{ij} A_{ik} A_{jl} x_k y_l. \tag{11.612}$$

En imposant que ce soit égal à $\sum_{kl} \eta_{kl}\eta_{kl}x_k y_l$ pour tout x, y nous avons la contrainte

$$\sum_{ij} \eta_{ij} A_{ik} A_{jl} = \eta_{kl} \tag{11.613}$$

qui signifie exactement $A^t \eta A = \eta$. □

11.19.3 Pseudo-réduction simultanée

Corollaire 11.274 (Pseudo-réduction simultanée[171]).
Soient $A, B \in \mathrm{S}(n, \mathbb{R})$ avec A définie positive[96]*. Alors il existe $Q \in \mathrm{GL}(n, \mathbb{R})$ telle que $Q^t B Q$ soit diagonale et $Q^t A Q = \mathbb{1}$.*

Démonstration. Nous allons noter $x \cdot y$ le produit scalaire usuel de $\mathbb{R}^n$ et $\{e_i\}_{i=1,\dots,n}$ sa base canonique.

Vu que A est définie positive, nous avons que l'expression[97] $\langle x, y\rangle = x \cdot Ay$ est un produit scalaire sur $\mathbb{R}^n$. Autrement dit, E muni de cette forme bilinéaire symétrique est un espace euclidien, ce qui fait dire à la proposition 11.40 qu'il existe une base de $\mathbb{R}^n$ orthonormée $\{f_i\}_{i=1,\dots,n}$ pour ce produit scalaire, c'est-à-dire qu'il existe une matrice $P \in \mathrm{GL}(n, \mathbb{R})$ telle que $P^t A P = \mathbb{1}$. Ici, P est la matrice de changement de base de la base canonique à notre base orthonormée, c'est-à-dire la matrice qui fait $Pe_i = f_i$ pour tout i. Voyons cela avec un peu de détails.

Pour savoir ce que valent les éléments de la matrice $P^t A P$, nous nous souvenons que $P^t A P e_j$ est un vecteur dont les coordonnées sont les éléments de la j^{e}colonne de $P^t A P$. Autrement dit,

96. Définition 11.191.
97. On peut aussi l'écrire de façon plus matricielle sous la forme $\langle x, y\rangle = x^t Ay$.

nous utilisons la formule (11.419). Calculons :

$$\begin{aligned}(P^tAP)_{ij} &= e_i \cdot P^tAPe_j && \text{(11.614a)}\\ &= Pe_i \cdot APe_j && \text{(11.614b)}\\ &= f_i \cdot Af_j && \text{(11.614c)}\\ &= \langle f_i, f_j\rangle && \text{(11.614d)}\\ &= \delta_{ij} && \text{(11.614e)}\end{aligned}$$

où nous avons fait attention à écrire $x \cdot y$ le produit scalaire usuel de $\mathbb{R}^n$ et $\langle x, y\rangle$ celui défini plus haut via la matrice A. Au final nous avons effectivement $P^tAP = \mathbb{1}$.

La matrice P^tBP est une matrice symétrique, donc le théorème spectral 11.189 nous donne une matrice $R \in \mathrm{O}(n, \mathbb{R})$ telle que R^tP^tBPR soit diagonale. En posant maintenant $Q = PR$ nous avons la matrice cherchée. □

Remarque 11.275.
Plusieurs remarques

(1) Nous n'avons pas prouvé l'existence d'une matrice P telle que $P^{-1}BP$ et $P^{-1}AP$ soient diagonales. Au contraire, nous avons Q^tBQ et Q^tAQ qui sont diagonales. Tant que Q n'est pas orthogonales, ce n'est pas la même chose.

Autrement dit, nous n'avons pas ici une réelle diagonalisation, parce que les matrices A et B ne sont pas semblables à des matrices diagonales. Voir les définitions 11.164 (diagonalisable) et 11.158 (semblable).

C'est pour cela que nous parlons de *pseudo*-diagonalisation.

(2) Dans le même ordre d'idée, la démonstration de la pseudo-diagonalisation simultanée parle clairement de formes bilinéaires, et non d'endomorphismes. Or en comparant les lois de transformations (11.437) et (11.440), nous voyons bien que la réduction en passant par Q^tAQ est bien une réduction de forme bilinéaire et non une réduction d'endomorphismes.

(3) Nous avons prouvé la pseudo-réduction simultanée comme corollaire du théorème de diagonalisation des matrices symétriques 11.189. Il aurait aussi pu être vu comme un corollaire du théorème spectral 11.287 sur les opérateurs autoadjoints via son corollaire 11.288.

11.19.4 Topologie

La topologie considérée sur $Q(E)$ est celle de la norme

$$N(q) = \sup_{\|x\|_E=1} |q(x)|, \tag{11.615}$$

qui du point de vue de $S(n, \mathbb{R})$ est

$$N(A) = \sup_{\|x\|_E=1} |x^tAx|. \tag{11.616}$$

Notons que à droite, c'est la valeur absolue usuelle sur $\mathbb{R}$.

Proposition 11.276.
Soit $\{e_i\}$ une base de E. L'application

$$\begin{aligned}\phi\colon Q(E) &\to S(n, \mathbb{R})\\ q &\mapsto \big(b(e_i, e_j)\big)_{i,j}\end{aligned} \tag{11.617}$$

où b est forme bilinéaire associée à q est une bijection linéaire et continue[98].

98. Pour les topologies des normes (11.615) et (11.616).

Démonstration. Si $\phi(q) = \phi(q')$; alors

$$q(x) = \sum_{i,j} \phi(q)_{ij} x_i x_j = \sum_{i,j} \phi(q')_{ij} x_i x_j = q'(x). \tag{11.618}$$

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

$$q(x) = \sum_{i,j} B_{ij} x_i x_j \tag{11.619}$$

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

$$\sup_{\|x\|=1} |q_n(x)| \to 0. \tag{11.620}$$

Nous rappelons l'identité de polarisation :

$$b_n(x, y) = \frac{1}{2}\big(q_n(x - y) - q(x) - q(y)\big). \tag{11.621}$$

En ce qui concerne deux des trois termes, il n'y a pas de problèmes :

$$\big|\phi(q_n)_{ij}\big| = \big|b_n(e_i, e_j)\big| \leqslant \frac{1}{2}\big|b_n(e_i - e_j)\big| + \frac{1}{2}\big|q_n(e_i)\big| + \frac{1}{2}\big|q_n(e_j)\big|. \tag{11.622}$$

Si n est assez grand, nous avons tout de suite

$$\big|\phi(q_n)_{ij}\big| \leqslant \frac{1}{2}\big|q_n(e_i - e_j)\big| + \epsilon. \tag{11.623}$$

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

$$q_n(e_i - e_j) = \alpha_{ij}^2 q_n(e_{ij}) \leqslant \alpha^2 q_n(e_{ij}). \tag{11.624}$$

Il suffit maintenant de prendre n assez grand pour avoir $\sup_{\|x\|=1} |q_n(x)| \leqslant \frac{\epsilon}{\alpha^2}$ pour avoir

$$\big|\phi(q_n)_{ij}\big| \leqslant \frac{\epsilon}{2} + \frac{\epsilon}{\alpha^2}. \tag{11.625}$$

□

11.19.5 Diagonalisation

Proposition 11.277.
Dans la base de diagonalisation de sa matrice associée, une forme quadratique a la forme

$$q(x) = \sum_i \lambda_i x_i^2 \tag{11.626}$$

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 diagonalisation [99] de la matrice de b alors dans cette base nous avons

$$q(x) = b(x, x) = \sum_{ij} x_i x_j b(f_i, f_j) = \sum_i \lambda_i x_i^2 \tag{11.627}$$

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 changement pas (à part l'ordre éventuellement). Cela pour dire que nous nous permettrons de parler des **valeurs propres** d'une forme quadratique comme étant les valeurs propres de la matrice associée.

99. Qui existe parce que la matrice est symétrique, théorème 11.189.

11.19.6 Isotropie

Définition 11.278 (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* ***totalement 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 :*

$$C(b)=\{x\in E \text{ tel que } b(x,x)=0\}. \tag{11.628}$$

Nous introduisons quelques notations. D'abord pour $y\in E$ nous notons

$$\begin{aligned}\Phi_y\colon E&\to\mathbb{R}\\ x&\mapsto b(x,y)\end{aligned} \tag{11.629}$$

et ensuite

$$\begin{aligned}\Phi\colon E&\to E^*\\ y&\mapsto \Phi_y.\end{aligned} \tag{11.630}$$

Définition 11.279.
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*

$$\ker(b)=\{z\in E \text{ tel que } b(z,y)=0\,\forall y\in E\}. \tag{11.631}$$

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.

Proposition 11.280 ([172])**.**
Soit b une forme bilinéaire et symétrique. Alors

(1) $\ker(b)\subset C(b)$ *(cône d'isotropie, définition 11.278)*

(2) si b est positive alors $\ker(b)=C(b)$.

Démonstration. (1) Si $z\in\ker(b)$ alors pour tout $y\in E$ nous avons $b(z,y)=0$. En particulier pour $y=z$ nous avons $b(z,z,)=0$ et donc $z\in C(b)$.

(2) Soit b positive et $x\in C(b)$. Par l'inégalité de Cauchy-Schwarz (proposition 11.10) nous avons

$$|b(x,y)|\leqslant\sqrt{b(x,x)b(y,y)}=0. \tag{11.632}$$

Donc pour tout y nous avons $b(x,y)=0$.

□

11.19.7 Inégalité de Minkowski

Ce qui est couramment nommé « inégalité de Minkowski » est la proposition 28.37 dans les espaces L^p. Nous allons en donner ici un cas très particulier.

Proposition 11.281.
Si q est une forme quadratique sur $\mathbb{R}^n$ et si $x,y\in\mathbb{R}^n$ alors

$$\sqrt{q(x+y)}\leqslant\sqrt{q(x)}+\sqrt{q(y)}. \tag{11.633}$$

Démonstration. La proposition 11.277 nous permet de « diagonaliser » la forme quadratique q. Quitte à ne plus avoir une base orthonormale, nous pouvons renormaliser les vecteurs de base pour avoir

$$q(x)=\sum_i x_i^2. \tag{11.634}$$

Le résultat n'est donc rien d'autre que l'inégalité triangulaire pour la norme euclidienne usuelle, laquelle est démontrée dans la proposition 11.11. □

11.19.8 Ellipsoïde

Lemme 11.282.
Toute matrice peut être décomposée de façon unique en une partie symétrique et une partie antisymétrique. Cette décomposition est donnée par

$$S = \frac{M + M^t}{2}, \quad A = \frac{M - M^t}{2} \tag{11.635}$$

Démonstration. L'existence est une vérification immédiate de $S + A = M$ en utilisant (11.635). 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 $A = A'$. □

Définition 11.283.
*Un **ellipsoïde** dans $\mathbb{R}^n$ centré en v est le lieu des points x vérifiant l'équation*

$$\langle x - v, M(x - v)\rangle = 1 \tag{11.636}$$

où M est une matrice symétrique strictement définie positive[100].

Lorsque nous parlons d'ellipsoïde plein, *il suffit de changer l'égalité en une inégalité.*

Remarque 11.284.
Le fait que M soit symétrique n'est pas tout à fait obligatoire ; la chose important 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 11.282). Alors pour tout $x \in \mathbb{R}^n$ nous avons

$$x^tAx = \langle x, Ax\rangle = \langle A^tx, x\rangle = -\langle Ax, x\rangle = -\langle x, Ax\rangle, \tag{11.637}$$

donc $x^tAx = 0$. L'équation $x^tMx = 1$ est donc équivalente à $x^tSx = 1$ (elles ont les mêmes solutions).

De plus S reste strictement définie positive parce que pour tout $x \in \mathbb{R}^n$ nous avons

$$0 < x^tMx = x^tSx. \tag{11.638}$$

Proposition 11.285.
Si $\mathcal{E}$ est un ellipsoïde centrée à l'origine, il existe une base de $\mathbb{R}^n$ dans laquelle son équation est :

$$\sum_{i=1}^{n} \frac{x_i^2}{a_i^2} = 1. \tag{11.639}$$

Démonstration. Nous avons une matrice symétrique strictement définie positive S telle que l'équation soit $\langle x, Sx\rangle = 1$. Le théorème spectral 11.189 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

$$\sum_i \lambda_i x_i^2 = 1. \tag{11.640}$$

En posant $a_i = \frac{1}{\sqrt{\lambda_i}}$, nous trouvons le résultat. Cette définition des a_i est toujours possible parce que $\lambda_i > 0$. □

Corollaire 11.286.
Un ellipsoïde plein centré en l'origine admet une équation de la forme $q(x) \leqslant 1$ 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 $Q^{++}(E)$.

100. Définition 11.191.

Démonstration. Soit $\{e_i\}$ une base de $\mathbb{R}^n$ telle que l'ellipsoïde $\mathcal{E}$ ait pour équation

$$\sum_{i=1}^{n} \frac{x_i^2}{a_i^2} \leqslant 1. \tag{11.641}$$

Nous considérons la forme quadratique

$$\begin{aligned} q\colon \mathbb{R}^n &\to \mathbb{R} \\ x &\mapsto \sum_{i=1}^{n} \frac{\langle x, e_i\rangle^2}{a_i^2}. \end{aligned} \tag{11.642}$$

Nous avons évidemment $\mathcal{E} = \{x \in \mathbb{R}^n \text{ tel que } q(x) \leqslant 1\}$. 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 $q(x) > 0$. □

11.20 Théorème spectral autoadjoint

Théorème 11.287 (Théorème spectral autoadjoint)**.**
Un endomorphisme autoadjoint d'un espace euclidien

(1) est diagonalisable dans une base orthonormée,

(2) a son spectre réel.

Démonstration. Nous procédons par récurrence sur la dimension de E, et nous commençons par $n = 1$ [101]. Soit donc $f\colon E \to E$ avec $\langle f(x), y\rangle = \langle x, f(y)\rangle$. Étant donné que f est également linéaire, il existe $\lambda \in \mathbb{R}$ tel que $f(x) = \lambda x$ pour tout $x \in E$. Tous les vecteurs de E sont donc vecteurs propres de f.

Passons à la récurrence. Nous considérons $\dim(E) = n + 1$ et $f \in \mathrm{S}(E)$. Nous considérons la forme bilinéaire symétrique Φ_f et la forme quadratique associée ϕ_f. Pour rappel,

$$\Phi_f(x, y) = \langle x, f(y)\rangle \tag{11.643a}$$

$$\phi_f(x) = \Phi_f(x, x). \tag{11.643b}$$

Et nous allons laisser tomber les indices f pour noter simplement Φ et ϕ. Étant donné que $\overline{B(0,1)}$ est compacte et que ϕ est continue, il existe $x_0 \in \overline{B(0,1)}$ tel que

$$\lambda = \phi(x_0) = \sup_{x \in \overline{B(0,1)}} \phi(x). \tag{11.644}$$

Notons aussi que $\|x_0\| = 1$: le maximum est pris sur le bord. Nous posons

$$g = \lambda \mathrm{Id} - f \tag{11.645}$$

ainsi que

$$\Phi_1(x, y) = \langle x, g(y)\rangle. \tag{11.646}$$

Cela est une forme bilinéaire et symétrique parce que

$$\Phi_1(y, x) = \langle y, g(x)\rangle = \langle g(y), x\rangle = \langle x, g(y)\rangle = \Phi_1(x, y) \tag{11.647}$$

où nous avons utilisé le fait que g était autoadjoint et la symétrie du produit scalaire. De plus Φ_1 est semi-définie positive parce que

$$\Phi_1(x, x) = \langle x, \lambda x - f(x)\rangle = \lambda\|x\|^2 - \phi(x). \tag{11.648}$$

101. Dans [43], l'auteur commence avec $n = 0$ mais moi je n'en ai pas le courage..

Vu que λ est le maximum, nous avons tout de suite $\Phi_1(x) \geqslant 0$ tant que $\|x\| = 1$. Et si x n'est pas de norme 1, c'est le même prix parce qu'on se ramène à $\|x\| = 1$ en multipliant par un nombre positif. Attention cependant :

$$\Phi_1(x_0, x_0) = \lambda\|x_0\|^2 - \phi(x_0) = 0. \tag{11.649}$$

Donc Φ_1 a un noyau contenant x_0 par la proposition 11.280. Nous en déduisons que $\text{Image}(g) \neq E$ en effet, $x_0 \in \text{Image}(g)^\perp$, mais nous avons la proposition 4.115 sur les dimensions :

$$\dim E = \dim(\text{Image}(g)) + \dim(\text{Image}(g)^\perp). \tag{11.650}$$

Vu que $\text{Image}(g)^\perp$ est un espace vectoriel non réduit à $\{0\}$, la dimension de $\text{Image}(g)$ ne peut pas être celle de E. L'endomorphisme g n'étant pas surjectif, il ne peut pas être injectif non plus parce que nous sommes en dimension finie ; il existe donc $e_1 \in E$ tel que $g(e_1) = 0$ et tant qu'à faire nous choisissons $\|e_1\| = 1$ (ici la norme est bien celle de l'espace euclidien considéré). Par définition,

$$f(e_1) = \lambda e_1, \tag{11.651}$$

c'est-à-dire que $\lambda \in \text{Spec}(f)$. Et ϕ étant une forme quadratique réelle nous avons $\lambda \in \mathbb{R}$.

Nous posons à présent $H = \text{Span}\{e_1\}^\perp$. C'est un sous-espace stable par f parce que si $x \in H$ alors

$$\langle e_1, f(x)\rangle = \langle f(e_1 j), x\rangle = \lambda\langle e_1, x\rangle = 0. \tag{11.652}$$

Nous pouvons donc considérer la restriction de f à H : $f_H \colon H \to H$. Cet endomorphisme est bilinéaire et symétrique sur l'espace H de dimension inférieure à celle de E, donc la récurrence nous donne une base orthonormée

$$\{e_2, \ldots, e_n\} \tag{11.653}$$

de vecteurs propres de f_H. De plus les valeurs propres sont réelles, toujours par récurrence. Donc

$$\text{Spec}(f) = \{\lambda\} \cup \text{Spec}(f_H) \subset \mathbb{R}. \tag{11.654}$$

Notons pour être complet que si $i \geqslant 2$ alors

$$\langle e_1, e_i\rangle = 0 \tag{11.655}$$

parce que le vecteur e_i est par construction choisi dans l'espace $H = e_1^\perp$. Nous avons donc bien une base orthonormée de E construite sur des vecteurs propres de f. □

Corollaire 11.288.
Soit E un espace vectoriel ainsi que ϕ et ψ des formes quadratiques sur E avec ψ définie positive. Alors il existe une base ψ-orthonormale dans laquelle ϕ est diagonale.

Démonstration. Il suffit de considérer l'espace euclidien E muni du produit scalaire $\langle x, y\rangle = \psi(x, y)$. Ensuite nous diagonalisons la matrice (symétrique) de ϕ pour ce produit scalaire à l'aide du théorème 11.287. □

Définition 11.289.
Dans le cas de $V = \mathbb{R}^m$ nous avons un produit scalaire canonique. Soient u et v, deux vecteurs de $\mathbb{R}^m$. Le ***produit scalaire*** *de u et v, noté $\langle u, v\rangle$ ou $u \cdot v$ est le réel*

$$\langle u, v\rangle = \sum_{k=1}^{m} u_k v_k = u_1 v_1 + u_2 v_2 + \cdots + u_m v_n. \tag{11.656}$$

Calculons par exemple le produit scalaire de deux vecteurs de la base canonique : $\langle e_i, e_j\rangle$. En utilisant la formule de définition et le fait que $(e_i)_k = \delta_{ik}$, nous avons

$$\langle e_i, e_j\rangle = \sum_{k=1}^{m} \delta_{ik}\delta_{jk}. \tag{11.657}$$

Nous pouvons effectuer la somme sur k en remarquant qu'à cause du δ_{ik}, seul le terme avec $k = i$ n'est pas nul. Effectuer la somme revient donc à remplacer tous les k par des i :

$$\langle e_i, e_j \rangle = \delta_{ii}\delta_{ji} = \delta_{ji}. \tag{11.658}$$

Une des propriétés intéressantes du produit scalaire est qu'il permet de décomposer un vecteur dans une base, comme nous le montre la proposition suivante.

Proposition 11.290.
Si nous notons v_i les composantes du vecteur v, c'est-à-dire si $v = \sum_{i=1}^{m} v_i e_i$, alors nous avons $v_j = \langle v, e_j \rangle$.

Démonstration.

$$v \cdot e_j = \sum_{i=1}^{m} \langle v_i e_i, e_j \rangle = \sum_{i=1}^{m} v_i \langle e_i, e_j \rangle = \sum_{i=1}^{m} v_i \delta_{ij} \tag{11.659}$$

En effectuant la somme sur i dans le membre de droite de l'équation (11.659), tous les termes sont nuls sauf celui où $i = j$; il reste donc

$$v \cdot e_j = v_j. \tag{11.660}$$

□

Le produit scalaire ne dépend en réalité pas de la base orthogonale choisie.

Lemme 11.291.
Si $\{e_i\}$ est la base canonique, et si $\{f_i\}$ est une autre base orthonormale, alors si u et v sont deux vecteurs de $\mathbb{R}^m$, nous avons

$$\sum_i u_i v_j = \sum_i u'_i v'_j \tag{11.661}$$

où u_i sont les composantes de u dans la base $\{e_i\}$ et u'_i sont celles dans la base $\{f_i\}$.

Démonstration. La preuve demande un peu d'algèbre linéaire. Étant donné que $\{f_i\}$ est une base orthonormale, il existe une matrice A orthogonale ($AA^t = \mathbb{1}$) telle que $u'_i = \sum_j A_{ij} u_j$ et idem pour v. Nous avons alors

$$\begin{aligned}
\sum_i u'_i v'_j &= \sum_i \left(\sum_j A_{ij} u_j \right) \left(\sum_k A_{ik} v_k \right) \\
&= \sum_{ijk} A_{ij} A_{ik} u_j v_k \\
&= \sum_{jk} \underbrace{\sum_i (A^t)_{ji} A_{ik}}_{=\delta_{jk}} u_j v_k \\
&= \sum_{jk} \delta_{jk} u_j v_k \\
&= \sum_k u_j v_k.
\end{aligned} \tag{11.662}$$

□

Cette proposition nous permet de réellement parler du produit scalaire entre deux vecteurs de façon intrinsèque sans nous soucier de la base dans laquelle nous regardons les vecteurs.

Nous dirons que deux vecteurs sont **orthogonaux** lorsque leur produit scalaire est nul. Nous écrivons que $u \perp v$ lorsque $\langle u, v \rangle = 0$.

Définition 11.292.
*La **norme euclidienne** d'un élément de $\mathbb{R}^m$ est définie par $\|u\| = \sqrt{u \cdot u}$.*

Cette définition est motivée par le fait que le produit scalaire $u \cdot u$ donne exactement la norme usuelle donnée par le théorème de Pythagore :

$$u \cdot u = \sum_{i=1}^{m} u_i u_i = \sum_{i=1}^{m} u_i^2 = u_1^2 + u_2^2 + \cdots + u_m^2. \tag{11.663}$$

Le fait que $e_i \cdot e_j = \delta_{ij}$ signifie que la base canonique est **orthonormée**, c'est-à-dire que les vecteurs de la base canonique sont orthogonaux deux à deux et qu'ils ont tout 1 comme norme.

Lemme 11.293.
Pour tout $u \in \mathbb{R}^m$, il existe un $\xi \in \mathbb{R}^m$ tel que $\|u\| = \xi \cdot u$ et $\|\xi\| = 1$.

Démonstration. Vérifions que le vecteur $\xi = u/\|u\|$ ait les propriétés requises. D'abord $\|\xi\| = 1$ parce que $u \cdot u = \|u\|^2$. Ensuite

$$\xi \cdot u = \frac{u \cdot u}{\|u\|} = \frac{\|u\|^2}{\|u\|} = \|u\|. \tag{11.664}$$

□

11.21 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 ;

$$\text{p.ex. } \left(\begin{array}{cc|c} 2 & 3 & 5 \\ 1 & 2 & 4 \end{array}\right) \overset{L_1 - 2.L_2 \mapsto L_1'}{\Longrightarrow} \left(\begin{array}{cc|c} 0 & -1 & -3 \\ 1 & 2 & 4 \end{array}\right)$$

(2b) Remplacer une ligne par un multiple d'elle-même ;

$$\text{p.ex. } \left(\begin{array}{cc|c} 0 & -1 & -3 \\ 1 & 2 & 4 \end{array}\right) \overset{-L_1 \mapsto L_1'}{\Longrightarrow} \left(\begin{array}{cc|c} 0 & 1 & 3 \\ 1 & 2 & 4 \end{array}\right)$$

(2c) Permuter des lignes.

$$\text{p.ex. } \left(\begin{array}{cc|c} 0 & 1 & 3 \\ 1 & 0 & -2 \end{array}\right) \overset{L_1 \mapsto L_2' \text{ et } L_2 \mapsto L_1'}{\Longrightarrow} \left(\begin{array}{cc|c} 1 & 0 & -2 \\ 0 & 1 & 3 \end{array}\right)$$

(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 11.294. — 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 :

$$\text{p.ex. } \left(\begin{array}{ccc|c} 3 & 4 & -2 & 2 \\ 4 & -1 & 3 & 0 \\ 0 & 0 & 0 & 7 \end{array}\right) \Leftrightarrow \begin{cases} \cdots \\ \cdots \\ 0x + 0y + 0z = 7 \end{cases} \Rightarrow \textbf{Impossible}$$

— 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 12

Espaces vectoriels normés

Plusieurs choses sur les espaces vectoriels normés (dont la définition 7.106) ont déjà été vues dans la section 9.4. Voir aussi le thème 7.

On fixe maintenant une définition largement utilisée dans la suite.

Définition 12.1.
Soient U et V, deux ouverts d'un espace vectoriel normé. Une application f de U dans V est un ***difféomorphisme*** *si elle est bijective, différentiable et dont l'inverse $f^{-1} : V \to U$ est aussi différentiable.*

Remarque 12.2.
Il n'est pas possible d'avoir une application inversible d'un ouvert de $\mathbb{R}^m$ vers un ouvert de $\mathbb{R}^n$ si $m \neq n$. Il n'y a donc pas de notion de difféomorphismes entre ouverts de dimensions différentes.

12.1 Équivalence des normes

Au premier coup d'œil, les notions dont nous parlons dans ce chapitre ont l'air très générales. Nous prenons en effet n'importe quel espace vectoriel V de dimension finie, et nous le munissons de n'importe quelle norme (rien que dans $\mathbb{R}^m$ nous en avons défini une infinité par l'équation (9.59)). À partir de ces données, nous définissons les boules, la topologie, l'adhérence, etc.

12.1.1 En dimension finie

Dans $\mathbb{R}^n$, les normes $\|.\|_{L^1}$, $\|.\|_{L^2}$ et $\|.\|_\infty$ ne sont pas égales. Cependant elles ne sont pas complètement indépendantes au sens où l'on sent bien que si un vecteur sera grand pour une norme, il sera également grand pour les autres normes ; les normes « vont dans le même sens ». Cette notion est précisée par le concept de norme équivalente.

Définition 12.3.
Deux normes N_1 et N_2 sur $\mathbb{R}^m$ sont ***équivalentes*** *s'il existe deux nombres réels strictement positifs k_1 et k_2 tels que*

$$k_1 N_1(x) \leqslant N_2(x) \leqslant k_2 N_1(x), \tag{12.1}$$

pour tout x dans $\mathbb{R}^m$. Dans ce cas nous écrivons que $N_1 \sim N_2$.

Lemme 12.4.
La définition de norme équivalentes donne une relation d'équivalence (définition 1.23) sur l'ensemble des normes existantes sur $\mathbb{R}^m$.

Proposition 12.5.
Pour $\mathbb{R}^N$, nous avons les équivalences de normes $\|.\|_{L^1} \sim \|.\|_{L^2}$, $\|.\|_{L^1} \sim \|.\|_\infty$ et $\|.\|_{L^2} \sim \|.\|_\infty$. Plus précisément nous avons les inégalités

(1) $\|x\|_2 \leqslant \|x\|_1 \leqslant \sqrt{n}\|x\|_2$

(2) $\|x\|_\infty \leqslant \|x\|_1 \leqslant n\|x\|_\infty$
(3) $\|x\|_\infty \leqslant \|x\|_2 \leqslant \sqrt{n}\|x\|_\infty$

Démonstration. En mettant au carré la première inégalité nous voyons que nous devons vérifier l'inégalité

$$|x_1|^2 + \cdots + |x_n|^2 \leqslant \big(|x_1| + \cdots + |x_n|\big)^2 \tag{12.2}$$

qui est vraie parce que le membre de droite est égal au carré de chaque terme plus les double produits. La seconde inégalité provient de l'inégalité de Cauchy-Schwarz (théorème 11.10) sur les vecteurs

$$v = \begin{pmatrix} 1/n \\ \vdots \\ 1/n \end{pmatrix}, \quad w = \begin{pmatrix} |x_1| \\ \vdots \\ |x_n| \end{pmatrix}. \tag{12.3}$$

Nous trouvons

$$\frac{1}{n}\sum_i |x_i| \leqslant \sqrt{n \cdot \frac{1}{n^2}}\sqrt{\sum_i |x_i|^2}, \tag{12.4}$$

et par conséquent

$$\sum_i |x_i| \leqslant \sqrt{n}\|x\|_2. \tag{12.5}$$

La première inégalité de (3) se démontre en remarquant que si a et b sont positifs, $a \leqslant \sqrt{a^2 + b}$. En appliquant cela à $a = \max_i |x_i|$, nous avons

$$\max_i |x_i| \leqslant \sqrt{|x_1|^2 + \cdots + |x_n|^2} \tag{12.6}$$

parce que $\max_i |x_i|$ est évidemment un des termes de la somme. Pour la seconde inégalité de (3), nous avons

$$\sqrt{\sum_k |x_k|^2} \leqslant \left(\sum_k \max_i |x_i|^2\right)^{1/2} = \sqrt{n}\|x\|_\infty. \tag{12.7}$$

Pour obtenir cette inégalité, nous avons remplacé tous les termes $|x_k|$ par le maximum. □

Pour les autres normes $\|.\|_p$, il y a des inégalités dans 13.350 et 18.96 ; voir aussi le thème 7.

En réalité, toutes les normes $\|.\|_{L^p}$ et $\|.\|_\infty$ sont équivalentes et, plus généralement, nous avons le résultat suivant, très étonnant à première vue, et en réalité assez difficile à prouver :

Théorème 12.6 ([173])**.**
Sur un espace vectoriel de dimension finie, toutes les normes sont équivalentes.

Corollaire 12.7.
Soit V un espace vectoriel de dimension finie et $\|.\|_1$, $\|.\|_2$ deux normes sur V. Alors l'identité $\mathrm{Id}\colon V \to V$ *est un isomorphisme d'espace topologique* $(V, \|.\|_1) \to (V, \|.\|_2)$.

De plus les ouverts sont les mêmes : une partie de V est ouverte dans $(V, \|.\|_1)$ si et seulement si elle est ouverte dans $(V, \|.\|_2)$.

12.8.
L'exemple 11.13 donne une norme sur $\mathbb{R}^2$ qui ne dérive pas d'un produit scalaire. Vu que toutes les normes sur $\mathbb{R}^2$ produisent la même topologie (c'est le corollaire 12.7), il y a parfaitement moyen pour deux espaces vectoriels topologiques d'être isomorphes alors que l'un a une norme dérivant d'un produit scalaire et l'autre non.

Le théorème d'équivalence de norme sera utilisé pour montrer que l'ensemble des formes quadratiques non dégénérées de signature (p, q) est ouvert dans l'ensemble des formes quadratiques, proposition 18.112. Plus généralement il est utilisé à chaque fois que l'on fait de la topologie sur les espaces de matrices en identifiant $\mathbb{M}(n, \mathbb{R})$ à $\mathbb{R}^{n^2}$, pour se rassurer en se disant que ce qu'on fait ne dépend pas de la norme choisie.

Proposition 12.9 ([1]).
Let V be a finite dimensional complex vector space. For a basis $B = \{e_1, \dots, e_n\}$ of V we define
Soit un espace vectoriel V de dimension finie sur $\mathbb{C}$. Pour une base $B = \{e_i\}$ de V nous définissons

$$\|\sum_k v_k e_k\|_B = \sqrt{\sum_k |v_k|^2}. \tag{12.8}$$

(1) La formule (12.8) définit une norme sur V.

(2) Si B et B' sont des bases de V, alors les topologies induites par le norme $\|.\|_B$ et $\|.\|_{B'}$ sont égales.

Démonstration. Nous commençons par fixer une base $B = \{e_i\}_{i=1,\dots,n}$ de V. Cette base nous permet de définir

$$\begin{aligned} \varphi\colon V &\to \mathbb{C}^n \\ \sum_k v_k e_k &\mapsto (v_1, \dots, v_n). \end{aligned} \tag{12.9}$$

Cette application linéaire permet d'écrire

$$\|v\|_V = \|\varphi(v)\|_{\mathbb{C}^n}. \tag{12.10}$$

À partir de là, la vérification des propriétés de la définition 7.106 est immédiate. Par exemple :

$$\|v + w\| = \|\varphi(v + w)\| = \|\varphi(v) + \varphi(w)\| \leqslant \|\varphi(v)\| + \|\varphi(w)\| = \|v\| + \|w\|. \tag{12.11}$$

En ce qui concerne la seconde assertion, c'est le théorème 12.6. □

12.1.2 Contre-exemple en dimension infinie

Lorsque nous considérons des espaces vectoriels de dimension infinie, les choses ne sons plus aussi simples. Nous voyons ici sur l'exemple de l'espace des polynômes que le théorème 12.6 n'est plus valable si on enlève l'hypothèse de dimension finie.

On considère l'ensemble des fonctions polynomiales à coefficients réels sur l'intervalle $[0, 1]$.

$$\mathcal{P}_{\mathbb{R}}([0,1]) = \{p : [0,1] \to \mathbb{R} \,|\, p : x \mapsto a_0 + a_1 x + a_2 x^2 + \dots,\ a_i \in \mathbb{R},\ \forall i \in \mathbb{N}\}. \tag{12.12}$$

Cet ensemble, muni des opérations usuelles de somme entre polynômes et multiplications par les scalaires, est un espace vectoriel.

Sur $\mathcal{P}(\mathbb{R})$ on définit les normes suivantes

$$\begin{aligned} \|p\|_\infty &= \sup_{x\in[0,1]} \{p(x)\}, \\ \|p\|_1 &= \int_0^1 |p(x)|\, dx, \\ \|p\|_2 &= \left(\int_0^1 |p(x)|^2\, dx\right)^{1/2}. \end{aligned} \tag{12.13}$$

Les inégalités suivantes sont immédiates

$$\begin{aligned} \|p\|_1 &= \int_0^1 |p(x)|\, dx \leqslant \|p\|_\infty, \\ \|p\|_2 &= \left(\int_0^1 |p(x)|^2\, dx\right)^{1/2} \leqslant \|p\|_\infty, \end{aligned} \tag{12.14}$$

mais la norme $\| \cdot \|_\infty$ n'est équivalente ni à $\| \cdot \|_1$, ni à $\| \cdot \|_2$. Soit $p_k(x) = x^k$. Alors

$$\begin{aligned} \|p_k\|_\infty &= 1, \\ \|p_k\|_1 &= \int_0^1 x^k \, dx = \frac{1}{k+1}, \\ \|p_k\|_2 &= \left(\int_0^1 x^{2k} \, dx \right)^{1/2} = \sqrt{\frac{1}{2k+1}}. \end{aligned} \tag{12.15}$$

Pour $k \to \infty$ les normes $\|p_k\|_1$, $\|p_k\|_2$ tendent vers zéro, alors que la norme $\|p_k\|_\infty$ est constante, donc les normes ne sont pas équivalentes parce que il n'existe pas un nombre positif m tel que

$$\begin{aligned} m\|p_k\|_\infty &\leqslant \|p_k\|_1, \\ m\|p_k\|_\infty &\leqslant \|p_k\|_2, \end{aligned} \tag{12.16}$$

uniformément pour tout k dans $\mathbb{N}$.

12.2 Norme opérateur

La proposition suivante donne une norme (au sens de la définition 7.106) sur $\mathcal{L}(V, W)$ dès que V et W sont des espaces vectoriels normés.

Proposition-définition 12.10 (Norme opérateur[174], thème 41)**.**
Soit une application linéaire $T : V \to W$, et le nombre

$$\|T\|_{\mathcal{L}} = \sup_{\substack{x \in V \\ x \neq 0}} \frac{\|T(x)\|_W}{\|x\|_V}. \tag{12.17}$$

(1) Si V est de dimension finie, alors $\|T\|_{\mathcal{L}} < \infty$.

(2) L'application $T \mapsto \|T\|_{\mathcal{L}}$ est une norme sur l'espace vectoriel des applications linéaires $V \to W$.

(3) Nous avons la formule

$$\|T\|_{\mathcal{L}} = \sup_{x \in V} \frac{\|T(x)\|_W}{\|x\|_V} = \sup_{\|x\|_V = 1} \|T(x)\|_W \tag{12.18}$$

*Le nombre $\|T\|_{\mathcal{L}}$ est la **norme opérateur** de T. Nous disons que cette norme est **subordonnée** aux normes choisies sur V et W.*

Démonstration. Si V est de dimension finie alors l'ensemble $\{\|x\| = 1\}$ est compact par le théorème de Borel-Lebesgue 8.9. Alors la fonction

$$x \mapsto \frac{\|T(x)\|}{\|x\|} \tag{12.19}$$

est une fonction continue sur un compact. Le corollaire 9.45 nous dit alors qu'elle est bornée. Le supremum est donc un nombre réel fini.

Nous vérifions que l'application $\|.\|$ de $\mathcal{L}(V, W)$ dans $\mathbb{R}$ ainsi définie est effectivement une norme.

(1) $\|T\|_{\mathcal{L}} = 0$ signifie que $\|T(x)\| = 0$ pour tout x dans V. Comme $\| \cdot \|_W$ est une norme nous concluons que $T(x) = 0_n$ pour tout x dans V, donc T est l'application nulle.

(2) Pour tout a dans $\mathbb{R}$ et tout T dans $\mathcal{L}(V, W)$ nous avons

$$\|aT\|_{\mathcal{L}} = \sup_{\|x\|_V \leqslant 1} \|aT(x)\|_W = |a| \sup_{\|x\|_V \leqslant 1} \|T(x)\|_W = |a| \|T\|_{\mathcal{L}}. \tag{12.20}$$

(3) Pour tous T_1 et T_2 dans $\mathcal{L}(V,W)$ nous avons

$$\begin{aligned}\|T_1+T_2\|_{\mathcal{L}} &= \sup_{\|x\|\leqslant 1}\|T_1(x)+T_2(x)\| \leqslant \\ &\leqslant \sup_{\|x\|\leqslant 1}\|T_1(x)\| + \sup_{\|x\|\leqslant 1}\|T_2(x)\| \\ &= \|T_1\|\|T_2\|.\end{aligned}$$

Enfin nous prouvons la formule alternative (12.18). Nous allons montrer que les ensembles sur lesquels ont prend le supremum sont en réalité les mêmes :

$$\underbrace{\left\{\frac{\|Ax\|}{\|x\|}\right\}_{x\neq 0}}_{A} = \underbrace{\{\|Ax\| \text{ tel que } \|x\|=1\}}_{B}. \tag{12.21}$$

Attention : ce sont des sous-ensembles de réels ; pas de sous-ensembles de $\mathbb{M}(\mathbb{R})$ ou des sous-ensembles de $\mathbb{R}^n$.

Pour la première inclusion, prenons un élément de A, et prouvons qu'il est dans B. C'est-à-dire que nous prenons $x\in V$ et nous considérons le nombre $\|Ax\|/\|x\|$. Le vecteur $y=x/\|x\|$ est un vecteur de norme 1, donc la norme de Ay est un élément de B, mais

$$\|Ay\| = \frac{\|Ax\|}{\|x\|}. \tag{12.22}$$

Nous avons donc $A\subset B$.

L'inclusion $B\subset A$ est immédiate. □

En d'autres termes, il y a autant de normes opérateur sur $\mathcal{L}(E,F)$ qu'il y a de paires de choix de normes sur E et F. En particulier, cela donne lieu à toutes les normes $\|A\|_p$ qui correspondent aux normes $\|.\|_p$ sur $\mathbb{R}^n$.

Exemple 12.11

Voyons la norme opérateur subordonnée à la norme $\|x\|_\infty = \max_i |x_i|$ sur $\mathbb{C}^n$. Par définition (et surtout par la propriété 12.10(3)),

$$\|A\|_\infty = \sup_{\|x\|_\infty=1} = \|Ax\|_\infty. \tag{12.23}$$

Vu que $(Ax)_i = \sum_k A_{ik}x_k$, lorsque $\|x\|_\infty\leqslant 1$ nous avons $|(Ax)_i|\leqslant\sum_k|A_{ik}|$. Donc nous avons toujours

$$\|A\|_\infty \leqslant \max_i\sum_k |A_{ik}|. \tag{12.24}$$

△

Définition 12.12.

*La **topologie forte** sur l'espace des opérateurs est la topologie de la norme opérateur.*

Lorsque nous considérons un espace vectoriel d'applications linéaires, nous considérons toujours [1] dessus la topologie liée à cette norme.

Il existe aussi la **topologie faible** donnée par la notion de convergence [2] $A_i\to A$ si et seulement si $A_ix\to Ax$ pour tout $x\in E$.

Problèmes et choses à faire

Je crois, mais demande confirmation, que la topologie faible est celle des semi-normes $\{p_v\}_{v\in E}$ données par $p_v(A)=\|A\|$. En effet la notion de convergence associée par la proposition 9.77 est $A_i\to A$ si et seulement si $p_v(A_i-A)\to 0$. Cette condition signifie $\|A_i(v)-A(v)\|\to 0$, c'est-à-dire $A_i(v)\to A(v)$.

Si le lecteur veut parler de cela au jury d'un concours, il est évident qu'il devra être capable d'ajouter des petits symboles au-dessus de toutes les flèches « → » du paragraphe précédent pour indiquer pour quelles topologies sont les convergences dont on parle.

1. Sauf lorsque les événements nous forceront à trahir.
2. Est-ce qu'on peut décrire cette topologie à partir de ses ouverts ? Facilement ?

Remarque 12.13.
Il faut noter que la topologie faible n'est pas une topologie métrique. Cela même si la condition $A_i x \to Ax$, elle, est métrique vu qu'elle est écrite dans E.

Dans le cas où E est de dimension infinie, la topologie faible est réellement différente de la topologie forte. Nous verrons à la sous-section 26.3.6 que dans le cas des projections sur un espaces de Hilbert, l'égalité

$$\sum_{i=1}^{\infty} \mathtt{proj}_{u_i} = \mathrm{Id} \tag{12.25}$$

est vraie pour la topologie faible, mais pas pour la topologie forte.

12.2.1 Norme d'algèbre

Définition 12.14 (Norme d'algèbre[174])**.**
Si A est une algèbre[3]*, une **norme d'algèbre** sur A est une norme telle que pour toute $x, y \in A$,*

$$\|xy\| \leqslant \|x\|\|y\|. \tag{12.26}$$

La norme opérateur est une norme d'algèbre, comme nous le verrons dans le lemme 12.20.

Un des intérêts d'utiliser une norme d'algèbre est que l'on a l'inégalité $\|x^k\| \leqslant \|x\|^k$. Cela sera particulièrement utile lors de l'étude des séries entières, voir par exemple 16.12.

Définition 12.15 ([175])**.**
*Le **rayon spectral** d'une matrice carrée A, noté $\rho(A)$, est défini de la manière suivante :*

$$\rho(A) = \max_i |\lambda_i| \tag{12.27}$$

où les λ_i sont les valeurs propres de A.

12.16.
Quelques remarques sur la définition du rayon spectral.

- Même si A est une matrice réelle, les valeurs propres sont dans $\mathbb{C}$. Donc dans (12.27), $|\lambda_i|$ est le module dans $\mathbb{C}$ de λ_i.
- Vu que les valeurs propres de A sont les racines de son polynôme caractéristique (théorème 11.150), il y en a un nombre fini et le maximum est bien défini.
- La définition s'applique uniquement pour les espaces de dimension finie.

Lemme 12.17.
Soient des espaces vectoriels normés E et F, sur les corps $\mathbb{R}$ ou $\mathbb{C}$. Pour tout $A \in \mathcal{L}(E, F)$, et pour tout $u \in E$ nous avons la majoration

$$\|Au\| \leqslant \|A\|\|u\| \tag{12.28}$$

où la norme sur A est la norme opérateur subordonnée à la norme sur u.

Démonstration. Si $u \in E$ alors, étant donné que le supremum d'un ensemble est plus grand ou égal à chacun de éléments qui le compose,

$$\|A\| = \sup_{x \in E} \frac{\|Ax\|}{\|x\|} \geqslant \frac{\|Au\|}{\|u\|}, \tag{12.29}$$

donc le résultat annoncé : $\|Au\| \leqslant \|A\|\|u\|$. □

Le lemme suivant est valable en dimension infinie. Nous en toucherons un mot dans l'exemple 12.37.

3. Définition 3.71.

Lemme 12.18.
Soient des espaces vectoriels normés E et F. Soit $x \in E$. Alors l'application d'évaluation

$$\begin{aligned} ev_x \colon \mathcal{L}(E,F) &\to F \\ f &\mapsto f(x) \end{aligned} \tag{12.30}$$

est continue.

Démonstration. Si $x = 0$, alors par linéarité de f nous avons $ev_0(f) = 0$ pour tout f. Donc d'accord pour la continuité.

Soit une suite convergente $f_k \xrightarrow{\mathcal{L}(E,F)} f$. Nous voulons prouver que $ev_x(f_k) \xrightarrow{F} ev_x(f)$, c'est-à-dire que

$$\lim_{k\to\infty} \|f_k(x) - f(x)\| = 0. \tag{12.31}$$

Par hypothèse si k est grand, alors $\|f_k - f\|_{\mathcal{L}(E,F)} \leqslant \epsilon$, c'est-à-dire que [4]

$$\sup_{y\in E} \frac{\|f_k(y) - f(y)\|}{\|y\|} \leqslant \epsilon. \tag{12.32}$$

En particulier pour notre x nous avons

$$\frac{\|f_k(x) - f(x)\|}{\|x\|} \leqslant \epsilon, \tag{12.33}$$

c'est-à-dire $\|f_k(x) - f(x)\| \leqslant \|x\|\epsilon$. Vu que $\|x\|$ est une simple constante et que ϵ est arbitraire, cela implique $f_k(x) \to f(x)$. □

12.2.2 Matrices, spectre et norme

La lien entre la norme opérateur d'une matrice et son spectre sera entre autres utilisé pour étudier le conditionnement de problèmes numériques. Voir la définition 35.105 et par exemple son lien avec la résolution numérique de systèmes linéaires dans la proposition 35.109.

Proposition 12.19 ([175]).
Soit une matrice $A \in \mathbb{M}(n,\mathbb{C})$ de rayon spectral $\rho(A)$. Soit une norme $\|.\|$ sur $\mathbb{C}^n$ et la norme opérateur correspondante. Alors

$$\rho(A) \leqslant \|A^k\|^{1/k} \tag{12.34}$$

pour tout $k \in \mathbb{N}$.

Démonstration. Soit $v \in \mathbb{C}^n$ et $\lambda \in \mathbb{C}$ un couple vecteur-valeur propre. Nous avons $\|Av\| = |\lambda|\|v\|$ et aussi

$$|\lambda|^k\|v\| = \|\lambda^k v\| = \|A^k v\| \leqslant \|A^k\|\|v\|. \tag{12.35}$$

La dernière inégalité est due au fait que nous avons choisi sur $\mathbb{M}(n,\mathbb{C})$ la norme subordonnée à celle choisie sur $\mathbb{C}^n$, via le lemme 12.17. Nous simplifions par $\|v\|$ et obtenons $|\lambda| \leqslant \|A^k\|^{1/k}$. Étant donné que $\rho(A)$ est la maximum de tous les λ possibles, la majoration passe au maximum :

$$\rho(A) \leqslant \|A^k\|^{1/k}. \tag{12.36}$$

□

Lemme 12.20 (La norme opérateur est une norme d'algèbre[1]).
Soient des espaces vectoriels normés E, F et G. Soient des opérateurs linéaires bornés $B \colon E \to F$, $A \colon F \to G$. Alors

$$\|AB\| \leqslant \|A\|\|B\|. \tag{12.37}$$

C'est à dire que la norme opérateur est une norme d'algèbre [5].

4. Définition 12.10 de la norme sur $\mathcal{L}(E,F)$.
5. Définition 12.14.

Démonstration. Nous avons les (in)égalités suivantes :

$$\|AB\| = \sup_{x\in E} \frac{\|ABx\|_G}{\|x\|_E} \tag{12.38a}$$
$$= \sup_{\substack{x\in E\\ Bx\neq 0}} \frac{\|ABx\|}{\|x\|}\frac{\|Bx\|_F}{\|Bx\|_F} \tag{12.38b}$$
$$= \sup_{\substack{x\in E\\ Bx\neq 0}} \frac{\|ABx\|}{\|Bx\|}\frac{\|Bx\|}{\|x\|} \tag{12.38c}$$
$$\leqslant \underbrace{\sup_{\substack{x\in E\\ Bx\neq 0}} \frac{\|ABx\|}{\|Bx\|}}_{\leqslant\|A\|} \underbrace{\sup_{\substack{y\in E\\ By\neq 0}} \frac{\|Bx\|}{\|y\|}}_{=\|B\|} \tag{12.38d}$$
$$\leqslant \|A\|\|B\|. \tag{12.38e}$$

La dernière inégalité provient que dans $\sup_{\substack{x\in E\\ Bx\neq 0}} \|ABx\|/\|x\|$, le supremum est pris sur un ensemble plus petit que celui sur lequel porte la définition de la norme de A : seulement l'image de B au lieu de tout l'espace de départ de A. □

Proposition 12.21.
Soient deux espaces vectoriels normés E et V. Soient des applications continues $f, g\colon E \to \mathrm{End}(V)$. Alors l'application

$$\begin{aligned}\psi\colon E &\to \mathrm{End}(V)\\ x &\mapsto f(x)\circ g(x)\end{aligned} \tag{12.39}$$

est continue.

Démonstration. Soit une suite $x_k \xrightarrow{E} x$. Nous devons montrer que $\psi(x_k) \xrightarrow{\mathrm{End}(V)} \psi(x)$. Pour cela nous utilisons le lemme 12.20 qui indique que la norme opérateur est une norme d'algèbre. Nous avons :

$$\|\psi(x_k) - \psi(x)\| = \|f(x_k)\circ g(x_k) - f(x)\circ g(x)\| \tag{12.40a}$$
$$\leqslant \|f(x_k)\circ g(x_k) - f(x_k)\circ g(x)\| + \|f(x_k)\circ g(x) - f(x)\circ g(x)\| \tag{12.40b}$$
$$= \|f(x_k)\circ \big(g(x_k)\circ g(x)\big)\| + \|\big(f(x_k) - f(x)\big)\circ g(x)\| \tag{12.40c}$$
$$\leqslant \|f(x_k)\|\|g(x_k) - g(x)\| + \|f(x_k) - f(x)\|\|g(x)\|. \tag{12.40d}$$

Pour $k \to \infty$ nous avons $\|f(x_k) \to \|f(x)\|\|$, $\|f(x_k) - f(x)\| \to 0$ (parce que f est continue) et similaire avec g. Donc le tout tend vers zéro. □

12.2.3 Rayon spectral

La chose impressionnante dans la proposition suivante est que $\rho(A)$ est définit indépendamment du choix de la norme sur $\mathbb{M}(n,\mathbb{K})$ ou sur $\mathbb{K}$. Lorsque nous écrivons $\|A\|$, nous disons implicitement qu'une norme a été choisie sur $\mathbb{K}$ et que nous avons pris la norme subordonnée sur $\mathbb{M}(n,\mathbb{K})$.

Proposition 12.22 ([176])**.**
Soit A une matrice de $\mathbb{M}(n,\mathbb{R})$ ou $\mathbb{M}(n,\mathbb{C})$. Alors

$$\rho(A) \leqslant \|A\|. \tag{12.41}$$

Démonstration. Nous devons séparer les cas suivant que le corps de base soit $\mathbb{R}$ ou $\mathbb{C}$.

Pour $A \in \mathbb{M}(n,\mathbb{C})$ Soit λ une valeur propre de A telle que $|\lambda|$ soit la plus grande. Nous avons donc $\rho(A) = |\lambda|$. Soit un vecteur propre $u \in \mathbb{C}^n$ pour la valeur propre λ. En prenant la norme sur l'égalité $Au = \lambda u$, et en utilisant le lemme 12.17,

$$|\lambda|\|u\| = \|Au\| \leqslant \|A\|\|u\|. \tag{12.42}$$

Donc $|\lambda| \leqslant \|A\|$ et $\rho(A) \leqslant \|A\|$.

Pour $A \in \mathbb{M}(n,\mathbb{R})$ L'endroit qui coince dans le raisonnement fait pour $\mathbb{M}(n,\mathbb{C})$ est que certes $A \in \mathbb{M}(n,\mathbb{R})$ possède une plus grande valeur propre en module et qu'un vecteur propre lui est associé. Mais ce vecteur propre est a priori dans $\mathbb{C}^n$, et non dans $\mathbb{R}^n$. Nous pouvons donc écrire $Au = \lambda u$, mais pas $\|Au\| = |\lambda|\|u\|$ parce que nous ne savons pas quelle norme prendre sur $\mathbb{C}^n$.

Il n'est pas certain que nous ayons une norme sur $\mathbb{C}^n$ qui se réduit sur $\mathbb{R}^n$ à celle choisie implicitement dans l'énoncé. Nous allons donc ruser un peu.

Soit une norme N sur $\mathbb{C}^n$ [6]. Nous nommons également N la norme subordonnée sur $\mathbb{M}(n,\mathbb{C})$ et la norme restreinte sur $\mathbb{M}(n,\mathbb{R})$. Vu que N est une norme sur $\mathbb{M}(n,\mathbb{R})$ et que ce dernier est de dimension finie, le théorème 12.6 nous indique que N est équivalente à $\|.\|$. Il existe donc $C > 0$ tel que

$$N(B) \leqslant C\|B\| \tag{12.43}$$

pour tout $B \in \mathbb{M}(n,\mathbb{R})$. Nous avons maintenant

$$\rho(A)^m \leqslant N(A^m) \leqslant C\|A^m\| \leqslant C\|A\|^m. \tag{12.44}$$

Justifications

— Par la proposition 12.19.

— Parce que $A^m \in \mathbb{M}(n,\mathbb{R})$ et la relation (12.43).

— Par itération du lemme 12.20.

Nous avons donc $\rho(A) \leqslant C^{1/m}\|A\|$ pour tout $m \in \mathbb{N}$. En prenant $m \to \infty$ et en tenant compte de $C^{1/m} \to 1$ nous trouvons $\rho(A) \leqslant \|A\|$.

□

Lemme 12.23 ([176]).
Soit $A \in \mathbb{M}(n,\mathbb{K})$ avec $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Soit $\epsilon > 0$. Il existe une norme algébrique sur $\mathbb{M}(n,\mathbb{K})$ telle que

$$N(A) \leqslant \rho(A) + \epsilon. \tag{12.45}$$

Démonstration. Soit par le lemme 11.176 une matrice inversible U telle que $T = UAU^{-1}$ soit triangulaire supérieure, avec les valeurs propres sur la diagonale. Notons que même si $A \in \mathbb{M}(n,\mathbb{R})$, les matrices U et T sont a priori complexes.

Soit $s \in \mathbb{R}$ ainsi que les matrices

$$D_s = \operatorname{diag}(1, s^{-1}, s^{-2}, \dots, s^{1-n}) \tag{12.46}$$

et $T_s = D_s T D_s^{-1}$. Nous fixerons un choix de s plus tard.

La norme que nous considérons est :

$$N(B) = \|(D_sU)B(D_sU)^{-1}\|_\infty \tag{12.47}$$

où $\|.\|_\infty$ est la norme sur $\mathbb{M}(,n\mathbb{K})$ subordonnée à la norme $\|.\|_\infty$ sur $\mathbb{K}^n$ dont nous avons déjà parlé dans l'exemple 12.11. Cela est bien une norme parce que

— Nous avons $\|B\|_\infty = 0$ si et seulement si $B = 0$, et vu que (D_sU) est inversible nous avons $(D_sU)B(D_sU)^{-1} = 0$ si et seulement si $B = 0$.

— $N(\lambda B) = |\lambda|N(B)$.

— Pour l'inégalité triangulaire :

$$\begin{aligned} N(B+C) &= \|(D_sU)B(D_sU)^{-1} + (D_sU)C(D_sU)^{-1}\|_\infty && \text{(12.48a)}\\ &\leqslant \|(D_sU)B(D_sU)^{-1}\|_\infty + \|(D_sU)C(D_sU)^{-1}\|_\infty && \text{(12.48b)}\\ &= N(B) + N(C). && \text{(12.48c)} \end{aligned}$$

6. Il y en a plein, par exemple celle du produit scalaire $\langle x, y\rangle = \sum_k x_k\bar{y}_k$.

En ce qui concerne la matrice A elle-même, nous avons

$$N(A) = \|(D_sU)A(D_sU)^{-1}\|_\infty = \|T_s\|_\infty. \tag{12.49}$$

C'est le moment de se demander comment se présente la matrice T_s. En tenant compte du fait que $(D_s)_{ik} = \delta_{ik}s^{1-i}$ nous avons

$$(T_s)_{ij} = \sum_{kl}(D_s)_{ik}T_{kl}(D_s^{-1})_{lj} = T_{ij}s^{j-i}. \tag{12.50}$$

La matrice T est encore triangulaire supérieure avec les valeurs propres de A sur la diagonale. Les éléments au-dessus de la diagonale sont tous multipliés par au moins s. Il est donc possible de choisir s suffisamment petit pour avoir [7]

$$\sum_{j=i+1}^{n} |(T_s)_{ij}| < \epsilon \tag{12.51}$$

Avec ce choix, la formule 12.24 donne

$$N(T_s) \leqslant \max_i \sum_k |(T_s)_{ik}| \leqslant \epsilon + \rho(A). \tag{12.52}$$

En effet le ϵ vient de la somme sur toute la ligne sauf la diagonale (c'est-à-dire la partie $k \neq i$) et du choix (12.51) pour s. Le $\rho(A)$ provient du dernier terme de la somme (le terme sur la diagonale) qui est une valeur propre de A, donc majorable par $\rho(A)$.

Nous devons encore prouver que N est une norme algébrique. Pour cela nous allons montrer qu'elle est subordonnée à la norme

$$\begin{aligned} n\colon \mathbb{K}^n &\to \mathbb{R}^+ \\ v &\mapsto \|(UD_s)v\|_\infty. \end{aligned} \tag{12.53}$$

Cela sera suffisant pour avoir une norme algébrique par le lemme 12.20. La norme n sur $\mathbb{K}^n$ produit la norme suivante sur $\mathbb{M}(n,\mathbb{K})$:

$$n(B) = \sup_{v\neq 0}\frac{n(B)}{n(v)} = \sup_{v\neq 0}\frac{\|(UD_s)Bv\|_\infty}{\|UD_sv\|_\infty}. \tag{12.54}$$

Vu que UD_s est inversible nous pouvons effectuer le changement de variables $v \mapsto (UD_s)^{-1}v$ pour écrire

$$n(B) = \sup_{v\neq 0}\frac{\|(UD_s)B(UD_s)^{-1}v\|_\infty}{\|(UD_s)(UD_s)^{-1}v\|_\infty} = \sup_{v\neq 0}\frac{\|(UD_s)B(UD_s)^{-1}v\|_\infty}{\|v\|_\infty} = \|(UD_s)B(UD_s)^{-1}\|_\infty = N(B). \tag{12.55}$$

□

Proposition 12.24.
Si $A \in \mathbb{M}(n,\mathbb{R})$ alors $\rho(A)^m = \rho(A^m)$ pour tout $m \in \mathbb{N}$.

Démonstration. La matrice A peut être vue dans $\mathbb{M}(n,\mathbb{C})$ et nous pouvons lui appliquer le corollaire 11.182 :

$$\mathrm{Spec}(A^k) = \{\lambda^k \text{ tel que } \lambda \in \mathrm{Spec}(A)\}. \tag{12.56}$$

À noter qu'il n'y a pas de magie : le spectre de la matrice réelle A est déjà défini en voyant A comme matrice complexe. Le spectre dont il est question dans (12.56) est bien celui dont on parle dans la définition du rayon spectral.

7. Il me semble qu'il manque un module dans [176].

Nous avons ensuite :

$$\rho(A^k) = \max\{|\lambda| \text{ tel que } \lambda \in \text{Spec}(A^k)\} \tag{12.57a}$$
$$= \max\{|\lambda^k| \text{ tel que } \lambda \in \text{Spec}(A)\} \tag{12.57b}$$
$$= \max\{|\lambda|^k \text{ tel que } \lambda \in \text{Spec}(A)\} \tag{12.57c}$$
$$= \rho(A)^k. \tag{12.57d}$$

□

Proposition 12.25 (Bornée si et seulement si continue[177])**.**
Soient E et F des espaces vectoriels normés. Une application linéaire $E \to F$ est bornée si et seulement si elle est continue.

Démonstration. Nous commençons par supposer que A est bornée. Par le lemme 12.20, pour tout $x, y \in E$, nous avons

$$\|A(x) - A(y)\| = \|A(x - y)\| \leqslant \|A\|\|x - y\|. \tag{12.58}$$

En particulier si $x_n \xrightarrow{E} x$ alors

$$0 \leqslant \|A(x_n) - A(x)\| \leqslant \|A\|\|x_n - x\| \to 0 \tag{12.59}$$

et A est continue en vertu de la caractérisation séquentielle de la continuité, proposition 7.74.

Nous supposons maintenant que $\|A\|$ n'est pas borné : l'ensemble $\{\|A(x)\| \text{ tel que } \|x\| = 1\}$ contient des valeurs arbitrairement grandes. Alors pour tout $k \geqslant 1$ il existe $x_k \in B(0,1)$ tel que $\|A(x_k)\| > k$. La suite x_k/k tend vers zéro parce que $\|x_k\| = 1$, mais $\|A(x_k)\| \geqslant 1$ pour tout k. Cela montre que A n'est pas continue. □

Définition 12.26 ([178])**.**
Soient E et F deux espaces vectoriels normés.

- *L'ensemble des applications linéaires $E \to F$ est noté $\mathcal{L}(E, F)$.*
- *Un **morphisme** est une application linéaire $E \to F$ continue pour la topologie de la norme opérateur. Nous avons vu dans la proposition 12.25 que la continuité était équivalente à être bornée. L'ensemble des morphismes est noté $L(E, F)$.*
- *Un **isomorphisme** est un morphisme continu inversible dont l'inverse est continu. Nous notons $\text{GL}(E, F)$ l'ensemble des isomorphismes entre E et F.*

Le point important de la définition 12.26 est la continuité. En dimension infine, la continuité n'est par exemple pas équivalente à l'inversibilité (penser à $e_k \mapsto ke_k$).

12.2.4 Normes de matrices et d'applications linéaires

Théorème 12.27 (Norme matricielle et rayon spectral[179])**.**
La norme 2 d'une matrice est liée au rayon spectral de la façon suivante :

$$\|A\|_2 = \sqrt{\rho(A^t A)} \tag{12.60}$$

ou plus généralement par $\|A\|_2 = \sqrt{\rho(A^* A)}$.

Lemme 12.28.
Soit une matrice $A \in \mathbb{M}(n, \mathbb{R})$ qui est symétrique, strictement définie positive. Soient λ_{min} et λ_{max} les plus petites et plus grandes valeurs propres. Alors

$$\|A\|_2 = \lambda_{max} \qquad \text{et} \qquad \|A^{-1}\|_2 = \frac{1}{\lambda_{min}}. \tag{12.61a}$$

Démonstration. Soient les vecteurs $v_1, \dots, v_n$ formant une base orthonormée de vecteurs propres[8] de A. Nous notons v_{max} celui de λ_{max}. Nous avons :

$$\|A\|_2 \geqslant \|Av_{max}\| = |\lambda_{max}|\|v_{max}\| = |\lambda_{max}| = \lambda_{max}. \tag{12.62}$$

Voilà l'inégalité dans un sens. Montrons l'inégalité dans l'autre sens. Soit $x = \sum_i x_i v_i$ avec $\|x\|_2 = 1$. Alors

$$\|Ax\| = \|\sum_i x_i\lambda_i v_i\| \leqslant \sqrt{\sum_i x_i^2\lambda_i^2} \leqslant \lambda_{max}\sqrt{\sum_i x_i^2} = \lambda_{max}. \tag{12.63}$$

En ce qui concerne l'affirmation pour la norme de A^{-1}, il suffit de remarquer que ses valeurs propres sont les inverses des valeurs propres de A. □

Proposition 12.29.
La fonction

$$\begin{aligned} f\colon \mathbb{M}(n,\mathbb{R}) \times \mathbb{M}(n,\mathbb{R}) &\to \mathbb{R} \\ (X,Y) &\mapsto \mathrm{Tr}(X^tY) \end{aligned} \tag{12.64}$$

est un produit scalaire sur $\mathbb{M}(n,\mathbb{R})$.

Démonstration. Il faut vérifier la définition 11.5.

— La bilinéarité est la linéarité de la trace.

— La symétrie de f est le fait que $\mathrm{Tr}(A^t) = \mathrm{Tr}(A)$.

— L'application f est définie positive parce que si $X \in \mathbb{M}$, alors X^tX est symétrique définie positive, donc diagonalisable avec des nombres positifs sur la diagonale. La trace étant un invariant de similitude, nous avons $f(X,X) = \mathrm{Tr}(X^tX) \geqslant 0$. De plus si $\mathrm{Tr}(X^tX) = 0$, alors $X^tX = 0$ (pour la même raison de diagonalisation). Mais alors $\|Xu\| = 0$ pour tout $u \in E$, ce qui signifie que $X = 0$.

□

Exemple 12.30
Soit $m = n$, un point λ dans $\mathbb{R}$ et T_λ l'application linéaire définie par $T_\lambda(x) = \lambda x$. La norme de T_λ est alors

$$\|T_\lambda\|_{\mathcal{L}} = \sup_{\|x\|_{\mathbb{R}^m}\leqslant 1} \|\lambda x\|_{\mathbb{R}^n} = |\lambda|.$$

Notez que T_λ n'est rien d'autre que l'homothétie de rapport λ dans $\mathbb{R}^m$. △

Exemple 12.31
Considérons la rotation T_α d'angle α dans $\mathbb{R}^2$. Elle est donnée par l'équation matricielle

$$T_\alpha\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}\cos\alpha & \sin\alpha\\ -\sin\alpha & \cos\alpha\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}\cos(\alpha)x + \sin(\alpha)y\\ -\sin(\alpha)x + \cos(\alpha)y\end{pmatrix} \tag{12.65}$$

Étant donné que cela est une rotation, c'est une isométrie : $\|T_\alpha x\| = \|x\|$. En ce qui concerne la norme de T_α nous avons

$$\|T_\alpha\| = \sup_{x\in\mathbb{R}^2}\frac{\|T_\alpha(x)\|}{\|x\|} = \sup_{x\in\mathbb{R}^2}\frac{\|x\|}{\|x\|} = 1. \tag{12.66}$$

Toutes les rotations dans le plan ont donc une norme 1. La même preuve tient pour toutes les rotations en dimension quelconque. △

Exemple 12.32
Soit $m = n$, un point b dans $\mathbb{R}^m$ et T_b l'application linéaire définie par $T_b(x) = b \cdot x$ (petit

8. Possible par le théorème spectral 11.189.

exercice : vérifiez qu'il s'agit vraiment d'une application linéaire). La norme de T_b satisfait les inégalités suivantes

$$\|T_b\|_{\mathcal{L}} = \sup_{\|x\|_{\mathbb{R}^m}\leqslant 1} \|b\cdot x\|_{\mathbb{R}^n} \leqslant \sup_{\|x\|_{\mathbb{R}^m}\leqslant 1} \|b\|_{\mathbb{R}^n}\|x\cdot x\|_{\mathbb{R}^n} \leqslant \|b\|_{\mathbb{R}^n},$$

$$\|T_b\|_{\mathcal{L}} = \sup_{\|x\|_{\mathbb{R}^m}\leqslant 1} \|b\cdot x\|_{\mathbb{R}^n} \geqslant \left\|b\cdot\frac{b}{\|b\|_{\mathbb{R}^n}}\right\|_{\mathbb{R}^n} = \|b\|_{\mathbb{R}^n},$$

donc $\|T_b\|_{\mathcal{L}} = \|b\|_{\mathbb{R}^n}$. △

Proposition 12.33.
Une application linéaire de $\mathbb{R}^m$ dans $\mathbb{R}^n$ est continue.

Démonstration. Soit x un point dans $\mathbb{R}^m$. Nous devons vérifier l'égalité

$$\lim_{h\to 0_m} T(x+h) = T(x). \tag{12.67}$$

Cela revient à prouver que $\lim_{h\to 0_m} T(h) = 0$, parce que $T(x+h) = T(x)+T(h)$. Nous pouvons toujours majorer $\|T(h)\|_n$ par $\|T\|_{\mathcal{L}(\mathbb{R}^m,\mathbb{R}^n)}\|h\|_{\mathbb{R}^m}$ (lemme 12.17). Quand h s'approche de 0_m sa norme $\|h\|_m$ tend vers 0, ce que nous permet de conclure parce que nous savons que de toutes façons, $\|T\|_{\mathcal{L}}$ est fini. □

Note : dans un espace de dimension infinie, la linéarité ne suffit pas pour avoir la continuité : il faut de plus être borné (ce que sont toutes les applications linéaires $\mathbb{R}^m \to \mathbb{R}^n$). Voir la proposition 12.25.

12.2.5 Application linéaire continue et bornée

Nous avons vu dans la proposition 12.25 que pour une application linéaire, être bornée est équivalent à être continue. Nous allons maintenant voir un certain nombre d'exemples illustrant ce fait.

Exemple 12.34(Une application linéaire non continue)
Soit V l'espace vectoriel normé des suites *finies* de réels muni de la norme usuelle $\|c\| = \sqrt{\sum_{i=0}^{\infty}|c_i|^2}$ où la somme est finie. Nous nommons $\{e_k\}_{k\in\mathbb{N}}$ la base usuelle de cet espace, et nous considérons l'opérateur $f\colon V\to V$ donnée par $f(e_k) = ke_k$. C'est évidemment linéaire, mais ce n'est pas continu en zéro. En effet la suite $u_k = e_k/k$ converge vers 0 alors que $f(u_k) = e_k$ ne converge pas. △

Cet exemple aurait pu également être donnée dans un espace de Hilbert, mais il aurait fallu parler de domaine.

Exemple 12.35(Une autre application linéaire non continue[180])
En dimension infinie, une application linéaire n'est pas toujours continue. Soit E l'espace des polynômes à coefficients réels sur $[0,1]$ muni de la norme uniforme. L'application de dérivation $\varphi\colon E\to E$, $\varphi(P) = P'$ n'est pas continue.

Pour la voir nous considérons la suite $P_n = \frac{1}{n}X^n$. D'une part nous avons $P_n \to 0$ dans E parce que $P_n(x) = \frac{x^n}{n}$ avec $x\in[0,1]$. Mais en même temps nous avons $\varphi(P_n) = X^{n-1}$ et donc $\|\varphi(P_n)\| = 1$.

Nous n'avons donc pas $\lim_{n\to\infty}\varphi(P_n) = \varphi(\lim_{n\to\infty}P_n)$ et l'application φ n'est pas continue en 0. Elle n'est donc continue nulle part par linéarité.

Nous avons utilisé le critère séquentiel de la continuité, voir la définition 7.72 et la proposition 7.74. △

Remarque 12.36.
Cette proposition permet de retrouver l'exemple 12.34 plus simplement. Si $\{e_k\}_{k\in\mathbb{N}}$ est une base d'un espace vectoriel normé formée de vecteurs de norme 1, alors l'opérateur linéaire donné par $u(e_k) = ke_k$ n'est pas borné et donc pas continu.

C'est également ce résultat qui montre que le produit scalaire est continu sur un espace de Hilbert par exemple.

Exemple 12.37
Nous avons vu dans le lemme 12.18 que pour un $x \in E$ donné, l'application

$$\begin{aligned} ev_x \colon \mathcal{L}(E,F) &\to F \\ f &\mapsto f(x) \end{aligned} \tag{12.68}$$

est continue. Vu que ev_x est linéaire, la proposition 12.25 nous indique que ev_x est bornée. Vérifions-le directement. Le calcul n'est pas très compliqué :

$$\|ev_x\| = \sup_{\|f\|=1} \|ev_x(f)\| = \sup_{\|f\|=1} \|f(x)\| \leqslant \sup_{\|f\|=1} \|x\|\|f\| = \|x\| \tag{12.69}$$

où nous avons utilisé le lemme 12.17 en passant. Donc la norme de ev_x est majorée par $\|x\|$.

Elle est même égale à $\|x\|$. En effet, pour chaque $f \in \mathcal{L}(E,F)$ tel que $\|f\| = 1$, nous avons

$$\|ev_x\| \geqslant \|ev_x(f)\| = \|f(x)\|. \tag{12.70}$$

En prenant $f = \mathrm{Id}$ nous trouvons $\|ev_x\| \geqslant \|x\|$. △

Définition 12.38.
*Soit un espace vectoriel E sur le corps $\mathbb{K}$. Son **dual topologique**, noté E', est l'ensemble des formes linéaires continues de E vers $\mathbb{K}$.*

Lemme 12.39.
Soit F un espace de Banach et deux suites $A_k \to A$ et $B_k \to B$ dans $\mathcal{L}(F,F)$. Alors $A_k \circ B_k \to A \circ B$ dans $\mathcal{L}(F,F)$, c'est-à-dire

$$\lim_{n\to\infty}(A_kB_k) = \left(\lim_{n\to\infty} A_k\right)\left(\lim_{n\to\infty} B_k\right). \tag{12.71}$$

Démonstration. Il suffit d'écrire

$$\|A_kB_k - AB\| \leqslant \|A_kB_k - A_kB\| + \|A_kB - AB\|. \tag{12.72}$$

Le premier terme tend vers zéro pour $k \to \infty$ parce que

$$\begin{aligned} \|A_kB_k - A_kB\| &= \|A_k(B_k - B)\| && \text{(12.73a)} \\ &\leqslant \|A_k\|\|B_k - B\| \to \|A\| \cdot 0 && \text{(12.73b)} \\ &= 0 && \text{(12.73c)} \end{aligned}$$

où nous avons utilisé la propriété fondamentale de la norme opérateur : la proposition 12.25. Le second terme tend également vers zéro pour la même raison. □

Proposition 12.40 (Distributivité de la somme infinie)**.**
Soient E un espace normé, une suite (u_k) dans $\mathrm{GL}(E)$ ainsi que $a \in \mathrm{GL}(E)$. Pourvu que la série $\sum_{n=0}^{\infty} u_k$ converge nous avons

$$\left(\sum_{k=0}^{\infty} u_k\right) a = \sum_{k=0}^{\infty} (u_k a). \tag{12.74}$$

Démonstration. Par définition de la somme infinie,

$$\spadesuit = \left(\sum_{k=0}^{\infty} u_k\right) a = \left(\lim_{n\to\infty} \sum_{k=0}^{n} u_k\right) a. \tag{12.75}$$

Le lemme 12.39 appliqué à $n \mapsto \sum_{k=0}^{n} u_k$ et à la suite constante a nous donne

$$\spadesuit = \lim_{n\to\infty} \left(\sum_{k=0} u_k a\right), \tag{12.76}$$

ce que nous voulions par distributivité de la somme finie : dans (12.76), le a est dans ou hors de la somme, au choix. L'important est qu'il soit dans la limite. □

12.3 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.

12.3.1 Norme

La définition de la norme sur un produit d'espaces vectoriels normés découle immédiatement de la définition de la distance 9.65 :

Lemme-définition 12.41.
Soient V et W deux espaces vectoriels normés.

(1) L'ensemble

$$V \times W = \{(v, w) \,|\, v \in V,\, w \in W\} \tag{12.77}$$

est un espace vectoriel.

(2) L'opération

$$\|(v, w)\|_{V\times W} = \max\{\|v\|_V, \|w\|_W\}. \tag{12.78}$$

est une norme sur $V \times V$.

*L'espace vectoriel $V \times W$ muni de cette norme est l'**espace produit** de V et W.*

Démonstration. Il est presque immédiat de vérifier que le produit cartésien $V \times W$ est un espace vectoriel pour les opération de somme et multiplication par les scalaires définies composante par composante. C'est-à-dire, si (v_1, w_1), (v_2, w_2) sont dans $V \times W$ et a, b sont des scalaires, alors

$$a(v_1, w_1) + b(v_2, w_2) = (av_1, aw_1) + (bv_2, bw_2) = (av_1 + bv_2, aw_1 + bw_2). \tag{12.79}$$

On doit vérifier les trois conditions de la définition 7.106.

— 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 :

$$\|a(v, w)\|_{V\times W} = \max\{\|av\|_V, \|aw\|_W\} = |a| \max\{\|v\|_V, \|w\|_W\} = |a|\|(v, w)\|_{V\times W}. \tag{12.80}$$

— Soient (v_1, w_1) et (v_2, w_2) dans $V \times W$.

$$\begin{aligned} \|(v_1, w_1) + (v_2, w_2)\|_{V\times W} &= \max\{\|v_1 + v_2\|_V, \|w_1 + w_2\|_W\} \\ &\leqslant \max\{\|v_1\|_V + \|v_2\|_V, \|w_1\|_W + \|w_2\|_W\} \\ &\leqslant \max\{\|v_1\|_V, \|w_1\|_W\} + \max\{\|v_2\|_V, \|w_2\|_W\} \\ &= \|(v_1, w_1)\|_{V\times W} + \|(v_2, w_2)\|_{V\times W}. \end{aligned} \tag{12.81}$$

□

Toutes ces définitions se généralisent à un produit fini d'espaces vectoriels normés. Si les espaces V_i sont des espaces vectoriels normés, nous pouvons mettre sur le produit une topologie et une norme :

— La topologie produit donnée en 7.9

— La norme maximum $\|v_1, \dots, v_n\|_{max} = \max\{\|v_1\|, \dots, \|v_n\|\}$. Dans le membre de droites, toutes les normes sont différentes.

Une question qui vient est la compatibilité entre ces deux constructions. Est-ce que la topologie associée à la norme maximum est le topologie produit ? Oui.

Lemme 12.42 ([181]).
La topologie de la norme maximum est la topologie produit[9].

En particulier, pour la topologie de la norme maximum, la convergence d'une suite implique la convergence « composante par composante » par la proposition 7.34.

Proposition 12.43 ([182]).
Soient des espaces vectoriels normés V et W ainsi qu'une forme sesquilinéaire $\phi\colon V \times W \to \mathbb{C}$. Il y a équivalence des faits suivants.

(1) ϕ est continue.

(2) ϕ est continue en $(0,0)$

(3) ϕ est bornée

(4) Il existe $C \geqslant 0$ telle que $|\phi(x,y)| \leqslant C\|x\|\|y\|$ pour tout $(x,y) \in V \times W$.

De plus la norme de ϕ est alors donnée par

$$\|\phi\| = \min\{C \geqslant 0 \text{ tel que } |\phi(x,y)| \leqslant C\|x\|\|y\| \forall (x,y) \in V \times W\}. \tag{12.82}$$

On remarque tout de suite que la norme $\|.\|_\infty$ sur $\mathbb{R}^2$ est la norme de l'espace produit $\mathbb{R} \times \mathbb{R}$. En outre cette définition nous permet de trouver plusieurs nouvelles normes dans les espaces $\mathbb{R}^p$. Par exemple, si nous écrivons $\mathbb{R}^4$ comme $\mathbb{R}^2 \times \mathbb{R}^2$ on peut munir $\mathbb{R}^4$ de la norme produit

$$\|(x_1, x_2, x_3, x_4)\|_{\infty,2} = \max\{\|(x_1, x_2)\|_\infty, \|(x_3, x_4)\|_2\}.$$

Les applications de projection de l'espace produit $V \times W$ vers les espaces «facteurs», V W sont notées $\mathtt{proj}_V$ et $\mathtt{proj}_W$ et sont définies par

$$\begin{aligned} \mathtt{proj}_V\colon V \times W &\to V \\ (v,w) &\mapsto v \end{aligned} \tag{12.83}$$

et

$$\begin{aligned} \mathtt{proj}_W\colon V \times W &\to W \\ (v,w) &\mapsto w. \end{aligned} \tag{12.84}$$

Les inégalités suivantes sont évidentes

$$\begin{aligned} \|\mathtt{proj}_V(v,w)\|_V &\leqslant \|(v,w)\|_{V\times W} \\ \|\mathtt{proj}_W(v,w)\|_W &\leqslant \|(v,w)\|_{V\times W}. \end{aligned} \tag{12.85}$$

La topologie de l'espace produit est induite par les topologies des espaces «facteurs». La construction est faite en deux passages : d'abord nous disons que une partie $A \times B$ de $V \times W$ est ouverte si A et B sont des parties ouvertes de V et de W respectivement. Ensuite nous définissons que une partie quelconque de $V \times W$ est ouverte si elle est une intersection finie ou une réunion de parties ouvertes de $V \times W$ de la forme $A \times B$.

Ce choix de topologie donne deux propriétés utiles de l'espace produit

9. Définition 7.9.

(1) Les projections sont des **applications ouvertes**. Cela veut dire que l'image par $\texttt{proj}_V$ (respectivement $\texttt{proj}_W$) de toute partie ouverte de $V \times W$ est une partie ouverte de V (respectivement W).

(2) Pour toute partir A de V et B de W, nous avons $\text{Int}(A \times B) = \text{Int}\, A \times \text{Int}\, B$.

Une propriété moins facile a prouver est que pour toute partie A de V et B de W nous avons $\overline{A \times B} = \bar{A} \times \bar{B}$. Voir le lemme 12.46.

Ce que nous avons dit jusqu'ici est valable pour tout produit d'un nombre fini d'espaces vectoriels normés. En particulier, pour tout $m > 0$ l'espace $\mathbb{R}^m$ peut être considéré comme le produit de m copies de $\mathbb{R}$.

Exemple 12.44
Si V et W sont deux espaces vectoriels, nous pouvons considérer le produit $E = V \times W$. Les projections $\texttt{proj}_V$ et $\texttt{proj}_W$, définies dans la section 12.3, sont des applications linéaires.

En effet, la projection $\texttt{proj}_V \colon V \times W \to V$ est donnée par $\texttt{proj}_V(v, w) = v$. Alors,

$$\begin{aligned} \texttt{proj}_V\big((v, w) + (v', w')\big) &= \texttt{proj}_V\big((v + v'), (w + w')\big) \\ &= v + v' \\ &= \texttt{proj}_V(v, w) + \texttt{proj}_V(v', w'), \end{aligned} \tag{12.86}$$

et

$$\texttt{proj}_V\big(\lambda(v, w)\big) = \texttt{proj}_V\big((\lambda v, \lambda w)\big) = \lambda v = \lambda\, \texttt{proj}_V(v, w). \tag{12.87}$$

Nous laissons en exercice le soin d'adapter ces calculs pour montrer que $\texttt{proj}_W$ est également une projection. △

Proposition 12.45.
Si $\mathcal{O}$ est un voisinage de (a, b) dans $V \times W$ alors $\mathcal{O}$ contient un ouvert de la forme $B(a, r) \times B(b, r)$.

Démonstration. Vu que $\mathcal{O}$ est un voisinage, il contient un ouvert et donc une boule

$$B\big((a, b), r\big) = \{(v, w) \in V \times W \text{ tel que } \max\{\|v - a\|, \|w - b\|\} < r\}. \tag{12.88}$$

Évidemment l'ensemble $B(a, r) \times B(b, r)$ est dedans. □

12.3.2 Suites

Nous allons maintenant parler de suites dans $V \times W$. Nous noterons (v_n, w_n) la suite dans $V \times W$ dont l'élément numéro n est le couple (v_n, w_n) avec $v_n \in V$ et $w_n \in W$. La notions de convergence de suite découle de la définition de la norme via la définition usuelle 8.12. Il se fait que dans le cas des produits d'espaces, la convergence d'une suite est équivalente à la convergence des composantes. Plus précisément, nous avons le lemme suivant.

Lemme 12.46.
La suite (v_n, w_n) converge vers (v, w) dans $V \times W$ si et seulement les suites (v_n) et (w_n) convergent séparément vers v et w respectivement dans V et W.

Démonstration. Pour le sens direct, nous devons étudier le comportement de la norme de $(v_n, w_n) - (v, w)$ lorsque n devient grand. En vertu de la définition de la norme dans $V \times W$ nous avons

$$\big\|(v_n, w_n) - (v, w)\big\|_{V \times W} = \max\big\{\|v_n - v\|_V, \|w_n - w\|_W\big\}. \tag{12.89}$$

Soit $\varepsilon > 0$. Par définition de la convergence de la suite (v_n, w_n), il existe un $N \in \mathbb{N}$ tel que $n > N$ implique

$$\max\big\{\|v_n - v\|_V, \|w_n - w\|_W\big\} < \varepsilon, \tag{12.90}$$

et donc en particulier les deux inéquations

$$\|v_n - v\| < \varepsilon \tag{12.91a}$$
$$\|w_n - w\| < \varepsilon. \tag{12.91b}$$

De la première, il ressort que $(v_n) \to v$, et de la seconde que $(w_n) \to w$.

Pour le sens inverse, nous avons pour tout ε un N_1 tel que $\|v_n - v\|_V \leqslant \varepsilon$ pour tout $n > N_1$ et un N_2 tel que $\|w_n - w\|_W \leqslant \varepsilon$ pour tout $n > N_2$. Si nous posons $N = \max\{N_1, N_2\}$ nous avons les deux inégalités simultanément, et donc

$$\max\left\{\|v_n - v\|_V, \|w_n - w\|_W\right\} < \varepsilon, \tag{12.92}$$

ce qui signifie que la suite (v_n, w_n) converge vers (v, w) dans $V \times W$. □

Proposition 12.47 ([1]).
Soit un espace E muni d'un produit scalaire à valeurs dans $\mathbb{K}$ (si $\mathbb{K} = \mathbb{C}$ nous supposons le produit hermitien, mais ce n'est pas très important ici). Alors l'application

$$\begin{aligned} a\colon E \times E &\to \mathbb{K} \\ (x, y) &\mapsto \langle x, y\rangle \end{aligned} \tag{12.93}$$

est continue.

Démonstration. Nous ne disons pas que l'espace $V \times V$ est muni d'un produit scalaire. Mais en tout cas c'est un espace métrique, et $\mathbb{K}$ l'est aussi. Donc a est une application entre deux espaces métriques et elle sera continue si et seulement si elle est séquentiellement continue (proposition 7.749.10).

Soit donc une suite convergente dans $E \times E$, c'est-à-dire $(x_k, y_k) \xrightarrow{E\times E} (x, y)$. Nous devons démontrer que $\langle x_k, y_k\rangle \xrightarrow{\mathbb{R}} \langle x, y\rangle$. Les majorations usuelles donnent

$$\begin{aligned} \big|\langle x_k, y_k\rangle - \langle x, y\rangle\big| &\leqslant \big|\langle x_k, y_k\rangle - \langle x, y_k\rangle\big| + \big|\langle x, y_k\rangle - \langle x, y\rangle\big| && (12.94a)\\ &= \big|\langle x_k - x, y_k\rangle\big| + \big|\langle x, y_k - y\rangle\big|. && (12.94b) \end{aligned}$$

Nous savons du lemme 12.46 que les suites (x_k) et (y_k) sont séparément convergentes : $x_k \xrightarrow{E} x$ et $y_k \xrightarrow{E} y$. En utilisant l'inégalité de Cauchy-Schwarz 11.9 nous trouvons

$$\big|\langle x_k - x, y_k\rangle\big| \leqslant \|x_k - x\|\|y_k\|. \tag{12.95}$$

Nous avons $\|x_k - x\| \to 0$ et $\|y_k\| \to \|y\|$, et par la règle du produit de limites dans $\mathbb{R}$ nous avons que $\big|\langle x_k - x, y_k\rangle\big| \to 0$. □

Remarque 12.48.
Il faut remarquer que la norme (12.78) est une norme *par défaut*. C'est la norme qu'on met quand on ne sait pas quoi mettre. Or il y a au moins un cas d'espace produit dans lequel on sait très bien quelle norme prendre : les espaces $\mathbb{R}^m$. La norme qu'on met sur $\mathbb{R}^2$ est

$$\|(x, y)\| = \sqrt{x^2 + y^2}, \tag{12.96}$$

et non la norme « par défaut » de $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ qui serait

$$\|(x, y)\| = \max\{|x|, |y|\}. \tag{12.97}$$

Les théorèmes que nous avons donc démontré à propos de $V \times W$ ne sont donc pas immédiatement applicables au cas de $\mathbb{R}^2$.

Cette remarque est valables pour tous les espaces $\mathbb{R}^m$. À moins de mention contraire explicite, nous ne considérons jamais la norme par défaut (12.78) sur un espace $\mathbb{R}^m$.

Étant donné la remarque 12.48, nous ne savons pas comment calculer par exemple la fermeture du produit d'intervalle $]0,1,[\times[4,5[$. Il se fait que, dans $\mathbb{R}^m$, les fermetures de produits sont quand même les produits de fermetures.

Proposition 12.49.
Soit $A\subset\mathbb{R}^m$ et $B\subset\mathbb{R}^m$. Alors dans $\mathbb{R}^{m+n}$ nous avons $\overline{A\times B}=\bar{A}\times\bar{B}$.

La démonstration risque d'être longue ; nous ne la faisons pas ici.

12.3.3 Continuité du produit de matrices

Nous avons introduit des normes sur $\mathbb{M}(n,\mathbb{K})$, entre autres la norme opérateur de la définition 12.10. Qui dit norme dit topologie. Il advient alors la question évidente : est-ce que des opérations aussi élémentaires que le produit de matrices sont continues pour ces topologies ?

Une façon simple de répondre à cela est d'introduire sur $\mathbb{M}(n,\mathbb{K})$ une nouvelle norme très simple : celle de $\mathbb{K}^n$. C'est la topologie par composante. Pour cette topologie, il est simple de voir que le produit matriciel est continu parce que les éléments de AB sont des polynômes en les éléments de A B. Ensuite il suffit d'invoquer l'équivalence de toutes les normes (théorème 12.6).

Voyons comment montrer cela de façon plus directe (bien que le raisonnement précédent soit une démonstration qui devrait déjà avoir convaincu les plus sceptiques). La preuve suivante va donc s'amuser à bien préciser les topologies et caractérisations utilisées.

Lemme 12.50.
Si $\|.\|$ est une norme algébrique sur $\mathbb{M}(n,\mathbb{K})$ ($\mathbb{K}$ est $\mathbb{R}$ ou $\mathbb{C}$) alors l'application

$$\begin{aligned}p\colon\mathbb{M}(n,\mathbb{K})\times\mathbb{M}(n,\mathbb{K})&\to\mathbb{M}(n,\mathbb{K})\\(A,B)&\mapsto AB\end{aligned}\tag{12.98}$$

est continue.

Démonstration. L'espace $\mathbb{M}(n,\mathbb{K})\times\mathbb{M}(n,\mathbb{K})$ est métrique (définition 12.41), donc la caractérisation séquentielle de la continuité (proposition 9.14) s'applique. Nous considérons donc une suite (A_k,B_k) dans $\mathbb{M}(n,\mathbb{K})\times\mathbb{M}(n,\mathbb{K})$ convergente vers AB.

Nous savons que la topologie sur $\mathbb{M}(n,\mathbb{K})\times\mathbb{M}(n,\mathbb{K})$ est la topologie produit (lemme 12.42) et que celle-ci donne la convergence composante par composante dès que nous avons convergence d'une suite ; c'est la proposition 7.34. Nous avons donc $A_k\xrightarrow{\mathbb{M}(n,\mathbb{K})}A$ et $B_k\xrightarrow{\mathbb{M}(n,\mathbb{K})}B$.

Voilà pour le contexte. Maintenant, la preuve de la continuité. Nous effectuons les majorations suivantes :

$$\begin{aligned}\|p(A_k,B_K)-AB\|&\leqslant\|p(A_k,B_k)-p(A_k,B)\|+\|p(A_k,B)-AB\|&\text{(12.99a)}\\&=\|A_Kb_k-A_kB\|+\|A_kB-AB\|&\text{(12.99b)}\\&=\|A_k(B_k-B)\|+\|(A_k-A)B\|&\text{(12.99c)}\\&\leqslant\underbrace{\|A_k\|}_{\to\|A\|}\underbrace{\|B_k-B\|}_{\to0}+\underbrace{\|A_k-A\|}_{\to0}\|B\|.&\text{(12.99d)}\end{aligned}$$

□

12.4 Applications multilinéaires

Définition 12.51 (Application multilinéaire)**.**
*Une application $T:\mathbb{R}^{m_1}\times\ldots\times\mathbb{R}^{m_k}\to\mathbb{R}^p$ est dite k-**linéaire** si pour tout $X=(x_1,\ldots,x_k)$ dans $\mathbb{R}^{m_1}\times\ldots\times\mathbb{R}^{m_k}$ les applications $x_i\mapsto T(x_1,\ldots,x_i,\ldots,x_k)$ sont linéaires pour tout i dans*

$\{1,\dots,k\}$, *c'est-à-dire*

$$\begin{aligned} T(\ \cdot\ , x_2, \dots, x_i, \dots, x_k) &\in \mathcal{L}(\mathbb{R}^{m_1}, \mathbb{R}^p),\\ T(x_1, \ \cdot\ , \dots, x_i, \dots, x_k) &\in \mathcal{L}(\mathbb{R}^{m_2}, \mathbb{R}^p),\\ &\vdots\\ T(x_1, \dots, x_i, \dots, x_{k-1}, \ \cdot\ ) &\in \mathcal{L}(\mathbb{R}^{m_k}, \mathbb{R}^p). \end{aligned} \tag{12.100}$$

En particulier lorsque $k = 2$, nous parlons d'applications ***bilinéaires****. Vous pouvez deviner ce que sont les applications* tri*linéaire ou* quadri*linéaire.*

L'ensemble des applications k-linéaires de $\mathbb{R}^{m_1} \times \dots \times \mathbb{R}^{m_k}$ dans $\mathbb{R}^p$ est noté $\mathcal{L}(\mathbb{R}^{m_1} \times \dots \times \mathbb{R}^{m_k}, \mathbb{R}^p)$ ou $\mathcal{L}(\mathbb{R}^{m_1}, \dots, \mathbb{R}^{m_k}; \mathbb{R}^p)$.

Exemple 12.52
Soit A une matrice avec m lignes et n colonnes. L'application bilinéaire de $\mathbb{R}^m \times \mathbb{R}^n$ dans $\mathbb{R}$ associée à A est définie par

$$T_A(x, y) = x^T A y = \sum_{i,j} a_{i,j} x_i y_j, \qquad \forall x \in \mathbb{R}^m,\ y \in \mathbb{R}^n.$$

△

Nous énonçons la proposition suivante dans le cas d'espaces vectoriels normés [10] parce que nous allons l'utiliser dans ce cas, mais le cas particulier $E_i = \mathbb{R}^{m_i}$ et $F = \mathbb{R}^p$ est important.

Proposition 12.53.
Soient des espaces vectoriels normés E_i et F. Une application n-linéaire

$$T\colon E_1 \times \dots \times E_n \to F \tag{12.101}$$

est est continue si et seulement s'il existe un réel $L \geqslant 0$ tel que

$$\|T(x_1, \dots, x_n)\|_F \leqslant L \|x_1\|_{F_1} \cdots \|x_n\|_{F_n}, \qquad \forall x_i \in E_i. \tag{12.102}$$

Démonstration. Pour simplifier l'exposition nous nous limitons au cas $n = 2$ et nous notons $T(x, y) = x * y$

Supposons que l'inégalité (12.102) soit satisfaite.

$$\begin{aligned} \|x * y - x_0 * y_0\| &= \|(x - x_0) * y - x_0 * (y - y_0)\|\\ &\leqslant \|(x - x_0) * y\| + \|x_0 * (y - y_0)\|\\ &\leqslant L\|x - x_0\|\|y\| + L\|x_0\|\|y - y_0\|. \end{aligned} \tag{12.103}$$

Si $x \to x_0$ et $y \to y_0$ on voit que T est continue en passant à la limite aux deux côtés de l'inégalité (12.103).

Soit T continue en $(0, 0)$. Évidemment [11] $0 * 0 = 0$, donc il existe $\delta > 0$ tel que si $x \in B_{E_1}(0, \delta)$ et $y \in B_{E_2}(0, \delta)$ alors $\|x * y\| \leqslant 1$. En particulier si $(x, y) \in B_{E_1 \times E_2}(0, \delta)$ nous sommes dans ce cas. Soient maintenant $x \in E_1 \backslash \{0\}$ et $y \in E_2 \backslash \{0\}$

$$x * y = \left(\frac{\|x\|}{\delta} \frac{\delta x}{\|x\|}\right) * \left(\frac{\|y\|}{\delta} \frac{\delta y}{\|y\|}\right) = \frac{\|x\|\|y\|}{\delta^2} \left(\frac{\delta x}{\|x\|}\right) * \left(\frac{\delta y}{\|y\|}\right). \tag{12.104}$$

On remarque que $\delta x / \|x\|_m$ est dans la boule de rayon δ centrée en 0_m et que $\delta y / \|y\|_n$ est dans la boule de rayon δ centrée en 0_n. On conclut

$$x * y \leqslant \frac{\|x\|_m \|y\|_n}{\delta^2}.$$

Il faut prendre $L = 1/\delta^2$. □

10. Sans hypothèses sur la dimension.
11. Dans la formule suivante, les trois zéros sont les zéros de trois espaces différents.

La norme de T est alors définie comme la plus petite constante L qui fait fonctionner la proposition 12.53.

Définition 12.54.
La norme sur l'espace $\mathcal{L}(E_1 \times \cdots \times E_n, F)$ des applications k-linéaires et continues est

$$\|T\|_{E_1\times\ldots\times E_n} = \sup\{\|T(u_1,\ldots,u_k)\|_F \,|\, \|u_i\|_{E_i} \leqslant 1, i = 1,\ldots,k\}. \tag{12.105}$$

Nous avons donc automatiquement

$$\|T(u,v)\| \leqslant \|T\|\|u\|\|v\|. \tag{12.106}$$

Et nous notons que cette norme est uniquement définie pour les applications linéaires continues. Ce n'est pas très grave parce qu'alors nous définissons $\|T\| = \infty$ si T n'est pas continue. Cela pour retrouver le principe selon lequel on est continue si et seulement si on est borné.

Proposition 12.55.
On définit les fonctions

$$\begin{array}{rccc} \omega_g: & \mathcal{L}(\mathbb{R}^m \times \mathbb{R}^n, \mathbb{R}^p) & \to & \mathcal{L}(\mathbb{R}^m, \mathcal{L}(\mathbb{R}^n, \mathbb{R}^p)), \\ \omega_d: & \mathcal{L}(\mathbb{R}^m \times \mathbb{R}^n, \mathbb{R}^p) & \to & \mathcal{L}(\mathbb{R}^n, \mathcal{L}(\mathbb{R}^m, \mathbb{R}^p)), \end{array} \tag{12.107}$$

par

$$\omega_g(T)(x) = T(x, \ \cdot\ ), \qquad \forall x \in \mathbb{R}^m,$$

et

$$\omega_d(T)(y) = T(\ \cdot\ , y), \qquad \forall y \in \mathbb{R}^n.$$

Les fonctions ω_g et ω_d sont des isomorphismes qui préservent les normes.

12.5 Séries

Pour une définition plus générale de somme indexée par un ensemble infine, voir la définition 12.100.

Définition 12.56.
*Soit (a_k) une suite dans un espace vectoriel normé $(V, \|.\|)$. La suite des **sommes partielles** associée est la suite (s_k) définie par*

$$s_k = \sum_{i=0}^{k} a_i \tag{12.108}$$

*La **série** associée est la limite des sommes partielles*

$$\sum_{n=0}^{\infty} a_k = \lim_{k\to\infty} \sum_{k=0}^{n} a_k \tag{12.109}$$

si elle existe.

*Si une telle limite existe nous disons que $\sum_{k=0}^{\infty} a_k$ **converge** dans V. Si la limite de la suite des sommes partielles n'existe pas nous disons que la série **diverge**.*

Remarque 12.57.
Si la limite de la suite des sommes partielles n'existe pas dans V, alors elle peut parfois exister dans des extensions de V. Par exemple une série de rationnels convergeant vers $\sqrt{2}$ dans $\mathbb{R}$ ne converge pas dans $\mathbb{Q}$. Autre exemple : avec une bonne topologie sur $\bar{\mathbb{R}}$, une série peut ne pas converger dans $\mathbb{R}$ mais converger vers $\pm\infty$ dans $\bar{\mathbb{R}}$.

Dans le cas des espaces de fonctions, nous avons une norme importante : la norme uniforme définie par $\|f\|_\infty = \sup\{f(x)\}$ où le supremum est pris sur l'ensemble de définition de f.

Lemme 12.58.
Soit une suite (a_k) dans un espace métrique complet[12] *dont la série converge.*

(1) Pour tout N nous avons

$$\sum_{k=0}^{\infty} a_k = \sum_{k=0}^{N} a_k + \sum_{k=N+1}^{\infty} a_k. \tag{12.110}$$

(2) La suite des queues de série converge vers 0, c'est à dire que

$$\lim_{N\to\infty} \sum_{k=N}^{\infty} a_k = 0. \tag{12.111}$$

Démonstration. Voici un petit calcul :

$$\lim_{n\to\infty} \sum_{k=0}^{n} a_k = \lim_{n\to\infty} \big(\sum_{k=0}^{N} a_k + \sum_{k=N+1}^{n} a_k \big) \tag{12.112a}$$

$$= \lim_{n\to\infty} \sum_{k=0}^{N} a_k + \lim_{n\to\infty} \sum_{k=N+1}^{n} a_k \tag{12.112b}$$

$$= \sum_{k=0}^{N} a_k + \sum_{k=N+1}^{\infty} a_k. \tag{12.112c}$$

Justifications :

— Pour (12.112a). Pour chaque n, la somme est finie et nous pouvons la décomposer. Si vous voulez vraiment couper les cheveux en quatre, vous devez fixer un ϵ, et un n de telle sorte à avoir $n > N$, parce que N est fixé dans l'énoncé du lemme.

— Pour (12.112b). Nous sommes dans un cas $\lim_{n\to\infty}(u_n + v_n)$ où (u_n) est constante et où $(u_n + v_n)$ converge. Nous pouvons donc permuter limite et somme[13].

Voila que (1) est prouvé.

Nous écrivons $s_n = \sum_{k=0}^{n} a_k$; l'hypothèse est que la suite (s_n) est une suite convergente dans un espace métrique. Elle est donc de Cauchy par la proposition 9.27.

Soit $\epsilon > 0$. Il existe $N \in \mathbb{N}$ tel que pour tout $p, q > N$, nous ayons $\|s_p - s_q\| \leqslant \epsilon$. Soit $p > N$. Pour tout $n \geqslant 0$ nous avons

$$\epsilon > \|s_{p+n} - s_{p+1}\| = \| \sum_{k=p}^{p+n} a_k \|. \tag{12.113}$$

En prenant la limite $n \to \infty$ nous avons

$$\| \sum_{k=p}^{\infty} a_k \| \leqslant \epsilon. \tag{12.114}$$

Nous avons donc démontré qu'il existe N tel que si $p > N$, alors $\| \sum_{k=p}^{\infty} a_k \| \leqslant \epsilon$. Cela signifie exactement que $\lim_{n\to\infty} \sum_{k=n}^{\infty} a_k = 0$. □

12.5.1 Les trois types de convergence

Trois notions de convergence à ne pas confondre :

(1) La convergence absolue,

(2) la convergence normale. C'est la même que la convergence absolue, mais dans le cas particulier d'un espace de fonctions muni de la norme uniforme.

(3) la convergence uniforme.

12. Définition 9.22.
13. Pour rappel, le lemme 8.13 demande la convergence des deux suites pour fonctionner.

Voici les définitions.

Définition 12.59 (Convergence absolue)**.**
*Nous disons que la série $\sum_{n=0}^{\infty} a_n$ dans l'espace vectoriel normé V **converge absolument** si la série $\sum_{n=0}^{\infty} \|a_n\|$ converge dans $\mathbb{R}$.*

Définition 12.60 (Convergence normale)**.**
*Une série de fonctions $\sum_{n\in\mathbb{N}} u_n$ converge **normalement** si la série de nombres $\sum_n \|u_n\|_\infty$ converge. C'est-à-dire si la série converge absolument pour la norme $\|f\|_\infty$.*

Définition 12.61 (Convergence uniforme)**.**
*La somme $\sum_n f_n$ **converge uniformément** vers la fonction F si la suite des sommes partielles converge uniformément, c'est-à-dire si*

$$\lim_{N\to\infty} \| \sum_{n=1}^{N} f_n - F\|_\infty = 0. \tag{12.115}$$

Proposition 12.62.
Une série convergeant absolument dans un espace de Banach[14] *y converge au sens usuel.*

Démonstration. Soit (a_k) une suite dans un espace vectoriel normé complet dont la série converge absolument. Nous allons montrer que la suite des sommes partielles est de Cauchy. Cela suffira à montrer sa convergence par hypothèse de complétude.

Nous avons

$$\|s_p - s_l\| = \| \sum_{k=l+1}^{p} a_k\| \leqslant \sum_{k=l+1}^{p} \|a_k\| = \bar{s}_p - \bar{s}_l \tag{12.116}$$

où $\bar{s}_n = \sum_{k=0}^{n} \|a_k\|$ est la suite des sommes partielles de la série des normes (qui converge). Vu que la suite $(\bar{s}_n)$ converge dans $\mathbb{R}$, elle y est de Cauchy par la proposition 1.79. Donc il existe un N tel que $p, l > N$ implique

$$\|s_p - s_l\| = \bar{s}_p - \bar{s}_l \leqslant \epsilon. \tag{12.117}$$

Cela signifie que (s_n) est une suite de Cauchy et donc convergente. □

Exemple 12.63(Si l'espace n'est pas complet[1])
Dans un espace pas complet, il est possible de construire un série qui converge absolument sans converger au sens usuel.

Nous allons trouver dans $\mathbb{Q}$ une série qui converge simplement vers $\sqrt{2}$ (et donc ne converge pas dans $\mathbb{Q}$) mais absolument vers 4.

La base est que si $A, B \in \mathbb{Q}$ avec $A < B$ il est possible de résoudre

$$\begin{cases} r_1 + r_2 = A & \text{(12.118a)} \\ |r_1| + |r_2| = B & \text{(12.118b)} \end{cases}$$

pour $r_1, r_2 \in \mathbb{Q}$. Ce n'est pas très compliqué : la solution est $r_1 = (A + B)/2$ et $r_2 = (A - B)/2$.

Nous considérons l'espace $\mathbb{Q}$ qui n'est pas complet dans $\mathbb{R}$. Soit une série (a_k) dans $\mathbb{Q}$ qui converge vers $\sqrt{2}$ (convergence dans $\mathbb{R}$) nous nommons (s_k) la suite des ses sommes partielles. Soit aussi la suite (b_k) qui converge vers 4 (zéro serait encore plus facile mais bon, juste pour faire un peu de généralité).

Nous supposons que $a_k < b_k$ pour tout k et que les deux suites sont constituées de rationnels positifs. Nous nommons (s_k) et (s'_k) les sommes partielles. En particulier $s_n < s'_n$ et ce sont des suites croissantes.

Nous savons comment trouver $r_1, r_2 \in \mathbb{Q}$ tels que $r_1 + r_2 = s_1$ et $|r_1| + |r_2| = s'_1$. Par récurrence, si nous savons $r_1, \dots, r_k$ tels que

$$\begin{cases} r_1 + \dots + r_k = s_n & \text{(12.119a)} \\ |r_1| + \dots + |r_k| = s'_n & \text{(12.119b)} \end{cases}$$

14. Un espace vectoriel normé complet. Typiquement $\mathbb{R}$.

(avec, soit dit en passant $k = 2n$), alors nous pouvons trouver des rationnels r_{k+1}, r_{k+2} tels que

$$\begin{cases} r_1 + \ldots + r_k + r_{k+1} + r_{k+2} = s_{n+1} & (12.120a) \\ |r_1| + \ldots + |r_k| + |r_{k+1}| + |r_{k+2}| = s'_{n+1}, & (12.120b) \end{cases}$$

en effet il s'agit de résoudre

$$\begin{cases} r_{k+1} + r_{k+2} = s_{n+1} - r_1 - \ldots - r_k = s_{n+1} - s_n > 0 & (12.121a) \\ |r_{k+1}| + |r_{k+2}| = s'_{n+1} - |r_1| - \ldots - |r_k| = s'_{n+1} - s'_n > 0. & (12.121b) \end{cases}$$

Cela se résout comme plus haut. Au final nous pouvons construire une suite (r_k) dans $\mathbb{Q}$ telle que

$$\sum_{k=0}^{2n} r_k = s_n \tag{12.122}$$

et

$$\sum_{k=0}^{2n} |r_k| = s'_n. \tag{12.123}$$

△

Remarque 12.64.
Nous savons que sur les espaces vectoriels de dimension finie toutes les normes sont équivalentes (théorème 12.3). La notion de convergence de série ne dépend alors pas du choix de la norme. Il n'en est pas de même sur les espaces de dimension infinie. Une série peut converger pour une norme mais pas pour une autre.

Lorsque nous verrons la convergence de séries, nous verrons que la convergence normale est la convergence absolue pour la norme uniforme.

Lemme 12.65.
Si E et F sont des espaces de Banach[15]*, l'espace $\mathcal{L}(E, F)$ est également de Banach.*

Démonstration. Soit (u_n) une suite de Cauchy dans $\mathcal{L}(E, F)$; si $x \in E$ il existe N tel que si $l, m > N$ alors $\|u_l - u_m\| < \epsilon$, c'est-à-dire que pour tout $\|x\| = 1$ on a $\|u_l(x) - u_n(x)\| < \epsilon$. Cela signifie que $u_n(x)$ est une suite de Cauchy dans l'espace complet F. Cette suite converge et nous pouvons définir l'application $u\colon E \to F$ par

$$u(x) = \lim_{n\to\infty} u_n(x). \tag{12.124}$$

Il suffit maintenant de prouver que u est linéaire, ce qui est une conséquence directe de la linéarité de la limite :

$$u(\alpha x + \beta y) = \lim_{n\to\infty} \big(\alpha u_n(x) + \beta u_n(y)\big). \tag{12.125}$$

□

Proposition 12.66.
Si une série converge dans un espace complet, la norme de son terme général converge vers 0.

Démonstration. Soit une suite (a_n) dont la série converge vers s. Soit $\epsilon > 0$. La suite des sommes partielles (s_n) est de Cauchy et converge vers s : $s_n \to s$. En particulier il existe un N tel que si $n > N$, nous avons $\|s_n - s_{n-1}\| < \epsilon$. Pour de telles valeurs de n nous avons :

$$\|a_n\| = \|s_n - s_{n-1}\| \leqslant \epsilon. \tag{12.126}$$

Cela prouve que $a_n \to 0$. □

15. Je crois qu'il ne faut pas que E soit complet.

Dans le même ordre d'idée nous avons la convergence des queues de suites.

Lemme 12.67.
Si $\sum_{k=0}^{\infty} a_k$ est finie, alors

$$\lim_{n\to\infty} \sum_{k=n}^{\infty} a_k = 0. \tag{12.127}$$

Proposition 12.68.
Si la série converge alors la somme est associative : $\sum_k (a_k + b_k) = \sum_k a_k + \sum_k b_k$.

Démonstration. Associativité. Supposons que $\sum_k a_k$ et $\sum_k b_k$ convergent tous deux. Alors nous avons pour tout N :

$$\sum_{k=0}^{N} (a_k + b_k) = \sum_{k=0}^{N} a_k + \sum_{k=0}^{N} b_k. \tag{12.128}$$

Mais si deux limites existent alors la somme commute avec la limite. C'est le cas pour la limite $N \to \infty$, donc

$$\lim_{N\to\infty} \sum_{k=1}^{\infty} (a_k + b_k) = \lim_{N\to\infty} \sum_{k=0}^{\infty} a_k + \lim_{N\to\infty} \sum_{k=0}^{\infty} b_k. \tag{12.129}$$

□

12.6 Série réelle

La notion de série formalise le concept de somme infinie. L'absence de certaines propriétés de ces objets (problèmes de commutativité et même d'associativité) incite à la prudence et montre à quel point une définition précise est importante.

12.6.1 Critères de convergence absolue

Étant donné le terme général d'une série, il est souvent –dans les cas qui nous intéressent– difficile de déterminer la somme de la série. L'exemple de la série géométrique est particulier [16], puisqu'on connaît une formule pour chaque somme partielle, mais pour l'exemple des séries de Riemann il n'y a aucune formule simple pour un α général. D'où l'intérêt d'avoir des critères de convergence ne nécessitant aucune connaissance de l'éventuelle limite de la série.

Lemme 12.69 (Critère de comparaison)**.**
Soient $\sum_i a_i$ et $\sum_j b_j$ deux séries à termes positifs vérifiant

$$0 \leqslant a_i \leqslant b_i$$

alors

(1) si $\sum_i a_i$ diverge, alors $\sum_j b_j$ diverge,

(2) si $\sum_j b_j$ converge, alors $\sum_i a_i$ converge (absolument).

Proposition 12.70 (Critère d'équivalence[173])**.**
Soient $\sum_i a_i$ et $\sum_j b_j$ deux séries à termes positifs. Supposons l'existence de la limite (éventuellement infinie) suivante

$$\lim_{i\to\infty} \frac{a_i}{b_i} = \alpha \tag{12.130}$$

avec $\alpha \in \mathbb{R} \cup \{+\infty\}$. Alors

(1) si $\alpha \neq 0$ et $\alpha \neq \infty$, alors

$$\sum_i a_i \text{ converge} \iff \sum_j b_j \text{ converge}, \tag{12.131}$$

16. Voir l'exemple 12.75.

(2) si $\alpha = 0$ et $\sum_j b_j$ converge, alors $\sum_i a_i$ converge (absolument),

(3) si $\alpha = +\infty$ et $\sum_j b_j$ diverge, alors $\sum_i a_i$ diverge.

Démonstration. (1) Le fait que la suite a_n/b_n converge vers α signifie que tant sa limite supérieure que sa limite inférieure convergent vers α. En particulier la suite $\frac{a_n}{b_n}$ est bornée vers le haut et vers le bas. À partir d'un certain rang N, il existe M tel que

$$\frac{a_n}{b_n} < M \tag{12.132}$$

et il existe m tel que

$$\frac{a_n}{b_n} > m. \tag{12.133}$$

Nous avons donc $a_n < Mb_n$ et $a_n > mb_n$. La série de (a_n) converge donc si et seulement si la série de (b_n) converge.

(2) Si $\alpha = 0$, cela signifie que pour tout ϵ, il existe un rang tel que $\frac{a_n}{b_n} < \epsilon$, et donc tel que $a_n < \epsilon b_k$. La suite de (a_i) converge donc dès que la suite de (b_i) converge.

(3) Pour tout M, il existe un rang dans la suite à partir duquel on a $\frac{a_i}{b_i} > M$, et donc $a_k > Mb_k$. Si la série de (b_k) diverge, la série de (a_k) doit également diverger.

□

Proposition 12.71 (Critère du quotient[183])**.**
Soit $\sum_i a_i$ une série. Supposons l'existence de la limite (éventuellement infinie) suivante

$$\lim_{i\to\infty} \left|\frac{a_{i+1}}{a_i}\right| = L \tag{12.134}$$

avec $L \in \mathbb{R} \cup \{+\infty\}$. Alors

(1) si $L < 1$, la série converge absolument,

(2) si $L > 1$, la série diverge,

(3) si $L = 1$ le critère échoue : il existe des exemples de convergence et des exemples de divergence.

Démonstration. (1) Soit b tel que $L < b < 1$. À partir d'un certain rang K, on a $\left|\frac{a_{i+1}}{a_i}\right| < b$. En particulier,

$$|a_{K+1}| < b|a_K|, \tag{12.135}$$

et pour a_{K+2} nous avons

$$|a_{K+2}| < b|a_{K+1}| < b^2|a_K|. \tag{12.136}$$

Au final,

$$|a_{K+n}| < b^n|a_K|. \tag{12.137}$$

Étant donné que la série $\sum_{n\geqslant K} b^n$ converge (parce que $b < 1$), la queue de suite $\sum_{i\geqslant K} a_i$ converge, et par conséquent la suite au complet converge.

(2) Si $L > 1$, on a

$$|a_K| < |a_{K+1}| < |a_{K+2}| < \dots \tag{12.138}$$

Il est donc impossible que la suite (a_i) converge vers zéro. La série ne peut donc pas converger.

(3) Par exemple la suite harmonique $a_n = \frac{1}{n}$ vérifie $L = 1$, mais la série ne converge pas. Par contre, la suite $a_n = \frac{1}{n^2}$ vérifie aussi le critère avec $L = 1$ tandis que la série $\sum_n \frac{1}{n^2}$ converge.

□

Proposition 12.72 (Critère de la racine[173])**.**
Soit $\sum_i a_i$ une série, et considérons

$$\limsup_{i\to\infty} \sqrt[i]{|a_i|} = L$$

avec $L \in \mathbb{R} \cup \{+\infty\}$. Alors

(1) si $L < 1$, la série converge absolument,

(2) si $L > 1$, la série diverge,

(3) si $L = 1$ le critère échoue.

Démonstration. (1) Si $L < 1$, il existe un $r \in]0, 1[$ tel que $|a_n|^{1/n} < r$ pour les grands n. Dans ce cas, $|a_n| < r^n$, et la série converge absolument parce que la série $\sum_n r^n$ converge du fait que $r < 1$.

(2) Si $L > 1$, il existe un $r > 1$ tel que $|a_n|^{1/n} > r > 1$. Cela fait que $|a_n|$ prend des valeurs plus grandes que n pour une infinité de termes. Le terme général a_n ne peut donc pas être une suite convergente. Par conséquent la suite diverge au sens où elle ne converge pas.

□

12.6.2 Critères de convergence simple

Les critères de comparaison, d'équivalence, du quotient et de la racine sont des critères de convergence absolue. Pour conclure à une convergence simple qui n'est pas une convergence absolue, le critère d'Abel sera notre outil principal.

12.6.2.1 Critère d'Abel

Proposition 12.73 (Critère d'Abel)**.**
Soit la série $\sum_i c_i z_i$ avec

(1) (c_i) est une suite réelle décroissante qui tend vers zéro,

(2) (z_i) est une suite dans $\mathbb{C}$ dont la suite des sommes partielles est bornée dans $\mathbb{C}$, c'est-à-dire qu'il existe un $M > 0$ tel que pour tout n,

$$\left| \sum_{i=1}^{n} z_i \right| \leqslant M. \tag{12.139}$$

Alors la série $\sum_i c_i z_i$ est convergente.

Remarquons que ce critère ne donne pas de convergence absolue.

12.6.3 Quelques séries usuelles

Exemple 12.74(Série harmonique)
La **série harmonique** est

$$\sum_{i=k}^{\infty} \frac{1}{k} = +\infty. \tag{12.140}$$

△

Exemple 12.75(Série géométrique)
La **série géométrique** de raison $q \in \mathbb{C}$ est

$$\sum_{i=0}^{\infty} q^i. \tag{12.141}$$

Étudions la somme partielle $S_N = 1+q+q^2+\cdots+q^N$. Nous avons évidemment $S_N - qS_N = 1-q^{N+1}$ et donc

$$S_N = \sum_{n=0}^{N} q^n = \frac{1 - q^{N+1}}{1 - q}. \tag{12.142}$$

La limite $\lim_{N\to\infty} S_N$ existe si et seulement si $|q| \leqslant 1$ et dans ce cas nous avons

$$\sum_{n=0}^{\infty} q^n = \frac{1}{1-q}. \tag{12.143}$$

La convergence est absolue.

Si la somme commence en $n = 1$ au lieu de $n = 0$ alors

$$\sum_{n=1}^{\infty} q^n = \frac{1}{1-q} - 1 = \frac{q}{1-q}. \tag{12.144}$$

△

Un cas particulier de la formule (12.142) est le calcul de $\sum_{j=1}^{N} q^{-j}$ bien utile lorsque l'on joue avec des nombres binaires (voir l'exemple 35.12). Nous avons

$$\sum_{j=1}^{N} q^{-j} = \sum_{j=0}^{N} q^{-j} - 1 = \frac{1-q^{-N}}{q-1}. \tag{12.145}$$

Exemple 12.76(Série de Riemann)
Pour $\alpha \in \mathbb{R}$, la **série de Riemann**

$$\sum_{i=1}^{\infty} \frac{1}{i^\alpha} \tag{12.146}$$

converge (absolument, puisque réelle et positive) si et seulement si $\alpha > 1$, et diverge sinon. △

Exemple 12.77(Série exponentielle)
La série exponentielle est la série (pour $t \in \mathbb{R}$)

$$\exp(t) = \sum_{k=0}^{\infty} \frac{t^k}{k!}. \tag{12.147}$$

Nous montrons qu'elle converge pour tout $t \in \mathbb{R}$. Si $a_k = t^k/k!$ alors $\frac{a_{k+1}}{a_k} = \frac{t}{k}$ dont la limite $k \to \infty$ est zéro (quel que soit t). En vertu du critère du quotient 12.71 la série exponentielle converge (absolument) pour tout $t \in \mathbb{R}$.

Pour tout savoir de l'exponentielle et de ses variations, voir le thème 56. △

Exemple 12.78(Série arithmético-géométrique[184])
Une **suite arithmético-géométrique** est une suite vérifiant pour tout n la relation

$$u_{n+1} = au_n + b \tag{12.148}$$

avec a et b non nuls. Si elle possède une limite, cette dernière doit résoudre $l = al + b$, et donc être donnée par

$$l = \frac{b}{1-a}. \tag{12.149}$$

Comportement amusant : la limite peut exister pour certains valeurs de a_0 et pas pour d'autres. Mais elle ne dépend pas de a_0 parmi ceux pour lesquelles la limite existe.

Il n'est pas très compliqué de trouver le terme général de la suite en fonction de a et de b. Il suffit de considérer la suite $v_n = u_n - r$, et de remarquer que cette suite est géométrique :

$$v_{n+1} = av_n. \tag{12.150}$$

Par conséquent $v_n = a^n v_0$, ce qui donne pour la suite (u_n) la formule

$$u_n = a^n(u_0 - r) + r. \tag{12.151}$$

△

Lemme 12.79 ([185]).
Nous avons :

$$\sum_{k=1}^{N} \frac{1}{k(k+1)} = \frac{N}{N+1}. \tag{12.152}$$

et

$$\sum_{k=1}^{\infty} \frac{1}{k(k+1)} = 1. \tag{12.153}$$

Démonstration. Nous posons

$$f(n) = \sum_{k=1}^{n} \frac{1}{k(k+1)} \tag{12.154a}$$

$$g(n) = \frac{n}{n+1} \tag{12.154b}$$

et nous montrons par récurrence que $f(n) = g(n)$. Pour $n = 1$ nous avons $f(1) = g(1) = \frac{1}{2}$.

Nous supposons que $f(n) = g(n)$ et nous prouvons que $f(n+1) = g(n+1)$. Facile :

$$f(n+1) = f(n) + \frac{1}{(n+1)(n+2)} \tag{12.155a}$$

$$= \frac{n}{n+1} + \frac{1}{(n+1)(n+2)} \tag{12.155b}$$

$$= \frac{n(n+2)+1}{(n+1)(n+2)} \tag{12.155c}$$

$$= \frac{n^2+2n+1}{(n+1)(n+2)} \tag{12.155d}$$

$$= \frac{(n+1)^2}{(n+1)(n+2)} \tag{12.155e}$$

$$= \frac{n+1}{n+2} \tag{12.155f}$$

$$= g(n+1). \tag{12.155g}$$

En ce qui concerne la seconde formule, par définition [17]

$$\sum_{k=1}^{\infty} \frac{1}{k(k+1)} = \lim_{n\to\infty} \sum_{k=1}^{n} \frac{1}{k(k+1)} = \lim_{n\to\infty} \frac{n}{n+1} = 1. \tag{12.156}$$

□

12.6.4 Séries alternées

Théorème 12.80 (Critère des séries alternées[111]).
Si a est une suite réelle décroissante à limite nulle, alors

(1) La série $\sum_n (-1)^n a_n$ converge,

(2) si nous notons (S_n) la suite des sommes partielles, les sous-suites (S_{2n}) et (S_{2n+1}) sont adjacentes de limite $\sum_{n=1}^{\infty}(-1)^n a_n$.

(3) Si nous considérons le reste

$$R_n = \sum_{k=n+1}^{\infty} (-1)^k a_k, \tag{12.157}$$

nous avons

$$\operatorname{sgn}(R_n) = (-1)^{n+1} \tag{12.158a}$$

$$|R_n| \leqslant a_{n+1}. \tag{12.158b}$$

17. Définition d'une série, 12.56.

Démonstration. En termes de notations, nous allons écrire (S_n) la suite des sommes partielles de $\sum_{k=0}^{\infty}(-1)^k a_k$. Nous notons (S_{2n}) la suite des termes pairs de cette suite. C'est donc la suite $n \mapsto S_{2n}$. Nous divisons en plusieurs morceaux.

S_{2n} **est croissante** Nous avons simplement

$$S_{2n+2} - S_{2n} = a_{2n+2} - a_{2n+1} \leqslant 0. \tag{12.159}$$

(S_{2n+1}) **est décroissante** Même calcul.

Les suites (S_{2n}) **et** S_{2n+1} **sont adjacentes** Nous avons simplement

$$S_{2n+1} - S_{2n} = a_{2n+1} \to 0. \tag{12.160}$$

Nous concluons par le théorème des suites adjacentes 8.24 que les sous-suites des termes pairs et impairs sont convergentes et convergent vers la même limite.

C'est le moment d'utiliser la proposition 8.25 qui convaincra la lectrice que (S_n) converge vers la même limite, que nous notons S. Le théorème des suites adjacentes nous dit encore que

$$S_{2n+1} \leqslant S \leqslant S_{2n} \tag{12.161}$$

et donc que $R_{2n} = S - S_{2n} \leqslant 0$. Cela donne la majoration

$$|R_{2n}| = |S - S_n| = S_{2n} - S \leqslant S_{2n} - S_{2n+1} = a_{2n+1}. \tag{12.162}$$

Nous faisons le même genre de majorations pour R_{2n+1}. □

12.6.5 Moyenne de Cesaro

Définition 12.81.
Si $(a_n)_{n\in\mathbb{N}}$ est une suite dans $\mathbb{R}$ ou $\mathbb{C}$, alors sa ***moyenne de Cesaro*** *est la limite (si elle existe) de la suite*

$$c_n = \frac{1}{n}\sum_{k=1}^{n} a_k. \tag{12.163}$$

En un mot, c'est la limite des moyennes partielles.

Lemme 12.82.
Si la suite (a_n) converge vers la limite ℓ alors la suite admet une moyenne de Cesaro qui vaudra ℓ.

Démonstration. Soit $\epsilon > 0$ et $N \in \mathbb{N}$ tel que $|a_n - \ell| < \epsilon$ pour tout $n > N$. En remarquant que

$$\frac{1}{n}\sum_{k=1}^{n} k - \ell = \frac{1}{n}\sum_{k=1}^{n}(a_k - \ell), \tag{12.164}$$

nous avons

$$\Big|\frac{1}{n}\sum_{k=1}^{n} a_k - \ell\Big| \leqslant \Big|\frac{1}{n}\sum_{k=1}^{N}|a_k - \ell|\Big| + \Big|\frac{1}{n}\sum_{k=N+1}^{n}\underbrace{|a_k - \ell|}_{\leqslant\epsilon}\Big| \tag{12.165a}$$

$$\leqslant \epsilon + \frac{n-N-1}{n}\epsilon \tag{12.165b}$$

$$\leqslant 2\epsilon. \tag{12.165c}$$

Dans ce calcul nous avons redéfinit N de telle sorte que le premier terme soit inférieur à ϵ. □

12.6.6 Écriture décimale d'un nombre

12.83.
Soit $b \geqslant 2$ un entier qui sera la base dans laquelle nous allons écrire les nombres. Nous considérons l'ensemble $\mathbb{D}_b$ des suites dans $\{0, 1, \dots, b-1\}$ qui n'ont pas une queue de suite uniquement formée de $b-1$. Autrement dit une suite (c_n) est dans $\mathbb{D}_b$ lorsque pour tout N, il existe $k > N$ tel que $c_k \neq b-1$. Associé à cet ensemble nous considérons la fonction

$$\begin{aligned} \varphi_b \colon \mathbb{D}_b &\to [0,1[\\ c &\mapsto \sum_{n=1}^{\infty} \frac{c_n}{b^n}. \end{aligned} \tag{12.166}$$

Lemme 12.84.
La fonction φ_b est bien définie au sens où elle converge et prend ses valeurs dans $[0,1[$.

Démonstration. Tout se base sur la somme de la série géométrique (12.143) sous la forme

$$\sum_{k=0}^{\infty} \frac{1}{b^k} = \frac{b}{b-1}. \tag{12.167}$$

La somme (12.166) est donc majorée par $\sum_n \frac{b-1}{b^n}$ qui converge.

Pour prouver que l'image de φ_b est bien $[0,1[$, nous savons qu'au moins un des c_n (en fait une infinité) est plus petit que $b-1$, donc nous avons la majoration stricte [18]

$$\varphi_b(c) < \sum_{n=1}^{\infty} \frac{b-1}{b^n} = (b-1)\left(\sum_{n=1}^{\infty} \frac{1}{b^n} - 1\right) = 1 \tag{12.168}$$

□

Le fait d'introduire l'ensemble $\mathbb{D}$ au lieu de l'ensemble de toutes les suites est justifié par la proposition suivante. Elle explique pourquoi un nombre possède au maximum deux écritures décimales distinctes et que ces deux sont obligatoirement de la forme, par exemple en base 10 :

$$0.34599999999\ldots = 0.34600000\ldots \tag{12.169}$$

mais qu'un nombre commençant par 0.347 ne peut pas être égal. C'est pour cela que dans la définition de $\mathbb{D}_b$ nous avons exclu les suites qui terminent par tout des $b-1$.

Proposition 12.85.
Soit la fonction

$$\begin{aligned} \varphi \colon \{0, \dots, b-1\}^{\mathbb{N}} &\to [0,1[\\ x &\mapsto \sum_{n=1}^{\infty} \frac{x_n}{b^n}. \end{aligned} \tag{12.170}$$

Si $\varphi(x) = \varphi(y)$ et si n_0 est le plus petit entier tel que $x_{n_0} \neq y_{n_0}$ alors soit

$$x_{n_0} - y_{n_0} = 1 \tag{12.171}$$

et $x_n = 0$, $y_n = b-1$ pour tout $n > n_0$, soit le contraire : $y_{n_0} - x_{n_0} = 1$ avec $y_n = 0$ et $x_n = b-1$ pour tout $n > n_0$.

Démonstration. Nous nous basons sur la formule (facilement dérivable depuis (12.167)) suivante :

$$\sum_{k=n_0+1}^{\infty} \frac{1}{b^k} = \frac{1}{b^{n_0+1}} \frac{b}{b-1}. \tag{12.172}$$

18. Notez que la somme (12.166) commence à un tandis que la série géométrique (12.167) commence à zéro.

Nous avons

$$0 = \varphi(x) - \varphi(y) = \frac{x_{n_0} - y_{n_0}}{b^{n_0}} + \sum_{n=n_0+1}^{\infty} \frac{x_n - y_n}{b^n} \geqslant \frac{x_{n_0} - y_{n_0}}{b^{n_0}} - \sum_{n=n_0+1}^{\infty} \frac{b-1}{b^n} = \frac{x_{n_0} - y_{n_0} - 1}{b^{n_0}}. \tag{12.173}$$

Le dernier terme étant manifestement positif [19], il est nul et nous avons $x_{n_0} - y_{n_0} = 1$.

Nous avons donc maintenant

$$0 = \varphi(x) - \varphi(y) = \frac{1}{b^{n_0}} + \sum_{n=n_0+1}^{\infty} \frac{x_n - y_n}{b^n}. \tag{12.174}$$

Nous majorons la dernière somme de la façon suivante, en supposant que $|x_n - y_n| \neq b-1$ pour un certain $n > n_0$:

$$\left| \sum_{n=n_0+1}^{\infty} \frac{x_n - y_n}{b^n} \right| \leqslant \sum_{n=n_0+1}^{\infty} \frac{|x_n - y_n|}{b^n} < \sum_{n=n_0+1}^{\infty} \frac{b-1}{b^n} = \frac{1}{b^{n_0}}. \tag{12.175}$$

Étant donné cette inégalité stricte, l'équation (12.174) ne peut pas être correcte (valoir zéro). Nous avons donc $|x_n - b_n| = b-1$ pour tout $n > n_0$. Donc pour chaque $n > n_0$ nous avons soit $x_n = 0$ et $y_n = b-1$, soit $a_n = b-1$ et $b_n = 0$. Pour conclure il faut encore prouver que le choix doit être le même pour tout n.

Nous nous mettons dans le cas $x_{n_0} - y_{n_0} = 1$; dans ce cas nous avons bien l'égalité (12.174) sans petites nuances de signes. Nous écrivons

$$\sum_{n=n_0+1}^{\infty} \frac{x_n - y_n}{b^n} = (b-1) \sum_{n=n_0+1}^{\infty} \frac{(-1)^{s_n}}{b^n} \tag{12.176}$$

où s_n est pair ou impair suivant que $x_n = 0$, $y_n = b-1$ ou le contraire. Si un des $(-1)^{s_n}$ est pas -1 alors nous avons l'inégalité stricte

$$(b-1) \sum_{n=n_0+1}^{\infty} \frac{(-1)^{s_n}}{b^n} > (b-1) \sum_{n=n_0+1}^{\infty} \frac{-1}{b^n} = -\frac{1}{b^{n_0}}. \tag{12.177}$$

Dans ce cas il est impossible d'avoir $\varphi(x) - \varphi(y) = 0$. Nous en concluons que $(-1)^{s_n}$ est toujours -1, c'est-à-dire $x_n - y_n = 1 - b$, ce qui laisse comme seule possibilité $x_n = 0$ et $y_n = b-1$. □

Théorème 12.86.
L'application $\varphi_b \colon \mathbb{D}_b \to [0,1[$ *est bijective.*

Démonstration. En ce qui concerne l'injection, nous savons de la proposition 12.85 que si $\varphi_b(x) = \varphi_b(y)$ pour $x, y \in \{0, \dots, b-1\}^{\mathbb{N}}$, alors soit x soit y a une queue de suite composée uniquement de $b-1$, ce qui est exclu dans $\mathbb{D}_b$. Nous en déduisons que φ_b est bien injective en prenant $\mathbb{D}_b$ comme ensemble départ.

La partie lourde est la surjectivité. Nous prenons $x \in [0,1[$ et nous allons construire par récurrence une suite $a \in \mathbb{D}_b$ telle que $\varphi_b(a) = x$. Si il existe $a_1 \in \{0, \dots, b-1\}$ tel que $x = a_1/b$ alors nous prenons la suite $(a_1, 0, \dots,)$ et nous avons évidemment $\varphi(a) = x$. Sinon il existe $a_1 \in \{0, \dots, b-1\}$ tel que

$$\frac{a_1}{b} < x < \frac{a_1 + 1}{b} \tag{12.178}$$

parce que les autres possibilités pour x sont dans l'ensemble $[0,1[\backslash \{\frac{k}{b}\}_{k=0,\dots,b-1}$ que nous subdivisons en

$$]0, \frac{1}{b}[\cup]\frac{1}{b}, \frac{2}{b}[\cup \dots \cup]\frac{b-1}{b}, 1[. \tag{12.179}$$

19. C'est ici qu'intervient la subdivision entre le cas $x_{n_0} - y_{n_0} = 1$ ou le contraire. En effet si « ce dernier terme était manifestement *négatif* », il aurait fallu majorer avec de $1-b$ au lieu de $1-b$.

Pour la récurrence nous supposons avoir trouvé $a_1, \dots, a_n$ tels que

$$\sum_{k=1}^{n} \frac{a_k}{b^k} < x < \sum_{k=1}^{n-1} \frac{a_k}{b^k} + \frac{a_n + 1}{b^n}. \tag{12.180}$$

Encore une fois s'il existe $a_{n+1} \in \{0, \dots, b-1\}$ tel que $\sum_{k=1}^{n+1} \frac{a_k}{b^k} = x$ alors nous prenons ce a_{n+1} et nous complétons la suite avec des zéros pour avoir $\varphi(a) = x$. Sinon , pour simplifier les notations nous notons $x' = x - \sum_{k=1}^{n} \frac{a_k}{b^k}$ et nous avons

$$0 < x' < \frac{a_n + 1}{b^n}. \tag{12.181}$$

Le nombre x' est forcément dans un des intervalles

$$]\frac{s}{b^{n+1}}, \frac{s+1}{b^{n+1}}[\tag{12.182}$$

avec $s \in \{0, \dots, b-1\}$. Nous prenons le s correspondant à x' comme a_{n+1}. Dans ce cas nous avons

$$\sum_{k=1}^{n+1} \frac{a_k}{b^k} < x < \sum_{k=1}^{n+1} \frac{a_k}{b^k} + \frac{1}{b^{n+1}}. \tag{12.183}$$

Note : les deux inégalités sont strictes. La première parce que s'il y avait égalité, nous nous serions déjà arrêté en complétant avec des zéros. La seconde parce que

$$\sum_{k=n+2}^{\infty} \frac{a_k}{b^k} \leqslant \sum_{k=n+2}^{\infty} \frac{b-1}{b^k} = \frac{1}{b^{n+1}} \tag{12.184}$$

où l'égalité n'est possible que si $a_k = b - 1$ pour tout $k \geqslant n + 2$. Dans ce cas nous aurions eu

$$x = \sum_{k=1}^{n} \frac{a_k}{b^k} + \frac{a_{n+1} + 1}{b^{n+1}} \tag{12.185}$$

et nous aurions choisi le nombre a_{n+1} autrement et complété la suite par des zéros à partir de là. Notons que cela prouve au passage que la suite que nous sommes en train de construire est bien dans $\mathbb{D}_b$ parce qu'elle ne contiendra pas de queue de suite composée de $b - 1$.

Ceci termine la construction par récurrence de la suite $a \in \mathbb{D}_b$. Par construction nous avons pour tout $N \geqslant 1$,

$$\sum_{k=1}^{N} \frac{a_k}{b^k} \leqslant x \leqslant \sum_{k=1}^{N} \frac{a_k}{b^k} + \frac{1}{b^{N+1}}, \tag{12.186}$$

autrement dit : $\varphi_b(a_1, \dots, a_N) \in B(x, \frac{1}{b^{N+1}})$. Nous avons donc bien convergence

$$\lim_{N \to \infty} \varphi_b(a_1, \dots, a_N) = x \tag{12.187}$$

et l'application φ_b est surjective. □

L'application $\varphi_b^{-1} : [0, 1[\to \mathbb{D}_b$ est la **décomposition décimale** en base b des nombres de $[0, 1[$.

Tout cela nous permet de montrer entre autres que $\mathbb{R}$ n'est pas dénombrable. Vu qu'il y a une bijection entre $[0, 1[$ et $\mathbb{D}_b$, il suffit de prouver que $\mathbb{D}_b$ est non dénombrable. De plus il suffit de démontrer que $\mathbb{D}_b$ est non dénombrable pour un entier $b \geqslant 2$ donné.

Proposition 12.87 ([8]).
Il n'existe pas de surjection $\mathbb{N} \to \mathbb{D}_b$. Autrement dit $\mathbb{D}_b$ est non dénombrable.

Démonstration. Nous prenons $b \neq 2$ pour des raisons qui seront claires plus tard. Soit $f : \mathbb{N} \to \mathbb{D}_b$. Pour $i \in \mathbb{N}$ nous notons

$$f(n) = (c_i^{(n)})_{i\geqslant 1}, \tag{12.188}$$

et nous définissons la suite

$$c_k = \begin{cases} 0 & \text{si } c_k^{(k)} \neq 0 \\ 1 & \text{si } c_k^{(k)} = 0. \end{cases} \tag{12.189}$$

Cela est une suite dans $\mathbb{D}_b$ parce que $b \neq 2$ et que la suite ne contient que des 0 et des 1. Mais nous n'avons $f(n) = c$ pour aucun $n \in \mathbb{N}$ parce que nous avons $c_n \neq f(n)_n$.

Si $b = 2$ alors nous savons que $\mathbb{D}_2 \sim [0, 1[\sim \mathbb{D}_3$. Donc $\mathbb{D}_2 \sim \mathbb{D}_3$ et $\mathbb{D}_2$ ne peut pas plus être mis en bijection avec $\mathbb{N}$ que $\mathbb{D}_3$. □

Remarque 12.88.
La preuve ne fonctionne pas en base $b = 2$ parce que rien n'empêche d'avoir une queue de 1. Il y a alors toutefois moyen de se débrouiller en construisant la suite c de façon plus subtile. Si $b = 2$ et $n \in \mathbb{N}$ alors $f(n)$ est une suite de 0 et 1 contenant une infinité de 0 (parce qu'il n'y a pas de queue de suite ne contenant que des 1). Nous construisons alors c de la façon suivante : d'abord nous recopions $f(0)$ jusqu'à son *deuxième* zéro que nous changeons en 1 ; nommons n_0 le rang de ce deuxième zéro. Ensuite nous recopions les éléments de $f(1)$ à partir du rang $n_0 + 1$ jusqu'au second zéro que nous changeons en 1, etc.

Le fait de prendre le deuxième zéro nous garanti que la suite c n'aura pas de queue de suite ne contenant que des 1.

Notons que cette construction s'adapte à tout b ; il suffit de prendre le second terme qui n'est pas $b - 1$ et le remplacer par $b - 1$.

Corollaire 12.89.
L'ensemble $[0, 1[$ *n'est pas dénombrable.*

Démonstration. L'ensemble $[0, 1[$ est en bijection avec $\mathbb{D}_b$ que nous venons de prouver n'être pas dénombrable. □

12.6.7 Théorème de Banach-Steinhaus

Lemme 12.90 ([186])**.**
Soient des espaces vectoriels normés X et Y ainsi qu'une application linéaire bornée $T : X \to Y$. Pour tout $a \in X$ et pour tout $r > 0$ nous avons

$$\sup_{x\in B(a,r)} \|Tx\| \geqslant r\|T\| \tag{12.190}$$

Démonstration. Nous commençons avec $a = 0$. En utilisant la définition 12.10 de la norme opérateur,

$$\|T\| = \sup_{x\in X} \frac{\|Tx\|}{\|x\|} = \sup_{x\in B(0,r)} \frac{\|Tx\|}{\|x\|} \leqslant \frac{1}{r} \sup_{x\in B(0,r)} \|Tx\|. \tag{12.191}$$

Donc

$$\sup_{x\in B(0,r)} \|Tx\| \geqslant r\|T\|. \tag{12.192}$$

Il y a maintenant une astuce. Nous considérons un maximum :

$$\max\{\|T(a + x), \|T(a - x)\|\|\} \geqslant \frac{1}{2}\big(\|T(a + x)\| + \|T(a - x)\|\big) \tag{12.193a}$$
$$\geqslant \frac{1}{2}\big(\|T(a + x) - T(a + x)\|\big) \tag{12.193b}$$
$$= \frac{1}{2}\|T(2x)\| \tag{12.193c}$$
$$= \|Tx\|. \tag{12.193d}$$

Justifications :

— Pour (12.193a), la moyenne est plus petite que le maximum.

— Pour (12.193b), inégalité triangulaire : $\|\alpha-\beta\|\leqslant\|\alpha\|+\|\beta\|$.

Si maintenant $y\in B(a,r)$, nous avons $y=a+x$ pour un certain $x\in B(0,r)$, donc

$$\sup_{y\in B(a,r)}\|Ty\| = \sup_{x\in B(0,r)}\|T(a+x)\| \tag{12.194a}$$

$$= \sup_{x\in B(0,r)}\max\{\|T(a+x)\|,\|T(a-x)\|\} \tag{12.194b}$$

$$\geqslant \sup_{x\in B(0,r)}\|Tx\| \tag{12.194c}$$

$$\geqslant r\|T\|. \tag{12.194d}$$

Pour (12.194b), l'ensemble sur lequel nous prenons le supremum n'est pas modifié fondamentalement si nous regroupons les éléments deux à deux en prenant le maximum : les éléments exclus sont majorés. □

Théorème 12.91 (Théorème de Banach-Steinhaus[186])**.**
Soient un espace de Banach[20] X *et un espace vectoriel normé* Y*. Soit une famille* $\mathcal{F}$ *d'opérateurs linéaire bornés. Si pour tout* $x\in X$*,*

$$\sup_{T\in\mathcal{F}}\|Tx\|<\infty, \tag{12.195}$$

alors

$$\sup_{T\in\mathcal{F}}\|T\|<\infty. \tag{12.196}$$

Démonstration. Nous supposons que $\sup_{T\in\mathcal{F}}\|T\|=\infty$, de telle sorte que nous pouvons choisir une suite (T_n) dans $\mathcal{F}$ telle que $\|T_n\|\to\infty$. Cette suite peut diverger arbitrairement vite, et nous fixerons exactement cela plus tard.

Soit par ailleurs une suite $\alpha_n>0$ d'éléments petits et tels que $\alpha_n\to 0$. Nous supposons que $\sum_{n=0}^{\infty}\alpha_n<\infty$.

Si $a\in X$, le lemme 12.90 dit que

$$\sup_{x\in B(a,\alpha_n)}\|T_nx\|\geqslant\|T_n\|\alpha_n. \tag{12.197}$$

En posant $x_0=0$, nous construisons une suite (x_n) par récurrence en imposant

(1) $x_n\in B(x_{n=1},\alpha_n)$

(2) $\|T_nx_n\|\geqslant\|T_n\|\alpha_n$.

En utilisant une série télescopique et l'inégalité triangulaire $\|x_k-x_{k+1}\|\leqslant\alpha_n$ à chaque étage,

$$\|x_p-x_q\|\leqslant\sum_{k=p}^{q}\alpha_k\leqslant\sum_{k=p}^{\infty}\alpha_k. \tag{12.198}$$

Mais vu que la somme des α_n converge, la suite des queues de somme converge vers zéro[21] : $\lim_{p\to\infty}\sum_{k=p}^{\infty}\alpha_n=0$. Cela implique que (x_n) est une suite de Cauchy[22]. Vu que X est de Banach, la suite (x_n) a une limite dans X. Soit x cette limite.

Nous avons $\beta_n=\|x_n-x\|\to 0$. Il y aurait moyen de calculer β_n en fonction de α_n (surtout si nous avions donné une forme explicite à α_n), mais c'est sans importance ici. L'important est que c'est une suite qui tend vers zéro.

Nous avons

$$x\in B(x_n,\beta_n), \tag{12.199}$$

20. Définition 9.24.
21. Lemme 12.58(2).
22. Proposition 9.27.

et donc il existe $a_n \in B(0,\beta_n)$ tel que $x = x_n + a_n$. Avec cela, pour chaque n nous avons :

$$\begin{aligned}\|T_n x\| &= \|T_n(x_n + a_n)\| && (12.200a)\\ &\geqslant \|T_n x_n\| - \|T_n a_n\| && (12.200b)\\ &\geqslant \|T_n x_n\| - \|T_n\|\beta_n && (12.200c)\\ &\geqslant \|T_n\|\alpha_n - \|T_n\|\beta_n && (12.200d)\\ &= \|T_n\|(\alpha_n - \beta_n). && (12.200e)\end{aligned}$$

Pour 12.200c, nous avons utilisé $\|T_n a_n\| \leqslant \|T_n\|\beta_n$. En résumé,

$$\|T_n x\| \geqslant \|T_n\|(\alpha_n - \beta_n). \tag{12.201}$$

Il suffit de choisir $\|T_n\|$ suffisamment rapidement croissant pour que [23]

$$\|T_n\|(\alpha_n - \beta_n) \to \infty, \tag{12.202}$$

et nous avons $\|T_n x\| \to \infty$, qui est contraire aux hypothèses. □

Théorème 12.92 (Théorème de Banach-Steinhaus[43, 187])**.**
Soit E un espace de Banach[24] *et F un espace vectoriel normé. Nous considérons une partie $H \subset \mathcal{L}_c(E,F)$ (espace des fonctions linéaires continues). Alors H est uniformément borné si et seulement s'il est simplement borné.*

Démonstration. Si H est uniformément borné, il est borné ; pas besoin de rester longtemps sur ce sens de l'équivalence. Supposons donc que H soit borné. Pour chaque $k \in \mathbb{N}^*$ nous considérons l'ensemble

$$\Omega_k = \{x \in E \text{ tel que } \sup_{f\in H} \|f(x)\| > k\}. \tag{12.203}$$

Les Ω_k sont ouverts Soit $x_0 \in \Omega_k$; nous avons alors une fonction $f \in H$ telle que $\|f(x_0)\| > k$, et par continuité de f il existe $\rho > 0$ tel que $\|f(x)\| > k$ pour tout $x \in B(x_0,\rho)$. Par conséquent $B(x_0,\rho) \subset \Omega_k$ et Ω_k est ouvert par le théorème 7.4.

Les Ω_k ne sont pas tous denses dans E Nous supposons que les ensembles Ω_k soient tous dense dans E. Le théorème de Baire 9.87 nous indique que E est un espace de Baire (parce que de Banach) et donc que

$$\overline{\bigcap_{k\in\mathbb{N}} \Omega_k} = E. \tag{12.204}$$

En particulier l'intersection des Ω_k n'est pas vide. Soit $x_0 \in \bigcap_{k\in\mathbb{N}} \Omega_k$. Nous avons alors

$$\sup_{f\in H} \|f(x)\| = \infty, \tag{12.205}$$

ce qui est contraire à l'hypothèse. Donc les ouverts Ω_k ne sont pas tous denses dans E.

La majoration Il existe $k \geqslant 0$ tel que Ω_k ne soit pas dense dans E, et nous voulons prouver que $\{\|f\| \text{ tel que } f \in H\}$ est un ensemble borné. Soit donc $k \geqslant 0$ tel que Ω_k ne soit pas dense dans E ; il existe un $x_0 \in E$ et $\rho > 0$ tels que

$$B(x_0,\rho) \cap \Omega_k = \varnothing. \tag{12.206}$$

Si $x \in B(x_0,\rho)$ alors x n'est pas dans Ω_k et donc

$$\sup_{f\in H} \|f(x)\| \leqslant k. \tag{12.207}$$

23. Le point important ici est que α_n (et donc β_n) est choisit sans référence à $\|T_n\|$.
24. Définition 9.24.

Afin d'évaluer $\|f\|$ nous devons savoir ce qu'il se passe avec les vecteurs sur une boule autour de 0. Pour tout $x \in B(0,\rho)$ et pour tout $f \in H$, la linéarité de f donne

$$\|f(x)\| = \|f(x+x_0) - f(x_0)\| \leqslant \|f(x+x_0) + f(x_0)\| \leqslant 2k. \tag{12.208}$$

Par continuité nous avons alors $\|f(x)\| \leqslant 2k$ pour tout $x \in \overline{B(0,\rho)}$. Si maintenant $x \in F$ vérifie $\|x\| = 1$ nous avons

$$\|f(x)\| = \frac{1}{\rho}\|f(\rho x)\| \leqslant \frac{2k}{\rho}, \tag{12.209}$$

et donc $\|f\| \leqslant \frac{2k}{\rho}$, ce qui montre que $2k/\rho$ est un majorant de l'ensemble $\{\|f\| \text{ tel que } f \in H\}$.

□

Une application du théorème de Banach-Steinhaus est l'existence de fonctions continues et périodiques dont la série de Fourier ne converge pas. Ce sera l'objet de la proposition 29.18.

12.6.8 Convergence forte

Lorsque nous avons une suite d'opérateurs linéaires, nous pouvons considérer la convergence d'une suite pour la norme opérateur : $A_k \to A$ lorsque $\|A_k - A\| \to 0$.

Définition 12.93 ([188]).
*Soient un espace vectoriel E et un espace vectoriel normé V. Nous disons que la suite d'opérateur $T_k : E \to V$ **converge fortement** vers l'opérateur T si pour tout $x \in E$ nous avons*

$$\|T_k x - Tx\| \to 0. \tag{12.210}$$

Cette notion s'appelle *forte* par opposition à la convergence *faible* dont nous ne parlerons pas. Elle est cependant moins forte que la convergence en norme dont nous avons déjà parlé.

Proposition 12.94.
Soient des espaces vectoriels normés E et F et une suite d'opérateurs $T_k : E \to F$ convergeant vers T [25]. Alors cette suite converge également fortement.

Démonstration. Soit $x \in E$ que nous supposons non nul. Soit $\lambda \in \mathbb{C}$ tel que $x = \lambda y$ avec $\|y\| = 1$. Nous avons

$$\|T_k x - Tx\| = |\lambda|\|T_k y - Ty\| \leqslant |\lambda| \sup_{\|z\|=1} \|T_k z - Tz\| = |\lambda|\|T_k - T\| \to 0. \tag{12.211}$$

La dernière étape est la convergence en norme $T_k \to T$. □

Proposition 12.95.
Soient E et F, des espaces vectoriels normés de dimension finie. Soit une suite (A_n) d'applications linéaires $E \to F$. Si elle converge fortement vers A, alors elle converge en norme vers A.

Démonstration. En plusieurs coups.

Si une sous-suite converge Commençons par montrer que si (B_n) est une sous-suite de (A_n) qui converge vers B, alors $B = A$. Autrement dit, A est le seul candidat limite pour A_n.
Soit $\|x\| = 1$. Nous avons

$$\|B_n x - Bx\| \leqslant \|B_n - B\|\|x\| = \|B_n - B\|, \tag{12.212}$$

mais pour la sous-suite (B_n) nous avons supposé $\|B_n - B\| \to 0$. Donc $\|B_n x - Bx\| \to 0$, ce qui signifie que $B_n x \to Bx$. Mais par hypothèse, $B_n x \to Ax$. Par unicité de la limite, $Bx = Ax$ pour tout x de norme 1. Pour les autres x, c'est la linéarité qui conclu.

25. Sans précisions, ce sera toujours la convergence en norme.

Utilisation de deux gros résultats Par l'hypothèse de convergence, pour chaque x nous avons $\sup_n \|A_n x\| < \infty$. Le théorème de Banach-Steinhaus 12.91 nous indique alors que l'ensemble $\mathcal{F} = \{A_n\}_{n\in\mathbb{N}}$ est borné. Il existe donc $M > 0$ tel que $\|A_n\| < M$ pour tout n.
Nous utilisons à présent l'hypothèse de dimension finie en disant que l'espace des applications linéaires $E \to F$ est de dimension finie, de telle sorte que ses boules fermées soient compactes. Donc la suite (A_n) est contenue dans un compact.

Les sous-suite convergentes La suite (A_n) est contenue dans un compact. Toutes ses sous-suites sont dans ce compact et possèdent donc une sous-suite convergente (théorème 7.97). Toutes ces sous-sous-suites convergent nécessairement vers A par ce que nous avons dit dans la première étape de la preuve. Le lemme 7.35 nous dit alors que $A_n \to A$.

□

12.7 Sommes de familles infinies

12.7.1 Convergence commutative

Définition 12.96.
*Soit x_k une suite dans un espace vectoriel normé E. Nous disons que la suite **converge commutativement** vers $x \in E$ si $\lim_{n\to\infty} \|x_n - x\| = 0$ et si pour toute bijection $\tau : \mathbb{N} \to \mathbb{N}$ nous avons aussi*

$$\lim_{n\to\infty} \|x_{\tau(k)} - x\| = 0. \tag{12.213}$$

La notion de convergence commutative est surtout intéressante pour les séries. La somme

$$\sum_{k=0}^{\infty} x_k \tag{12.214}$$

converge commutativement vers x si $\lim_{N\to\infty} \|x - \sum_{k=0}^{N} x_k\| = 0$ et si pour toute bijection $\tau : \mathbb{N} \to \mathbb{N}$ nous avons

$$\lim_{N\to\infty} \|x - \sum_{k=0}^{N} x_{\tau(k)}\| = 0. \tag{12.215}$$

Nous démontrons maintenant qu'une série converge réelle commutativement si et seulement si elle converge absolument.

Proposition 12.97.
Soit $(a_i)_{i\in\mathbb{N}}$ une suite absolument convergente[26] *dans $\mathbb{C}$. Alors elle converge commutativement.*

Démonstration. Soit $\epsilon > 0$. Nous posons $\sum_{i=0}^{\infty} a_i = a$ et nous considérons N tel que

$$|\sum_{i=0}^{N} a_i - a| < \epsilon. \tag{12.216}$$

Étant donné que la série des $|a_i|$ converge, il existe N_1 tel que pour tout $p, q > N_1$ nous ayons $\sum_{i=p}^{q} |a_i| < \epsilon$. Nous considérons maintenant une bijection $\tau : \mathbb{N} \to \mathbb{N}$. Prouvons que la série $\sum_{i=0}^{\infty} |a_{\tau(i)}|$ converge. Nous choisissons M de telle sorte que pour tout $n > M$, $\tau(n) > N_1$. Si s_k est la somme partielle de la suite $(a_{\tau(i)})_{i\in\mathbb{N}}$ et si $M < p < q$ nous avons

$$|s_q - s_p| = |\sum_{i=p}^{q} a_{\tau(i)}| \leqslant \sum_{i=p}^{q} |a_{\tau(i)}| < \epsilon. \tag{12.217}$$

Cela montre que (s_k) est une suite de Cauchy. Elle est alors convergente et nous en déduisons que la série

$$\sum_{i=0}^{\infty} a_{\tau(i)} \tag{12.218}$$

26. Définition 12.59.

converge. Nous devons montrer à présent qu'elle converge vers la même limite que la somme « usuelle » $\lim_{N\to\infty}\sum_{i=0}^{N}a_i$.

Soit $n>\max\{M,N\}$. Alors

$$\sum_{k=0}^{n}a_{\tau(k)}-\sum_{k=0}^{n}a_k=\sum_{k=0}^{M}a_{\tau(k)}-\sum_{k=0}^{N}a_k+\underbrace{\sum_{M+1}^{n}a_{\tau(k)}}_{<\epsilon}-\underbrace{\sum_{k=N+1}^{n}a_k}_{<\epsilon}. \tag{12.219}$$

Par construction les deux derniers termes sont plus petits que ϵ parce que M et N sont les constantes de Cauchy pour les séries $\sum a_{\tau(i)}$ et $\sum a_i$. Afin de traiter les deux premiers termes, quitte à redéfinir M, nous supposons que $\{1,\ldots,N\}\subset\tau\{1,\ldots,M\}$; par conséquent tous les a_i avec $i<N$ sont atteints par les $a_{\tau(i)}$ avec $i<M$. Dans ce cas, les termes qui restent dans la différence

$$\sum_{k=0}a_{\tau(k)}-\sum_{k=0}^{N}a_k \tag{12.220}$$

sont des a_k avec $k>N$. Cette différence est donc en valeur absolue plus petite que ϵ, et nous avons en fin de compte que

$$\left|\sum_{k=0}^{n}a_{\tau(k)}-\sum_{k=0}^{n}a_k\right|<\epsilon. \tag{12.221}$$

□

Proposition 12.98.
Soit $\sum_{k=0}^{\infty}a_k$ une série réelle qui converge mais qui ne converge pas absolument. Alors pour tout $b\in\mathbb{R}$, il existe une bijection $\tau\colon\mathbb{N}\to\mathbb{N}$ telle que $\sum_{i=0}^{\infty}a_{\tau(i)}=b$.

Pour une preuve, voir chez Gilles Dubois.

Les propositions 12.97 et 12.98 disent entre autres qu'une série dans $\mathbb{C}$ est commutativement sommable si et seulement si elle est absolument sommable.

Soit $(a_i)_{i\in I}$ une famille de nombres complexes indexée par un ensemble I quelconque. Nous allons nous intéresser à la somme $\sum_{i\in I}a_i$.

Soit $\{a_i\}_{i\in I}$ des nombres positifs. Nous définissons la somme

$$\sum_{i\in I}a_i=\sup_{J\text{ fini}}\sum_{j\in J}a_j. \tag{12.222}$$

Notons que cela est une définition qui ne fonctionne bien que pour les sommes de nombres positifs. Si $a_i=(-1)^i$, alors selon la définition nous aurions $\sum_i(-1)^i=\infty$. Nous ne voulons évidemment pas un tel résultat.

Dans le cas de familles de nombres réels positifs, nous avons une première définition de la somme.

Définition 12.99.
Soit $(a_i)_{i\in I}$ une famille de nombres réels positifs indexés par un ensemble quelconque I. Nous définissons

$$\sum_{i\in I}a_i=\sup_{J\text{ fini dans }I}\sum_{j\in J}a_j. \tag{12.223}$$

Définition 12.100.
*Si $\{v_i\}_{i\in I}$ est une famille de vecteurs dans un espace vectoriel normé indexée par un ensemble quelconque I. Nous disons que cette famille est **sommable** de somme v si pour tout $\epsilon>0$, il existe un J_0 fini dans I tel que pour tout ensemble fini K tel que $J_0\subset K$ nous avons*

$$\|\sum_{j\in K}v_j-v\|<\epsilon. \tag{12.224}$$

Notons que cette définition implique la convergence commutative.

Exemple 12.101
La suite $a_i = (-1)^i$ n'est pas sommable parce que quel que soit J_0 fini dans $\mathbb{N}$, nous pouvons trouver J fini contenant J_0 tel que $\sum_{j\in J}(-1)^j > 10$. Pour cela il suffit d'ajouter à J_0 suffisamment de termes pairs. De la même façon en ajoutant des termes impairs, on peut obtenir $\sum_{j\in J'}(-1)^i < -10$. △

Exemple 12.102
De temps en temps, la somme peut sortir d'un espace. Si nous considérons l'espace des polynômes $[0,1] \to \mathbb{R}$ muni de la norme uniforme, la somme de l'ensemble

$$\{1, -1, \pm\frac{x^n}{n!}\}_{n\in\mathbb{N}} \tag{12.225}$$

est zéro.

Par contre la somme de l'ensemble $\{1, \frac{x^n}{n!}\}_{n\in\mathbb{N}}$ est l'exponentielle qui n'est pas un polynôme. △

Exemple 12.103
Au sens de la définition 12.100 la famille

$$\frac{(-1)^n}{n} \tag{12.226}$$

n'est pas sommable. En effet la somme des termes pairs est ∞ alors que la somme des termes impairs est $-\infty$. Quel que soit $J_0 \in \mathbb{N}$, nous pouvons concocter, en ajoutant des termes pairs, un J avec $J_0 \subset J$ tel que $\sum_{j\in J}(-1)^j/j$ soit arbitrairement grand. En ajoutant des termes négatifs, nous pouvons également rendre $\sum_{j\in J}(-1)^j/j$ arbitrairement petit. △

Proposition 12.104.
Si (a_{ij}) est une famille de nombres positifs indexés par $\mathbb{N}\times\mathbb{N}$ alors

$$\sum_{(i,j)\in\mathbb{N}^2} a_{ij} = \sum_{i=1}^{\infty}\Big(\sum_{j=1}^{\infty} a_{ij}\Big) \tag{12.227}$$

où la somme de gauche est celle de la définition 12.99.

Démonstration. Nous considérons $J_{m,n} = \{0,\dots,m\}\times\{0,\dots,n\}$ et nous avons pour tout m et n :

$$\sum_{(i,j)\in\mathbb{N}^2} a_{ij} \geqslant \sum_{(i,j)\in J_{m,n}} a_{ij} = \sum_{i=1}^{m}\Big(\sum_{j=1}^{n} a_{ij}\Big). \tag{12.228}$$

Si nous fixons m et que nous prenons la limite $n \to \infty$ (qui commute avec la somme finie sur i) nous trouvons

$$\sum_{(i,j)\in\mathbb{N}^2} a_{ij} \geqslant= \sum_{i=1}^{m}\Big(\sum_{j=1}^{\infty} a_{ij}\Big). \tag{12.229}$$

Cela étant valable pour tout m, c'est encore valable à la limite $m \to \infty$ et donc

$$\sum_{(i,j)\in\mathbb{N}^2} a_{ij} \geqslant \sum_{i=1}^{\infty}\Big(\sum_{j=1}^{\infty} a_{ij}\Big). \tag{12.230}$$

Pour l'inégalité inverse, il faut remarquer que si J est fini dans $\mathbb{N}^2$, il est forcément contenu dans $J_{m,n}$ pour m et n assez grand. Alors

$$\sum_{(i,j)\in J} a_{ij} \leqslant \sum_{(i,j)\in J_{m,n}} a_{ij} = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij} \leqslant \sum_{i=1}^{\infty}\Big(\sum_{j=1}^{\infty} a_{ij}\Big). \tag{12.231}$$

Cette inégalité étant valable pour tout ensemble fini $J \subset \mathbb{N}^2$, elle reste valable pour le supremum. □

La définition générale de la somme 12.100 est compatible avec la définition usuelle dans les cas où cette dernière s'applique.

Proposition 12.105 (commutative sommabilité)**.**
Soit I un ensemble dénombrable et une bijection $\tau: \mathbb{N} \to I$. Soit $(a_i)_{i\in I}$ une famille dans un espace vectoriel normé. Si $\sum_{i\in I} a_i$ existe, alors il est donné par

$$\sum_{i\in I} a_i = \lim_{N\to\infty} \sum_{k=0}^{N} a_{\tau(k)}. \tag{12.232}$$

Démonstration. Nous posons $a = \sum_{i\in I} a_i$. Soit $\epsilon > 0$ et J_0 comme dans la définition. Nous choisissons

$$N > \max_{j\in J_0}\{\tau^{-1}(j)\}. \tag{12.233}$$

En tant que sommes sur des ensembles finis, nous avons l'égalité

$$\sum_{k=0}^{N} a_{\tau(k)} = \sum_{j\in J_0} a_j \tag{12.234}$$

où J est un sous-ensemble de I contenant J_0. Soit J fini dans I tel que $J_0 \subset J$. Nous avons alors

$$\| \sum_{k=0}^{N} a_{\tau(k)} - a\| = \| \sum_{j\in J} a_j - a\| < \epsilon. \tag{12.235}$$

Nous avons prouvé que pour tout ϵ, il existe N tel que $n > N$ implique $\| \sum_{k=0}^{n} a_{\tau(k)} - a\| < \epsilon$. □

La réciproque n'est pas vraie. Même en supposant que $\lim_{N\to\infty} \sum_{n=0}^{N} a_n$ existe, il n'est pas forcé que $\sum_{n\in\mathbb{N}} a_n$ existe. Cela est une conséquence de l'exemple 12.103.

Corollaire 12.106.
Nous pouvons permuter une somme dénombrable et une fonction linéaire continue. C'est-à-dire que si f est une fonction linéaire continue sur l'espace vectoriel normé E et $(a_i)_{i\in I}$ une famille sommable dans E alors

$$f\left(\sum_{i\in I} a_i\right) = \sum_{i\in I} f(a_i). \tag{12.236}$$

Problèmes et choses à faire

À mon avis, ce corollaire est faux parce qu'il manque l'hypothèse que la famille $f(a_i)$ est sommable. Voir la proposition 12.108.

Démonstration. En utilisant une bijection τ entre I et $\mathbb{N}$ avec la proposition 12.105 ainsi que le résultat connu à propos des sommes sur $\mathbb{N}$, nous avons

$$f\left(\sum_{i\in I} a_i\right) = f\left(\sum_{k=0}^{\infty} a_{\tau(k)}\right) \tag{12.237a}$$

$$= \sum_{k=0}^{\infty} f(a_{\tau(k)}) \tag{12.237b}$$

$$= \sum_{i\in I} f(a_i). \tag{12.237c}$$

Notons que le passage à (12.237b) n'est pas du tout une trivialité à deux francs cinquante. Il s'agit d'écrire la somme comme la limite des sommes partielles, et de permuter f avec la limite en invoquant la continuité, puis de permuter f avec la somme partielle en invoquant sa linéarité.

Ah, tiens et tant qu'on y est-à-dire qu'il y a des choses évidentes qui ne le sont pas, oui, il existe des applications linéaires non continues, voir le thème 21. □

La proposition suivante nous enseigne que les sommes infinies peuvent être manipulée de façon usuelle.

Proposition 12.107.
Soit I un ensemble dénombrable. Soient $(a_i)_{i\in I}$ et $(b_i)_{i\in I}$, deux familles de réels positifs telles que $a_i < b_i$ et telles que (b_i) est sommable. Alors (a_i) est sommable.

Si $(a_i)_{i\in I}$ est une famille de complexes telle que $(|a_i|)$ est sommable, alors (a_i) est sommable.

Proposition 12.108 ([1])**.**
Soit un espace vectoriel normé E et une famille sommable[27] *$\{v_i\}_{i\in I}$ d'éléments de E. Soit $f\colon E \to \mathbb{C}$ une application sur laquelle nous supposons*

(1) f est linéaire et continue ;

(2) la partie $\{f(v_i)_{i\in I}\}$ est sommable.

Alors nous pouvons permuter la somme et f :

$$f\big(\sum_{i\in I} v_i\big) = \sum_{i\in I} f(v_i). \tag{12.238}$$

Démonstration. Soit $\epsilon > 0$; vu que les familles $\{v_i\}_{i\in I}$ et $\{f(v_i)\}_{i\in I}$ sont sommables, nous pouvons considérer les parties finies J_1 et J_2 de I telles que

$$\Big\| \sum_{j\in J_1} v_j - \sum_{i\in I} v_i \Big\| \leqslant \epsilon \tag{12.239}$$

et

$$\Big\| \sum_{j\in J_2} f(v_j) - \sum_{i\in I} f(v_i) \Big\| \leqslant \epsilon \tag{12.240}$$

Ensuite nous posons $J = J_1 \cup J_2$. Avec cela nous calculons un peu avec les majorations usuelles :

$$\|f(\sum_{i\in I} v_i) - \sum_{i\in I} f(v_i)\| \leqslant \|f(\sum_{i\in I} v_i) - f(\sum_{j\in J} v_j)\| + \|f(\sum_{j\in J} v_j) - \sum_{i} \in I f(v_i)\|. \tag{12.241}$$

Le second terme est majoré par ϵ, tandis que le premier, en utilisant la linéarité de f possède la majoration

$$\|f(\sum_{i\in I} v_i) - f(\sum_{j\in J} v_j)\| = \|f(\sum_{i\in I} v_i - \sum_{j\in J} v_j)\| \leqslant \|f\| \|\sum_{i\in I} v_i - \sum_{j\in J} v_j\| \leqslant \epsilon\|f\|. \tag{12.242}$$

Donc pour tout $\epsilon > 0$ nous avons

$$\|f(\sum_{i\in I} v_i) - \sum_{i\in I} f(v_i)\| \leqslant \epsilon(1 + \|f\|). \tag{12.243}$$

D'où l'égalité (12.238). □

12.8 Produit tensoriel d'espaces vectoriels

Si vous êtes pressés, vous pouvez aller lire la définition 12.118 de produit tensoriel d'espaces vectoriels. Mais si vous étiez vraiment pressés, vous ne seriez pas en train de lire des choses sur le produit tensoriel (il vous suffit de croire que $x \otimes y$ n'est finalement que la concatenation de x et y).

Définition 12.109.
*Soient un espace vectoriel V et un sous-espace N. Le **quotient** de V par N, noté V/N est l'ensemble des classes d'équivalence pour la relation $x \sim y$ si et seulement si $x - y \in N$.*

27. Définition 12.100.

Proposition 12.110.
Soient un espace vectoriel V et un sous-espace vectoriel N de V. Les définitions

(1) $[v] + [w] = [v + w]$

(2) $\lambda[v] = [\lambda v]$

ont un sens et définissent une structure d'espace vectoriel sur V/N.

Démonstration. Un élément général de la classe $[v]$ est de la forme $v + n$ avec $n \in N$. Le calcul suivant montre que la somme fonctionne :

$$[v + n_1] + [w + n_2] = [v + w + n_1 + n_2] = [v + w] \tag{12.244}$$

parce que $n_1 + n_2 \in N$. De même,

$$\lambda[v + n] = [\lambda v + \lambda n] = [\lambda v] \tag{12.245}$$

toujours parce que $\lambda n \in N$.

Notons que nous avons utilisé de façon on ne peut plus cruciale le fait que N soit un sous-espace vectoriel. □

Proposition 12.111.
Si $\{e_i\}$ est une base de V et si N est un sous-espace de V, alors $\{[e_i]\}$ est une partie génératrice de V/N.

Démonstration. Si $x = \sum_k x_k e_k$, alors $[x] = \sum_k x_k [e_k]$, donc oui. □

12.8.1 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 12.112 ([189])**.**
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.*

Proposition 12.113 ([190])**.**
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) $\dim(M_1) + \dim(M_2) \geqslant \dim(V)$.

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

$$\sum_i a_i e_i + \sum_\alpha b_\alpha f_\alpha. \tag{12.246}$$

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

$$\sum_i a_i e_i = 0 \tag{12.247}$$

et

$$\sum_\alpha b_\alpha f_\alpha = 0. \tag{12.248}$$

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 $\dim(M_1) + \dim(M_2) \geqslant \dim(V)$ éléments. La proposition 4.16(2) 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). □

La proposition suivante est une version plus « pragmatique » de la proposition 4.115.

Proposition 12.114 ([190]).
Soient un espace euclidien[28] *de dimension finie V ainsi qu'un sous-espace M. Nous posons*

$$M^\perp = \{x \in V \text{ tel que } x \cdot y = 0 \forall y \in M\}. \tag{12.249}$$

Alors $M \oplus M^\perp = V$.

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

$$\begin{aligned} f\colon V &\to \mathbb{R}^k \\ x &\mapsto (x \cdot b_1, \dots, x \cdot b_k). \end{aligned} \tag{12.250}$$

Nous avons que $M^\perp = \ker(f)$. Le théorème du rang 4.39 nous indique que

$$\dim(V) = \dim\big(\ker(f)\big) + \dim\big(\text{Image}(f)\big) \leqslant \dim(M^\perp) + k = \dim(M^\perp) + \dim(M). \tag{12.251}$$

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

$$\dim(M) + \dim(M^\perp) \geqslant \dim(V), \tag{12.252}$$

et la proposition 12.113 nous permet de conclure que $M \oplus M^\perp = V$. □

12.8.2 Les produits tensoriels

Nous allons procéder en deux temps. D'abord nous allons définir ce qu'est *un* produit tensoriel entre deux espaces vectoriels V et W, et nous allons montrer que tous les produits tensoriels possibles sont isomorphes. Ensuite nous allons montrer qu'un produit tensoriel existe en en construisant un. Voir la proposition 12.120.

Définition 12.115 ([191]).
*Soient deux espaces vectoriels V et W. Un **produit tensoriel** de V et W est un couple (T, h) où T est un espace vectoriel et $h\colon V \oplus W \to T$ est une application*

(1) bilinéaire[29]

(2) surjective

(3) telle que pour tout espace vectoriel U et toute applications bilinéaire $f\colon V \oplus W \to U$, il existe une application linéaire $g\colon T \to U$ telle que $f = g \circ h$.

*La propriété (3) est appelée **propriété universelle** du produit tensoriel.*

Définition 12.116.
*Un **morphisme** entre (T, h) et (T', h') est une application linéaire $\psi\colon T \to T'$ telle que $h' = \psi \circ h$.*

*Nous parlons d'**isomorphisme** si ψ a un inverse qui est également un morphisme.*

28. Qui possède un produit scalaire, définition 11.7.
29. Définition 11.1.

Proposition 12.117 ([191]).
Si V et W sont des espaces vectoriels, tous les produits tensoriels entre V et W sont isomorphes entre eux au sens de la définition 12.116.

Plus précisément, si (T,h) et (T',h') sont deux produits tensoriels de V et W, alors

(1) il existe une unique unique application linéaire $g\colon T\to T'$ telle que $h'=g\circ h$,

(2) cette application g est inversible.

En particulier, l'application g est un isomorphisme d'espaces vectoriels.

Démonstration. Soient deux produits tensoriels (T,h) et (T',h').

Existence L'application $h'\colon V\oplus W\to T'$ est bilinéaire, et (T,h) est un produit tensoriel. Donc il existe $g\colon T\to T'$ tel que $h'=g\circ h$. De même, il existe une application $g'\colon T'\to T$ telle que $h=g'\circ h$.

Unicité En ce qui concerne l'unicité, vu que $h\colon V\oplus W\to T$ est surjective, la relation $h'=g\circ h$ prescrit les valeurs de g sur tous les éléments de T.

Inversible Ces deux applications g et g' vérifient $h'=gg'h$ et $h=g'gh$, et de plus $h\colon V\oplus W\to T$ est surjective. Soient $t\in T$ et $x\in V\oplus W$ tel que $t=h(x)$. Nous avons $h(x)=g'gh(x)$. C'est-à-dire $t=(g'\circ g)(t)$. De même dans l'autre sens, il existe $x'\in V\oplus W$ tel que $t=h'(x')$. En appliquant l'égalité $h'=gg'h'$ à x', nous trouvons $t=(g\circ g')(t)$.

Tout cela pour dire que $g'=g^{-1}$. Cette application g est donc un isomorphisme de produits tensoriels entre (T,h) et (T',h').

Au final, l'application $g\colon T\to T'$ étant linéaire et inversible, elle est un isomorphisme d'espaces vectoriels. □

Tout cela est fort bien : nous avons unicité à isomorphisme près du produit tensoriel d'espaces vectoriels. Mais nous n'avons pas encore de certitudes à propos de l'existence d'un couple (T,h) vérifiant les propriétés demandées pour être un produit tensoriel.

Nous allons maintenant construire un produit tensoriel.

12.8.3 Le produit tensoriel

C'est le moment pour vous de relire la définition 4.22 d'espace vectoriel librement engendré, et surtout le lemme 4.23 qui en donne une base.

Définition 12.118 ([191]).
Soient deux espaces vectoriels V et W sur le corps commutatif[30] $\mathbb{K}$. *Dans $F_{\mathbb{K}}(V\times W)$ nous considérons les sous-espaces suivants :*

$$A_1=\{\delta_{(v_1,w)}+\delta_{(v_2,w)}-\delta_{(v_1+v_2,w)}\text{ tel que }v_1,v_2\in V,w\in W\} \tag{12.253a}$$
$$A_2=\{\delta_{(v,w_1)}+\delta_{(v,w_2)}-\delta_{(v,w_1+w_2)}\text{ tel que }v\in V,w_1,w_2\in W\} \tag{12.253b}$$
$$A_3=\{\lambda\delta_{v,w}-\delta_{(\lambda v,w)}\text{ tel que }v\in V,w\in W,\lambda\in\mathbb{K}\} \tag{12.253c}$$
$$A_4=\{\lambda\delta_{v,w}-\delta_{(v,\lambda w)}\text{ tel que }v\in V,w\in W,\lambda\in\mathbb{K}\}. \tag{12.253d}$$

Nous considérons alors $N=\operatorname{Span}(A_1,A_2,A_3,A_4)$ et le quotient

$$V\otimes_{\mathbb{K}}W=F_{\mathbb{K}}(V\times W)/N. \tag{12.254}$$

*Ce dernier espace vectoriel est le **produit tensoriel** de V par W.*

Remarque 12.119.
Quelque remarques.

30. À part mention du contraire, tous les corps du Frido sont commutatifs.

(1) Les éléments de $V \otimes W$ ne s'écrivent pas tous sous la forme $v \otimes w$. Certains ont vraiment besoin d'être écrits avec des sommes. En cela, la situation de $V \otimes W$ est réellement différente de celle de $V \times W$. Dans ce dernier, tous les éléments sont des couples.

(2) La classe de l'élément $\delta_{(v,w)} \in F(V \times W)$ sera d'habitude noté $v \otimes w$.

(3) Pour insister sur la notion de classe, nous allons aussi noter $[x]$ la classe de $x \in F(V \times W)$.

(4) L'arithmétique dans $V \otimes W$ est relativement simple. En ajoutant et soustrayant le même élément de A_3 nous avons par exemple

$$(\lambda v) \otimes w = (\lambda v) \otimes w + \lambda(v \otimes w) - (\lambda v) \otimes w. \tag{12.255}$$

Nous obtenons de cette façon

$$\lambda(v \otimes w) = (\lambda v) \otimes w = v \otimes (\lambda w), \tag{12.256}$$

que nous noterons $\lambda v \otimes w$ sans plus de précision.

Proposition 12.120 ([191]).
L'espace vectoriel $V \times W$ muni de

$$\begin{aligned} h\colon V \oplus W &\to V \otimes W \\ (v, w) &\mapsto v \otimes w \end{aligned} \tag{12.257}$$

est un produit tensoriel entre V et W.

Démonstration. Nous devons prouver les conditions de la définition 12.115.

<u>h **est bilinéaire**</u> Ce sont des calculs tels que faits dans la remarque 12.119(4) qui font le travail.

<u>h **est surjective**</u> Un élément de $V \otimes W$ est la classe d'un élément de $F(V \times W)$, c'est-à-dire de la forme

$$\big[\sum_{i\alpha} \delta_{(v_i, w_\alpha)}\big] = \sum_{i\alpha} a_{i\alpha} v_i \otimes w_\alpha. \tag{12.258}$$

Cet élément est dans l'image de h comme le montre le calcul suivant [31] :

$$h\big(\sum_{i\alpha}(v_i, w_\alpha)\big) = \sum_{i\alpha} a_{i\alpha} h(v_i, w_\alpha) = \sum_{i\alpha} v_i \otimes w_\alpha. \tag{12.259}$$

<u>**Propriété universelle**</u> Soient un espace vectoriel U et une application linéaire $f\colon V \oplus W \to U$. Nous devons trouver une application linéaire $g\colon V \otimes W \to U$ telle que $f = g \circ h$. Pour cela nous commençons par considérer l'application

$$\begin{aligned} g\colon F(V \times W) &\to U \\ \delta_{(v,w)} &\mapsto f(v, w) \end{aligned} \tag{12.260}$$

définie sur tout $F(V \times W)$ par linéarité sans encombres parce que les $\delta_{v,w}$ forment une base par le lemme 4.23.

Nous démontrons que $g(N) = 0$ pour avoir le droit de passer g aux classes et le considérer comme application partant de $V \otimes W$ au lieu de $F(V \times W)$. Prenons par exemple

$$\begin{aligned} g\big(\delta_{(v_1,w)} + \delta_{(v_2,w)} - \delta_{(v_1+v_2,w)}\big) &= g(\delta_{(v_1,w)}) + g(\delta_{(v_2,w)}) - g(\delta_{v_1+v_2,w}) && \text{(12.261a)} \\ &= f(v_1, w) + f(v_2, w) - f(v_1 + v_2, w) && \text{(12.261b)} \\ &= 0 && \text{(12.261c)} \end{aligned}$$

par la bilinéarité de f. Cela montre que $g(A_1) = 0$. Nous montrons de même que $g(A_2) = g(A_3) = g(A_4) = 0$, et enfin toujours par linéarité que $g(N) = 0$. Pour rappel, les éléments de N sont les combinaisons linéaires finies d'éléments de A_1, A_2, A_3 et A_4.

31. Faites bien la distinction entre $\delta_{v,w}$, (v, w) et $v \otimes w$. Sachez dans quel ensemble se trouvent chacun de ces trois objets.

Par passage aux classes, nous avons une application (que nous notons également g)

$$g\colon F(V\times W)/N\to U \tag{12.262}$$

vérifiant $g(v\otimes w)=f(v,w)$. Mais comme $h(v,w)=v\otimes w$, nous avons $g\circ h\colon V\oplus W\to U$ vérifiant $g\circ h=f$.

L'espace vectoriel $V\otimes W$ est donc un produit tensoriel. □

12.121.
Vu que $V\otimes W$ est un produit tensoriel de V et W, et vu qu'il y a unicité par la proposition 12.117, nous avons bien le droit de dire que $V\otimes W$ est *le* produit tensoriel. Cela justifie le titre.

12.122.
Les prochains lemmes et propositions vont nous dire que l'application

$$\begin{aligned}\varphi\colon V^*\otimes W&\to\mathcal{L}(V,W)\\ \alpha\otimes w&\mapsto\big(v\mapsto\alpha(v)w\big)\end{aligned} \tag{12.263}$$

est un isomorphisme d'espaces vectoriels lorsque V est de dimension finie. Vu que nous aimons les énoncés très explicites, ça va être découpé en plusieurs morceaux, l'énoncé va devenir un peu long ; mais c'est pour la bonne cause.

Lemme 12.123.
Soient deux espaces vectoriels V et W dont W est de dimension finie. Alors l'application définie par

$$\begin{aligned}\varphi\colon F(V^*\times W)&\to\mathcal{L}(V,W)\\ \delta_{(\alpha,w)}&\mapsto\big(v\mapsto\alpha(v)w\big)\end{aligned} \tag{12.264}$$

sur la base « canonique » de $F(V^*\times W)$ passe aux classes.

Démonstration. Avec les notations de la définition 12.118 nous devons prouver que $\varphi(N)=0$. Nous montrons que $\varphi(A_4)=0$, et nous vous laissons faire les autres. Pour $\lambda\in\mathbb{K}$, $\alpha\in V^*$ et $w\in W$ en utilisant la linéarité de φ nous avons :

$$\varphi\big(\lambda\delta_{(\alpha,w)}-\delta_{(\alpha,\lambda w)}\big)v=\lambda\varphi(\delta_{(\alpha,w)})(v)-\varphi(\delta_{(\alpha,\lambda w)})(v) \tag{12.265a}$$
$$=\lambda\alpha(v)w-\alpha(v)(\lambda w) \tag{12.265b}$$
$$=0 \tag{12.265c}$$

parce que $\alpha(v)(\lambda w)=\lambda\alpha(v)w$ du fait que $\mathbb{K}$ est commutatif. La commutativité de $\mathbb{K}$ est ce qui permet de permuter le produit $\lambda\alpha(v)$.

Nous laissons à la lectrice le soin de prouver que $\varphi(A_1)=\varphi(A_2)=\varphi(A_3)=0$. □

Lemme 12.124.
Si W est de dimension finie, alors $\mathcal{L}(V,W)$ muni de

$$\begin{aligned}h'\colon V^*\oplus W&\to\mathcal{L}(V,W)\\ (\alpha,w)&\mapsto\big(v\mapsto\alpha(v)w\big)\end{aligned} \tag{12.266}$$

est un produit tensoriel[32] *de V^* par W.*

Démonstration. Nous devons prouver que

— h est bilinéaire,

— h est surjective

— pour tout espace vectoriel U, et pour toute application bilinéaire $f\colon V^*\oplus W\to U$, il existe une application linéaire $g\colon\mathcal{L}(V,W)\to U$ tel que $f=g\circ h$.

32. Définition 12.115.

Bilinéaire Le fait que h soit bilinéaire est une simple vérification.

Surjective L'espace W étant de dimension finie, nous pouvons en considérer une base $\{z_i\}_{i\in I}$. Soit $\alpha \in \mathcal{L}(V,W)$. Si $v \in V$, l'élément $\alpha(v)$ peut être décomposé dans la base $\{z_i\}$, ce qui définit des applications linéaires $\alpha_i\colon V \to \mathbb{K}$ par

$$\alpha(v) = \sum_{i\in I} \alpha_i(v) z_i. \tag{12.267}$$

Notons que $\alpha_i \in V^*$. En comparant avec la définition de h', nous voyons que

$$\alpha(v) = \sum_i h(\alpha_i, z_i)(v), \tag{12.268}$$

c'est-à-dire $\alpha = \sum_i h(\alpha_i, w_i) = h\big(\sum_i(\alpha_i, z_i)\big)$. Nous avons donc bien $\alpha \in h(V^* \oplus W)$.

Propriété universelle Soient un espace vectoriel U et une application bilinéaire $f\colon V^*\oplus W \to U$. Pour $\alpha \in \mathcal{L}(V,W)$ nous définissons $g(\alpha)$ comme suit. D'abord nous écrivons α sous la forme

$$\alpha(v) = \sum_i \alpha_i(v) z_i, \tag{12.269}$$

et nous posons

$$g(\alpha) = \sum_i f(\alpha_i, z_i). \tag{12.270}$$

Avec cette définition, en posant $w = \sum_i w_i z_i$, nous avons

$$\begin{aligned}
(g \circ h')(\alpha, w) &= g\big(v \mapsto \alpha(v)w\big) && \text{(12.271a)}\\
&= g\big(v \mapsto \sum_i \alpha(v) w_i z_i\big) && \text{(12.271b)}\\
&= \sum_i f(w_i\alpha, z_i) && \text{(12.271c)}\\
&= \sum_i f(\alpha, w_i z_i) && \text{(12.271d)}\\
&= f(\alpha, \sum_i w_i z_i) && \text{(12.271e)}\\
&= f(\alpha, w). && \text{(12.271f)}
\end{aligned}$$

Cela prouve que $g \circ h = f$.

□

Proposition 12.125 ([192]).
Soient deux espaces vectoriels V et W dont V est de dimension finie. Alors l'application

$$\begin{aligned}
\varphi\colon V^* \otimes W &\to \mathcal{L}(V,W)\\
\alpha \otimes w &\mapsto \big(v \mapsto \alpha(v)w\big)
\end{aligned} \tag{12.272}$$

est bien définie[33] *et est un isomorphisme d'espaces vectoriels.*

Démonstration. Le lemme 12.124 donne une structure de produit tensoriel de V^* par W sur $\mathcal{L}(V,W)$. Rappelons les structures :

$$\begin{aligned}
h\colon V^* \oplus W &\to V^* \otimes W\\
(\alpha, w) &\mapsto \alpha \otimes w
\end{aligned} \tag{12.273}$$

et

$$\begin{aligned}
h'\colon V^* \oplus W &\to \mathcal{L}(V,W)\\
(\alpha, w) &\mapsto \big[v \mapsto \alpha(v)w\big].
\end{aligned} \tag{12.274}$$

La proposition 12.117 a déjà fait tout le boulot. La seule chose à faire est de vérifier qu'il existe une application $\varphi\colon V^* \otimes W \to \mathcal{L}(V,W)$ vérifiant simultanément les deux conditions suivantes :

33. Au sens où il existe une fonction φ définie sur tout $V^* \otimes W$ qui se réduit à cela pour les éléments de la forme $\alpha \otimes w$.

(1) $\varphi(\alpha\otimes w)=\big[v\mapsto\alpha(v)w\big]$

(2) $h'=\varphi\varphi\circ h$.

La seconde condition assure que φ sera un isomorphisme d'espaces vectoriels.

L'existence de φ vérifiant la condition (1) est un effet du lemme 12.123 qui donne une fonction sur $F(V^*\times W)$ dont le φ qui nous concerne est un quotient. Il reste à voir que cette application vérifie $h'=\varphi\circ h$.

En nous rappellant que $\alpha\otimes w=[\delta_{(\alpha,w)}]$ et en écrivant φ à la fois l'application et son passage au quotient,

$$(\varphi\circ h)(\alpha,w)=\varphi(\alpha\otimes w)=\varphi\big([\delta_{(\alpha,w)}]\big)=\varphi(\delta_{(\alpha,w)}).\tag{12.275}$$

En appliquant à $v\in V$ nous avons :

$$(\varphi\circ h)(\alpha,w)v=\varphi(\delta_{(\alpha,w)})v=\alpha(v)w=h'(\alpha,w)v.\tag{12.276}$$

Et voila. Nous avons $\varphi\circ h=h'$. □

Une conséquence de la proposition 12.125 est que

$$\dim(V\otimes W)=\dim(V)\dim(W)\tag{12.277}$$

via le lemme 4.34(2).

12.8.4 Bases

Voici un lemme entièrement dédié au principe « dans le Frido, on ne fait pas d'abus de notations, sauf pour la logique formelle et la théorie des ensembles, que nous admettons ».

Lemme 12.126 ([1]).
Si $\tau\colon V_1\to V_2$ est un isomorphisme d'espaces vectoriels, alors

$$\begin{aligned}\varphi\colon V_1\otimes W&\to V_2\otimes W\\ v\otimes w&\mapsto\tau(v)\otimes W\end{aligned}\tag{12.278}$$

est un isomorphisme d'espaces vectoriels.

Démonstration. Comme d'habitude, l'expression (12.278) ne définit pas réellement φ parce que nous ne savons pas du tout si $\{v\otimes w\text{ tel que }v\in V,w\in W\}$ est plus ou moins une base de $V\otimes W$ [34]. Ce que dit réellement ce lemme est qu'il existe une application $V_1\otimes W\to V_2\otimes W$ qui est isomorphisme et qui se réduit à l'expression donnée dans le cas d'éléments de $V_1\otimes W$ de la forme $v\otimes w$.

L'application

$$\begin{aligned}\varphi_0\colon F(V_1\times W)&\to F(V_2\times W)\\ \delta(v,w)&\mapsto\delta_{\big(\tau(v),w\big)}\end{aligned}\tag{12.279}$$

est un isomorphisme.

Cette application passe aux classes, mais pas au sens où $x\in[y]$ impliquerait $\varphi_0(x)=\varphi_0(y)$; au sens où si $x\in[y]$, alors $\varphi_0(x)\in[\varphi_0(y)]$. Par exemple

$$\varphi_0\big(\lambda\delta_{(v,w)}-\delta_{(v,\lambda w)}\big)=\lambda\delta_{\big(\tau(v),w\big)}-\delta_{\big(\tau(v),w\big)}\in[0].\tag{12.280}$$

Nous vous laissons le soin de vérifier les égalités correspondantes pour les autres parties de N.

Le passage au classes de φ_0 signifie que l'on considère l'application

$$\begin{aligned}\varphi\colon V_1\otimes W&\to V_2\otimes W\\ [x]&\mapsto[\varphi_0(x)]\end{aligned}\tag{12.281}$$

34. Ne lisez pas la proposition 12.127 qui dévoile toute l'intrigue.

où vous aurez noté que la prise de classe à gauche n'est pas la même que celle à droite.

Il faut prouver que ce φ est un isomorphisme. En ce qui concerne la linéarité,

$$\begin{aligned}\varphi\big([x]+[y]\big) &= \varphi\big([x+y]\big) && (12.282a)\\ &= [\varphi_0(x+y)] && (12.282b)\\ &= [\varphi_0(x)+\varphi_0(y)] && (12.282c)\\ &= [\varphi_0(x)]+[\varphi_0(y)] && (12.282d)\\ &= \varphi([x])+\varphi([y]). && (12.282e)\end{aligned}$$

Je vous laisse le reste de la linéarité. Et en ce qui concerne le fait que ce soit une bijection, allez-y. □

Proposition 12.127 ([192]).
Soient des espaces vectoriels de dimension finie V et W. Soient une base $\{e_i\}$ de V et une base $\{f_\alpha\}$ de W.

Alors :

(1) La partie $\{e_i \otimes f_\alpha\}$ est une base de $V \otimes W$.

(2) Au niveau des dimensions, $\dim(V \otimes W) = \dim(V)\dim(W)$.

Démonstration. Vu que V est de dimension finie, nous avons un isomorphisme d'espaces vectoriels $V^* = V$, et même un isomorphisme d'espaces vectoriels

$$\begin{aligned}\tau\colon V &\to (V^*)^*\\ \tau(v)\alpha &= \alpha(v).\end{aligned} \tag{12.283}$$

Recopions l'isomorphisme de la proposition 12.125 en utilisant V^* au lieu de V :

$$\begin{aligned}\psi_0\colon (V^*)^* \otimes W &\to \mathcal{L}(V^*, W)\\ \tau(v)\otimes w &\mapsto \big(\alpha \mapsto \tau(v)(\alpha)w = \alpha(v)w\big).\end{aligned} \tag{12.284}$$

En écrivant cela, nous avons tenu compte du fait que tout élément de $(V^*)^*$ peut être écrit de façon univoque sous la forme $\tau(v)$ pour un certain $v \in V$.

Vu que τ est un isomorphisme, l'application suivante est encore un isomorphisme [35] :

$$\begin{aligned}\psi\colon V \otimes W &\to \mathcal{L}(V^*, W)\\ v\otimes w &\mapsto \big(\alpha \mapsto \alpha(v)w\big).\end{aligned} \tag{12.285}$$

Nous avançons. Vu que nous avons un isomorphisme, nous pouvons faire passer des bases. Le lemme 4.34 nous donne une base de $\mathcal{L}(V^*, W)$ en les éléments $\beta_{i\alpha}\colon V^* \to W$ définies par

$$\beta_{ij}(\alpha) = \alpha(e_i)f_\alpha. \tag{12.286}$$

Donc $\{\psi^{-1}(\beta_{i\alpha})\}$ est une base de $V \otimes W$.

Pour $a = \sum_i a_i e_i^*$ (base duale, définition 4.113) nous avons :

$$\psi(e_i \otimes f_\alpha)a = a(e_i)f_\alpha = \beta_{i\alpha}(a). \tag{12.287}$$

Cela prouve que $\psi^{-1}(\beta_{i\alpha}) = e_i \otimes f_\alpha$, et donc que ces $e_i \otimes f_\alpha$ est une base de $V \otimes W$.

La formule concernant les dimensions est simplement la définition 4.13 de la dimension : le nombre d'éléments dans une base. □

Exemple 12.128
Dans le produit tensoriel $\mathbb{R}\otimes\mathbb{R}$, nous avons $x\otimes 1 = 1\otimes x = x(1\otimes x)$ pour tout $x \in \mathbb{R}$. Et si $x \geqslant 0$ nous avons aussi $x \otimes 1 = \sqrt{x} \otimes \sqrt{x}$. △

35. Lemme 12.126.

12.8.5 Norme

Nous considérons des espaces vectoriels V et W de dimension finie. L'application (12.285) donne un isomorphisme d'espaces vectoriels

$$\begin{aligned}\psi\colon V\otimes W &\to \mathcal{L}(V^*,W)\\ v\otimes w &\mapsto \big(\alpha\mapsto\alpha(v)w\big).\end{aligned}\tag{12.288}$$

Et ça, c'est très bien, parce que nous connaissons une norme sur $\mathcal{L}(V^*,W)$: la norme opérateur 12.10.

Définition 12.129 ([1]).
Soient deux espaces vectoriels normés de dimension finie V et W. Sur $V\otimes W$ nous définissons, pour $t\in V\otimes W$

$$\|t\|=\|\psi(t)\|_{\mathcal{L}(V^*,W)}.\tag{12.289}$$

Lemme 12.130 ([1]).
La norme sur $V\otimes W$ vérifie

$$\|v\otimes w\|=\|v\|\|w\|\tag{12.290}$$

pour tout $v\in V$ et $w\in W$.

Démonstration. C'est un simple(?) calcul :

$$\|v\otimes w\|=\|\psi(v\otimes w)\|=\|\alpha\mapsto\alpha(v)w\|=\sup_{\|\alpha\|=1}\|\alpha(v)w\|=\sup_{\|\alpha\|=1}|\alpha(v)|\|w\|.\tag{12.291}$$

Étant donné que V est de dimension finie, $\sup_{\|\alpha\|=1}|\alpha(v)|=\|v\|$ [36]. Nous avons donc

$$\|v\otimes w\|=\|v\|\|w\|.\tag{12.292}$$

□

Le lemme suivant montre que $\mathbb{R}\otimes\mathbb{R}$ n'est pas du tout $\mathbb{R}\times\mathbb{R}=\mathbb{R}^2$. Au contraire, $\mathbb{R}\otimes\mathbb{R}$ est isomorphe à $\mathbb{R}$.

Lemme 12.131 ([1]).
L'application

$$\begin{aligned}\varphi\colon\mathbb{R}\otimes\mathbb{R}&\to\mathbb{R}\\ 1\otimes1&\mapsto1\end{aligned}\tag{12.293}$$

prolongée par linéarité est un isomorphisme isométrique.

Démonstration. D'abord une base de $\mathbb{R}$ est $\{1\}$; donc une base de $\mathbb{R}\otimes\mathbb{R}$ est $\{1\otimes1\}$ par la proposition 12.127. Donc l'application proposée se prolonge par linéarité à tout $\mathbb{R}\otimes\mathbb{R}$.

Le fait que φ soit une bijection provient du fait que φ transforme une base en une base ; si vous n'y croyez pas, la vérification de l'injectivité et de la surjectivité est facile.

Pour que φ soit isométrique, nous faisons le calcul

$$\|\varphi(x\otimes y)\|=\|xy(1\otimes1)\|=|xy|\|1\otimes1\|=|xy|=\|x\otimes y\|.\tag{12.294}$$

Nous avons utilisé la propriété 7.106(2) d'une norme ainsi que le lemme 12.130 pour la norme sur $\mathbb{R}\otimes\mathbb{R}$. □

36. Cela est une des raisons pour lesquelles nous sommes en dimension finie : je ne sais pas si cette égalité est vraie en dimension inifinie.

12.8.6 Applications bilinéaires, matrices et produit tensoriel

Soit E, un espace vectoriel de dimension finie. Si α et β sont deux formes linéaires sur un espace vectoriel E, nous définissons $\alpha \otimes \beta$ comme étant la 2-forme donnée par

$$(\alpha \otimes \beta)(u, v) = \alpha(u)\beta(v). \tag{12.295}$$

Si a et b sont des vecteurs de E, ils sont vus comme des formes sur E via le produit scalaire et nous avons

$$(a \otimes b)(u, v) = (a \cdot u)(b \cdot v). \tag{12.296}$$

Cette dernière équation nous incite à pousser un peu plus loin la définition de $a \otimes b$ et de simplement voir cela comme la matrice de composantes

$$(a \otimes b)_{ij} = a_i b_j. \tag{12.297}$$

Cette façon d'écrire a l'avantage de ne pas demander de se souvenir qui est une vecteur ligne, qui est un vecteur colonne et où il faut mettre la transposée. Évidemment $(a \otimes b)$ est soit ab^t soit $a^t b$ suivant que a et b soient ligne ou colonne.

12.8.7 Application d'opérateurs

Lemme 12.132.
Soient $x, y \in E$ et A, B deux opérateurs linéaires sur E vus comme matrices. Alors

$$(Ax \otimes By) = A(x \otimes y)B^t. \tag{12.298}$$

Démonstration. Calculons la composante ij de la matrice $(Ax \otimes By)$. Nous avons

$$\begin{aligned}
(Ax \otimes By)_{ij} &= (Ax)_i (By)_j && \text{(12.299a)}\\
&= \sum_{kl} A_{ik} x_k B_{jl} y_l && \text{(12.299b)}\\
&= A_{ik}(x \otimes y)_{kl} B_{jl} && \text{(12.299c)}\\
&= \big(A(x \otimes y)B^t\big)_{ij}. && \text{(12.299d)}
\end{aligned}$$

□

12.9 Calcul différentiel dans un espace vectoriel normé

Quelque motivations pour la notion de différentielle sont données dans 13.20.1.

12.9.1 Définition de la différentielle

Proposition-définition 12.133 ([1]).
Soient deux espaces vectoriels normés E et F ainsi qu'une fonction $f : \mathcal{U} \to F$ où $\mathcal{U}$ est un ouvert de E.

Si il existe une une application linéaire $T \in \mathcal{L}(E, F)$ satisfaisant

$$\lim_{\substack{h \to 0 \\ h \in E}} \frac{f(a+h) - f(a) - T(h)}{\|h\|_E} = 0, \tag{12.300}$$

alors il en existe une seule.

*Dans ce cas nous disons que f est **différentiable au point** a et l'application T ainsi définie est appelée **différentielle** de f au point a, et nous la notons df_a.*

Démonstration. Soient deux applications linéaires T_1, T_2 satisfaisant la condition (12.300). Nous avons

$$\frac{\|T_1(h)-T_2(h)\|_F}{\|h\|_E} \leqslant \frac{\|T_1(h)-f(a+h)+f(a)\|}{\|h\|} + \frac{\|f(a+h)-f(a)-T_2(h)\|}{\|h\|} \to 0. \tag{12.301}$$

Nous avons donc

$$\lim_{h\to 0} \frac{\|(T_1-T_2)(h)\|_F}{\|h\|_E} = 0. \tag{12.302}$$

Soit $\epsilon > 0$. Ce que signifie la limite est qu'il existe un $r > 0$ tel que pour tout $u \in B_E(0,r)$, nous ayons

$$\frac{\|(T_1-T_2)(u)\|_F}{\|u\|_E} < \epsilon. \tag{12.303}$$

Soit $v \in E$. Nous considérons $\lambda \in \mathbb{R}$ tel que $\lambda v \in B(0,r)$, par exemple $\lambda < r/\|v\|$. Nous avons

$$\epsilon > \frac{\|(T_1-T_2)(\lambda v)\|_F}{\|\lambda v\|_E} = \frac{\|(T_1-T_2)(v)\|}{\|v\|}. \tag{12.304}$$

Cela donne

$$\|(T_1-T_2)(v)\| < \|v\|\epsilon. \tag{12.305}$$

Nous avons donc $\|(T_1-T_2)(v)\| = 0$, soit $T_1(v) = T_2(v)$. □

L'application différentielle

$$\begin{aligned} df\colon E &\to \mathcal{L}(E,F) \\ a &\mapsto df_a \end{aligned} \tag{12.306}$$

est également très importante.

Définition 12.134.
*Une application $f\colon E \to F$ est de **classe** C^1 lorsque l'application différentielle $df\colon E \to \mathcal{L}(E,F)$ est continue. Voir aussi les définitions 13.263 pour les applications de classe C^k.*

Remarque 12.135.
L'application norme étant continue, le critère du théorème 7.99 est en réalité assez général. Par exemple à partir d'une application différentiable[37] $f\colon X \to Y$ nous pouvons considérer la fonction réelle

$$a \mapsto \|df_a\| \tag{12.307}$$

où la norme est la norme opérateur[38]. Si f est de classe C^1 alors cette application est continue et donc bornée sur un compact K de X.

12.9.2 Accroissements finis

Lemme 12.136.
Soit une fonction $f\colon E \to V$ (espaces vectoriels normés) différentiable en $a \in E$. Alors il existe une fonction $\alpha\colon E \to V$ telle que

$$\begin{cases} \lim_{h\to 0} \dfrac{\alpha(h)}{\|h\|} = 0 & \text{(12.308a)} \\ f(a+h) = f(a) + df_a(h) + \alpha(h). & \text{(12.308b)} \end{cases}$$

Démonstration. Il s'agit seulement de poser

$$\alpha(h) = f(a+h) - f(a) - df_a(h). \tag{12.309}$$

Le fait que $\alpha(h)/\|h\| \to 0$ est alors la définition de la différentiabilité de f. □

37. Définition 12.133.
38. Définition 12.10.

12.9.3 (non ?) Différentiabilité des applications linéaires

Si E et F sont deux espaces vectoriels nous notons $\mathcal{L}(E,F)$ l'ensemble des applications linéaires de E vers F et $L(E,F)$ l'ensemble des applications linéaires continues de E vers F. Ces espaces seront bien entendu, sauf mention du contraire, toujours munis de la norme opérateur de la définition 12.10.

Lemme 12.137.
Soit une application linéaire f.

(1) Si f est continue, alors elle est différentiable et $df_a(u) = f(u)$ pour tout a et u.

(2) Si f n'est pas continue, alors elle n'est pas différentiable.

Démonstration. La linéarité de f donne :

$$f(a+h) - f(a) - f(h) = 0, \tag{12.310}$$

et donc prendre $T = f$ dans la définition 12.133 fait fonctionner la limite. De plus T est alors continue par hypothèse ; elle est donc bien la différentielle de f.

Supposons que f ne soit pas continue, prenons une application linéaire continue T, et calculons

$$\frac{f(a+h) - f(a) - T(h)}{\|h\|} = \frac{(f-T)(h)}{\|h\|} = (f-T)(e_h) \tag{12.311}$$

où e_h est le vecteur unitaire dans la direction de h. Vu que f n'est pas continue et que T l'est, l'application $f - T$ n'est pas continue. Elle n'est pas pas bornée par la proposition 12.25. Il existe alors un vecteur h tel que $\|(f-T)(e_h)\| > 1$ (et même plus grand que ce qu'on veut).

Donc la limite de (12.311) pour $h \to 0$ ne peut pas être nulle. □

Lemme 12.138.
Une application linéaire continue est de classe C^∞.

Démonstration. Soit $a \in E$. Étant donné que f est linéaire et continue, elle est différentiable et

$$\begin{aligned} df \colon E &\to L(E,F) \\ a &\mapsto f \end{aligned} \tag{12.312}$$

est une fonction constante et en particulier continue ; nous avons donc $f \in C^1$. Pour la différentielle seconde nous avons $d(df)_a = 0$ parce que $df(a+h) - df(a) = f - f = 0$. Toutes les différentielles suivantes sont nulles. □

12.9.4 Dérivation en chaine et formule de Leibnitz

Proposition 12.139.
Soient $f_i \colon U \to F_i$, des fonctions de classe C^r où U est ouvert dans l'espace vectoriel normé E et les F_i sont des espaces vectoriels normés. Alors l'application

$$\begin{aligned} f = f_1 \times \cdots \times f_n \colon U &\to F_1 \times \cdots \times F_n \\ x &\mapsto \big(f_1(x), \dots, f_n(x)\big) \end{aligned} \tag{12.313}$$

est de classe C^r et

$$d^r f = d^r f_1 \times \dots d^r f_n. \tag{12.314}$$

Démonstration. Soit $x \in U$ et $h \in E$. La différentiabilité des fonctions f_i donne

$$f_i(x+h) = f_i(x) + (df_i)_x(h) + \alpha_i(h) \tag{12.315}$$

avec $\lim_{h\to 0} \alpha_i(h)/\|h\| = 0$. Par conséquent

$$f(x+h) = \big(\dots, f_i(x) + (df_i)_x(h) + \alpha_i(h), \dots\big) \tag{12.316a}$$

$$= \big(\dots, f_i(x), \dots\big) + \big(\dots, (df_i)_x(h), \dots\big) + \big(\dots, \alpha_i(h), \dots\big). \tag{12.316b}$$

Mais la définition 12.41 de la norme dans un espace produit donne

$$\lim_{h\to 0}\frac{\|\big(\alpha_1(h),\dots,\alpha_n(h)\big)\|}{\|h\|}=0, \tag{12.317}$$

ce qui nous permet de noter $\alpha(h)=\big(\alpha_1(h),\dots,\alpha_n(h)\big)$ et avoir $\lim_{h\to 0}\alpha(h)/\|h\|=0$. Avec tout ça nous avons bien

$$f(x+h)=f(x)+\big((df_1)_x(h)+\cdots+(df_n)_x(h)\big)+\alpha(h), \tag{12.318}$$

ce qui signifie que f est différentiable et

$$df_x=\big(df_1,\dots,df_n\big). \tag{12.319}$$

□

Théorème 12.140.
Soient des espaces vectoriels normés E,V et W. Nous considérons deux fonctions $f\colon E\to V$ et $g\colon V\to W$. Nous supposons que f est différentiable en $a\in E$ et que g est différentiable en $f(a)\in V$.

Nous supposons de plus que df_a est de norme finie[39].

Alors $g\circ f\colon E\to W$ est différentiable en a et

$$f(g\circ f)_a(u)=df_{f(a)}\big(df_a(u)\big), \tag{12.320}$$

ou encore

$$f(g\circ f)_a=dg_{f(a)}\circ df_a. \tag{12.321}$$

Démonstration. En utilisant le lemme 12.136 pour les fonctions f et g, nous avons

$$f(a+h)=f(a)+df_a(h)+\alpha(h) \tag{12.322}$$

et

$$g\big(f(a)+k\big)=g\big(f(a)\big)+dg_{f(a)}(k)+\beta(k). \tag{12.323}$$

L'application $dg_{f(a)}\circ df_a$ est une application linéaire, et est notre candidat différentielle. En suivant la définition 12.133, nous allons calculer

$$\lim_{h\to 0}\frac{(g\circ f)(a+h)-(g\circ f)(a)-(dg_{f(a)}\circ df_a)(h)}{\|h\|}. \tag{12.324}$$

Si cette limite existe et vaut zéro, alors nous aurons prouvé que le candidat différentielle est correct.

Pour cela, nous emboîtons les formules (12.322) et (12.323) l'une dans l'autre pour avoir :

$$g(a+h)=g\big(f(a)+df_a(h)+\alpha(h)\big)=g\big(f(a)\big)+dg_{f(a)}\big(df_a(h)+\alpha(h)\big)+\beta\big(df_a(h)+\alpha(h)\big). \tag{12.325}$$

Vu que $dg_{f(a)}$ est linéaire, le deuxième terme peut être coupé en deux et après recombinaisons,

$$(g\circ f)(a+h)-(g\circ f)(a)-(df_{f(a)}\circ df_a)(h)=dg_{f(a)}\big(\alpha(h)\big)+\beta\big(df_a(h)+\alpha(h)\big). \tag{12.326}$$

Étant donné que $dg_{f(a)}$ est linéaire,

$$\frac{dg_{f(a)}\big(\alpha(h)\big)}{\|h\|}=dg_{f(a)}\left(\frac{\alpha(h)}{\|h\|}\right)\to 0. \tag{12.327}$$

Il nous reste à voir que

$$\lim_{h\to 0}\frac{\beta\big(df_a(h)+\alpha(h)\big)}{\|h\|} \tag{12.328}$$

39. Je ne suis pas totalement certain que cette hypothèse soit nécessaire, mais en tout cas, elle est utilisée.

existe au vaut zéro. Vu que df_a est linéaire, il existe $M > 0$ tel que[40] $\|df_a(h)\| \leqslant M\|h\|$. D'autre part, vu que $\alpha(h)/\|h\| \to 0$, nous avons $\|\alpha(h)\| \leqslant \|h\|$ pour tout h suffisamment petit.

Donc si h est assez petit, nous avons

$$\|df_a(h) + \alpha(h)\| \leqslant (M+1)\|h\|. \tag{12.329}$$

Soit $\epsilon > 0$. Soit $\delta > 0$ tel que $\|h\| \leqslant \delta$ implique $\beta(h)/\|h\| \leqslant \epsilon$ et (12.329) en même temps. Soit r tel que $(M+1)r < \delta$; et notons que $r < \delta$. Nous considérons alors $h \in B(0,r)$ et nous calculons :

$$\frac{\beta\big(df_a(h)+\alpha(h)\big)}{\|h\|} = \frac{\beta\big(df_a(h)+\alpha(h)\big)}{\|df_a(h)+\alpha(h)\|}\frac{\|df_a(h)+\alpha(h)\|}{\|h\|} \leqslant (M+1)\epsilon. \tag{12.330}$$

La limite (12.328) existe donc et vaut zéro. □

Théorème 12.141 (Différentielle de fonctions composées[193])**.**
Soient E, F et G des espaces vectoriels normés, U ouvert dans E et V ouvert dans F. Soient des applications de classe C^r ($r \geqslant 1$)

$$f : U \to V \tag{12.331a}$$
$$g : V \to G. \tag{12.331b}$$

Alors l'application $g \circ f : V \to G$ est de classe C^r et

$$d(g\circ f)_x = dg_{f(x)} \circ df_x. \tag{12.332}$$

Démonstration. Nous nous fixons $x \in U$. La fonction f est différentiable en $x \in U$ et g en $f(x)$, donc nous pouvons écrire

$$f(x+h) = f(x) + df_x(h) + \alpha(h) \tag{12.333}$$

et

$$g\big(f(x)+u\big) = g\big(f(x)\big) + dg_{f(x)}(u) + \beta(u) \tag{12.334}$$

où la fonction α a la propriété que

$$\lim_{h\to 0}\frac{\|\alpha(h)\|}{\|h\|} = 0; \tag{12.335}$$

et la même chose pour β. La fonction composée en $x+h$ s'écrit donc

$$(g\circ f)(x+h) = g\big(f(x)+df_x(h)+\alpha(h)\big) = g\big(f(x)\big) + dg_{f(x)}\big(df_x(h)+\alpha(h)\big) + \beta\big(df_x(h)+\alpha(h)\big). \tag{12.336}$$

Nous montrons que tous les « petits » termes de cette formule peuvent être groupés. D'abord si h est proche de 0, nous avons

$$\frac{\|df_x(h)+\alpha(h)\|}{\|h\|} \leqslant \frac{\|df_x\|\|h\|}{\|h\|} + \frac{\|\alpha(h)\|}{\|h\|}. \tag{12.337}$$

Si h est petit, le second terme est arbitrairement petit, donc en prenant n'importe que $M > \|df_x\|$ nous avons

$$\frac{\|df_x(h)+\alpha(h)\|}{\|h\|} \leqslant M. \tag{12.338}$$

Par ailleurs, nous avons

$$\frac{\|\beta\big(df_x(h)+\alpha(h)\big)\|}{\|h\|} = \frac{\|\beta\big(df_x(h)+\alpha(h)\big)\|}{\|df_x(h)+\alpha(h)\|}\frac{\|df_x(h)+\alpha(h)\|}{\|h\|} \leqslant M\frac{\|\beta\big(df_x(h)+\alpha(h)\big)\|}{\|df_x(h)+\alpha(h)\|}. \tag{12.339}$$

Vu que la fraction est du type $\frac{\beta(f(h))}{f(h)}$ avec $\lim_{h\to 0} f(h) = 0$, la fraction tend vers zéro lorsque $h \to 0$. En posant

$$\gamma_1(h) = \beta\big(df_x(h)+\alpha(h)\big) \tag{12.340}$$

40. Ce M est par exemple la norme opérateur de df_a, comme nous l'assure le lemme 12.17. C'est pour ce passage-ci que nous avons supposé que df_a était de norme finie.

nous avons $\lim_{h\to 0}\gamma_1(h)/\|h\|=0$.

L'autre candidat à être un petit terme dans (12.336) est traité en utilisant le lemme 12.20 :

$$\|dg_{f(x)}\big(\alpha(h)\big)\|\leqslant\|dg_{f(x)}\|\|\alpha(h)\|. \tag{12.341}$$

Donc

$$\frac{\|dg_{f(x)}\big(\alpha(h)\big)\|}{\|h\|}\leqslant\|dg_{f(x)}\|\frac{\|\alpha(h)\|}{\|h\|}, \tag{12.342}$$

ce qui nous permet de poser

$$\gamma_2(h)=dg_{f(x)}\big(\alpha(h)\big) \tag{12.343}$$

avec γ_2 qui a la même propriété que γ_1. Avec tout cela, en posant $\gamma=\gamma_1+\gamma_2$ nous récrivons

$$(g\circ f)(x+h)=g\big(f(x)\big)+dg_{f(x)}\big(df_x(h)\big)+\gamma(h) \tag{12.344}$$

avec $\lim_{h\to 0}\frac{\gamma(h)}{\|h\|}=0$. Tout cela pour dire que

$$\lim_{h\to 0}\frac{(g\circ f)(x+h)-(g\circ f)(x)-\big(dg_{f(x)}\circ df_x\big)(h)}{\|h\|}=0, \tag{12.345}$$

ce qui signifie que

$$d(g\circ f)_x=dg_{f(x)}\circ df_x. \tag{12.346}$$

Nous avons donc montré que si f et g sont différentiables, alors $g\circ f$ est différentiable avec différentielle donnée par (12.332).

Nous passons à la régularité. Nous supposons maintenant que f et g sont de classe C^r et nous considérons l'application

$$\begin{aligned}\varphi\colon L(F,G)\times L(E,F)&\to L(E,G)\\(A,B)&\mapsto A\circ B.\end{aligned} \tag{12.347}$$

Montrons que l'application φ est continue en montrant qu'elle est bornée [41]. Pour cela nous écrivons la norme opérateur

$$\|\varphi\|=\sup_{\|(A,B)\|=1}\|\varphi(A,B)\|=\sup_{\|(A,B)\|=1}\|A\circ B\|\leqslant\sup_{\|(A,B)\|=1}\|A\|\|B\|\leqslant 1. \tag{12.348}$$

Justifications : d'une part la norme opérateur est une norme algébrique [42], et d'autre part la définition 12.41 de la norme sur un espace produit pour la dernière majoration. L'application φ est donc continue et donc C^∞ par le lemme 12.138. Nous considérons également l'application

$$\begin{aligned}\psi\colon U&\to L(F,G)\times L(E,F)\\x&\mapsto\big(dg_{f(x)},df_x\big).\end{aligned} \tag{12.349}$$

Vu que f et g sont C^1, l'application ψ est continue. Ces deux applications φ et ψ sont choisies pour avoir

$$(\varphi\circ\psi)(x)=\varphi\big(dg_{f(x)},df_x\big)=dg_{f(x)}\circ df_x, \tag{12.350}$$

c'est-à-dire $\varphi\circ\psi=d(g\circ f)$. Les applications φ et ψ étant continues, l'application $d(g\circ f)$ est continue, ce qui prouve que $g\circ f$ est C^1.

Si f et g sont C^r alors $dg\in C^{r-1}$ et $dg\circ f\in C^{r-1}$ où il ne faut pas se tromper : $dg\colon F\to L(F,G)$ et $f\colon U\to F$; la composée est $dg\circ f\colon x\mapsto dg_{f(x)}\in L(F,G)$.

Pour la récurrence nous supposons que $f,g\in C^{r-1}$ implique $g\circ f\in C^{r-1}$ pour un certain $r\geqslant 2$ (parce que nous venons de prouver cela avec $r=1$ et $r=2$). Soient $f,g\in C^r$ et montrons que $g\circ f\in C^r$. Par la proposition 12.139 nous avons

$$\psi=dg\circ f\times df\in C^{r-1}, \tag{12.351}$$

et donc $d(g\circ f)=\varphi\circ\psi\in C^{r-1}$, ce qui signifie que $g\circ f\in C^r$. □

41. Proposition 12.25.
42. Lemme 12.20.

Proposition 12.142 ([1]).
Soit une application $f\colon E \to V$ de classe C^1. Soit une application linéaire $\varphi\colon V \to W$. Alors $\varphi \circ f$ est de classe C^p.

Démonstration. Toute la preuve est un grand jeu de cohérence des espaces en présence, alors soyez attentifs et capable de dire précisément à quel espace appartient chacun de objets entrant en jeu.

Nous posons $V_0 = V$ et $V_{k+1} = \mathcal{L}(E, V_k)$. Idem pour les espaces W_k. Ensuite nous posons

$$\begin{aligned} \varphi_1\colon \mathcal{L}(E,V) &\to \mathcal{L}(E,W) \\ \alpha &\mapsto \varphi \circ \alpha. \end{aligned} \tag{12.352}$$

et

$$\begin{aligned} \varphi_k\colon \mathcal{L}(E,V_{k-1}) &\to \mathcal{L}(E,W_{k-1}) \\ \alpha &\mapsto \varphi_{k-1} \circ \alpha. \end{aligned} \tag{12.353}$$

Notez la cohérence : si $a \in E$, $\alpha(a) \in V_{k-1} = \mathcal{L}(E, V_{k-2})$, et donc

$$(\varphi_{k-1} \circ \alpha)(a) = \varphi_{k-1}\big(\alpha(a)\big). \tag{12.354}$$

À droite nous avons $\varphi_{k-1}\big(\alpha(a)\big) \in \mathcal{L}(E, W_{k-2}) = V_{k-1}$.

De plus, φ est linéaire ; ça se prouve par récurrence en partant de φ_1 et en se basant sur le fait que φ est linéaire.

C'est parti pour une récurrence.

Énoncé Nous allons prouver par récurrence que

$$d^k(\varphi \circ f) = \varphi_k \circ d^k f. \tag{12.355}$$

pour tout $k \leqslant p$.

Initialisation D'abord, f est de classe C^p, donc différentiable et φ est linéaire donc différentiable. Donc la composée est différentiable et le théorème 12.140 nous donne la différentiabilité de $\varphi \circ f$ ainsi que la formule

$$d(\varphi \circ f)_a(u) = d\varphi_{f(a)}\big(df_a(u)\big) = (\varphi \circ df_a)(u) = \varphi_1(df_a)(u). \tag{12.356}$$

Donc $d(\varphi \circ f)_a = \varphi_1(df_a)$, ce qui signifie

$$d(\varphi \circ f) = \varphi_1 \circ df. \tag{12.357}$$

C'est bon pour $k = 1$.

La pas de récurrence Vu que f est de classe C^p, $d^k f$ est encore différentiable. Vu que φ_k est encore linéaire, nous pouvons encore utiliser la règle de différentiation de fonctions composées sur l'application $\varphi_k \circ d^k f$. Nous avons :

$$d^{k+1}(\varphi \circ f)_a(u) = d\big(d^k(\varphi \circ f)\big)_a(u) = d(\varphi_k \circ d^k f)_a(u). \tag{12.358}$$

C'est le moment d'utiliser la formule de différentiation en chaîne :

$$d^{k+1}(\varphi \circ f)_a(u) = \big((d\varphi_k)_{d^k f_a} \circ d^{k+1} f_a\big)(u). \tag{12.359}$$

Mais φ_k étant linéaire, $(d\varphi_k)_{d^k f_a} = \varphi_k$, donc

$$d^{k+1}(\varphi \circ f)_a(u) = (\varphi_k \circ d^{k+1} f_a)(u). \tag{12.360}$$

Donc, en oubliant l'application au vecteur u,

$$d^{k+1}(\varphi \circ f)_a = \varphi_k \circ d^{k+1} f_a = \varphi_{k+1}\big(d^{k+1} f_a\big) = (\varphi_{k+1} \circ d^{k+1} f)(a). \tag{12.361}$$

Nous avons donc bien

$$d^{k+1}(\varphi \circ f) = \varphi_{k+1} \circ d^{k+1} f. \tag{12.362}$$

□

Lemme 12.143.
Si $f\colon U \to V$ est un difféomorphisme[43] *alors pour tout $a \in U$, l'application df_a est inversible et*

$$(df_a)^{-1} = (df^{-1})_{f(a)}. \tag{12.363}$$

Démonstration. Il suffit d'apercevoir qu'en vertu de la règle de différentiation en chaîne (12.332),

$$(df_a)(df^{-1})_{f(a)} = d(f \circ f^{-1})_{f(a)} = \mathrm{Id}\,. \tag{12.364}$$

□

Proposition 12.144.
Soient des ouverts A de $\mathbb{R}^p$ et B de $\mathbb{R}^m$. Si il existe un difféomorphisme $f\colon A \to B$, alors $p = m$.

Démonstration. Vu que f est un difféomorphisme, le lemme 12.143 fait son travail : l'application linéaire $df_a\colon \mathbb{R}^p \to \mathbb{R}^m$ est inversible d'inverse $df^{-1}_{f(a)}\colon \mathbb{R}^m \to \mathbb{R}^m$.

Or une application linéaire ne peut pas être bijective entre espaces de dimensions différentes (finies). Donc $p = m$. □

12.9.5 Différentiation de produit

Si nous avons deux application $f\colon E \to V$ et $g\colon E \to W$, alors nous voudrions considérer la fonction

$$\begin{aligned} f \otimes g\colon E &\to V \otimes W \\ a &\mapsto f(a) \otimes g(a). \end{aligned} \tag{12.365}$$

Le problème avec cette notation est que très souvent, les applications f et g sont des éléments d'espaces vectoriels. Si par exemple $f \in \mathcal{L}(E, V)$ et $g \in \mathcal{L}(E, W)$, nous avons $f \otimes g \in \mathcal{L}(E, V) \otimes \mathcal{L}(E, W)$. Dans le Frido nous ne nous permettons pas de dire calmement que $\mathcal{L}(E, V) \otimes \mathcal{L}(E, W) = \mathcal{L}(E, V \otimes W)$. Et je ne vous dit même pas à quel point il n'est pas évident, si $f \in C^\infty(E, V)$ et $g \in C^\infty(E, W)$ que nous aurions $f \otimes g \in C^\infty(E, V) \otimes C^\infty(E, W) = C^\infty(E, V \otimes W)$.

Tout cela pour dire que nous n'allons pas nous lancer dans des abus de notations. Non. Au lieu de cela, nous introduisons une notation. Pour rappel, dans tout le Frido, $\mathrm{Fun}(A, B)$ désigne l'ensemble de toutes les application de A vers B sans suppositions de régularité. Pour les puristes, nous précisions que si $f \in \mathrm{Fun}(A, B)$, nous supposons que f est définie sur tout A. hum . . . sauf mention du contraire.

Définition 12.145.
Si $f \in \mathrm{Fun}(E, V)$ et $g \in \mathrm{Fun}(E, W)$, alors nous définissons

$$\begin{aligned} f\tilde{\otimes}g\colon E &\to V \otimes W \\ a &\mapsto f(a) \otimes g(a). \end{aligned} \tag{12.366}$$

Proposition 12.146.
Soient des applications continues $f\colon E \to V$ et $g\colon E \to W$ entre espaces vectoriels de dimension finies. Alors la fonction $f\tilde{\otimes}g\colon E \to V \otimes W$ est continue.

Démonstration. Soit $a \in E$ et une suite $x_k \to a$ dans E. Nous voulons prouver que $f\tilde{\otimes}g(x_k) \xrightarrow{V\otimes W} f(a) \otimes g(a)$. Nous avons :

$$\|f(x_k)\otimes g(x_k) - f(a)\otimes g(a)\| \leqslant \|f(x_k)\otimes g(x_k) - f(x_k)\otimes g(a)\| + \|f(x_k)\otimes g(a) - f(a)\otimes g(a)\|. \tag{12.367}$$

Ensuite en utilisant la classe d'équivalence (12.253b),

$$f(x_k) \otimes g(x_k) - f(x_k) \otimes g(a) = f(x_k) \otimes \big(g(x_k) - g(a)\big), \tag{12.368}$$

43. Définition 12.1

et en ce qui concerne les normes,

$$\|f(x_k)\otimes g(x_k)-f(x_k)\otimes g(a)\| = \|f(x_k)\|\otimes\big(g(x_k)-g(a)\big)\|. \tag{12.369}$$

Mais par hypothèse, $f(x_k)\to f(a)$ et $g(x_k)\to g(a)$. Donc le tout tend vers zéro lorsque $k\to\infty$.

Le même raisonnement fonctionne avec le second terme de (12.367). □

Lorsque nous parlons de différentielle de produit de fonctions, nous voulons étudier la différentiabilité de $f\tilde{\otimes}g$ sous l'hypothèse de différentiabilité de f et g. Et aussi, si f et g sont de classe C^p, est-ce que $f\tilde{\otimes}g$ est également de classe C^p ?

Nous voudrions avoir une formule du type

$$d(f\tilde{\otimes}g) = df\tilde{\otimes}g + f\tilde{\otimes}dg, \tag{12.370}$$

mais ça ne colle pas au niveau des espaces. En effet, en évaluant cela en $a\in E$, nous avons à gauche $d(f\tilde{\otimes}g)_a\in\mathcal{L}(E,V\otimes W)$, tandis qu'à droite nous avons $df_a\otimes g(a)\in\mathcal{L}(E,V)\otimes W$ et $f(a)\otimes dg_a\in V\otimes\mathcal{L}(E,W)$.

Nous pourrions bien entendu dire que $V\otimes\mathcal{L}(E,W)$ est isomorphe à $\mathcal{L}(E,V\otimes W)$ et hop voila, on n'en parle plus. Ce serait passer sur deux points importants. D'abord est-ce que $V\otimes\mathcal{L}(E,W)$ est vraiment isomorphe à $\mathcal{L}(E,V\otimes W)$? Et ensuite, l'isomorphisme implique une utilisation du théorème 12.140 qui est tout sauf une trivialité.

Bref, fidèle au principe fridesque de ne pas cacher des difficultés techniques sous des abus de notations, nous allons écrire les choses explicitement.

Lemme 12.147.
Si E, V et W sont de dimension finie, les applications

$$\begin{aligned}\psi\colon \mathcal{L}(E,V)\otimes W &\to \mathcal{L}(E,V\otimes W)\\ f\otimes w &\mapsto \Big(u\mapsto f(u)\otimes w\Big)\end{aligned} \tag{12.371}$$

et

$$\begin{aligned}\varphi\colon V\otimes\mathcal{L}(E,W) &\to \mathcal{L}(E,V\otimes W)\\ v\otimes g &\mapsto \big(a\mapsto v\otimes g(a)\big).\end{aligned} \tag{12.372}$$

sont des isomorphismes d'espaces vectoriels.

Dans le meilleur des mondes, ces applications devraient être affublés d'indices V et W.

Démonstration. Nous donnons des détails à propos de ψ. Pour φ c'est la même chose.

Linéaire La formule (12.371) définit ψ en particulier sur une base de $\mathcal{L}(E,V)\otimes W$ par la proposition 12.127(1). Ce que signifie réellement la formule (12.371) est que ψ est ainsi définie sur la base et est prolongée par continuité.

Injective Si pour un f et un w fixé nous avons $\psi(f\otimes w)=0$, alors il y a deux cas : soit $w=0$ soit $w\neq 0$. Dans le premier cas, $f\otimes w=0$, et dans le second cas, nous remarquons que

$$0=\psi(f\otimes w)(a)=f(a)\otimes w \tag{12.373}$$

pour tout $a\in E$. Cela implique $f(a)=0$ pour tout a et donc $f=0$, ce qui signifie que $f\otimes w=0$.

Bijective En utilisant la proposition 12.127 et le lemme 4.34(2), nous avons égalité des dimensions entre $\mathcal{L}(E,V)\otimes W$ et $\mathcal{L}(E,V\otimes W)$.

Une application linéaire injective entre deux espaces vectoriels de même dimension (finie) est une bijection.

□

Proposition 12.148.
Soient des espaces vectoriels normés de dimension finie. Soient $f\colon E \to V$ et $g\colon E \to W$ des fonctions de classe C^1. Alors $f\tilde{\otimes}g\colon E \to V \otimes W$ est de classe C^1 nous avons les formules

$$d(f\tilde{\otimes}g)_a(u) = df_a(u) \otimes g(a) + f(a) \otimes dg_a(u) \tag{12.374}$$

ainsi que

$$d(f\tilde{\otimes}g) = \psi \circ (df\tilde{\otimes}g) + \varphi \circ (f\tilde{\otimes}dg). \tag{12.375}$$

Démonstration. Nous commençons par prouver que $f\tilde{\otimes}g$ est différentiable en injectant le candidat (12.374) dans la définition. Au numérateur nous avons :

$$(f\tilde{\otimes}g)(a+h) - (f\tilde{\otimes}g)(a) - df_a(h) \otimes g(a) - f(a) \otimes dg_a(h). \tag{12.376}$$

Le lemme 12.136 assure qu'il existe une fonction $\alpha\colon E \to V$ telle que $\lim_{h\to 0} \alpha(h)/\|h\|$ et $f(a+h) + f(a) + df_a(h) + \alpha(h)$. Même chose pour g. Nous avons donc

$$(f\tilde{\otimes}g)(a+h) = f(a+h) \otimes g(a+h) = \big(f(a) + df_a(h) + \alpha(h)\big) \otimes \big(g(a) + dg_a(h) + \beta(h)\big) \tag{12.377}$$

qui se développe en 9 termes. En effectuant les différences dans (12.376), nous nous retrouvons avec un numérateur qui vaut

$$f(a)\otimes\beta(h) + df_a(h)\otimes dg_a(h) + df_a(h)\otimes\beta(h) + \alpha(h)\otimes g(a) + \alpha(h)\otimes dg_a(h) + \alpha(h)\otimes\beta(h). \tag{12.378}$$

Nous pouvons prouver terme à terme qu'en divisant par $\|h\|$ nous avons une limite qui vaut zéro. Par exemple,

$$\lim_{h\to 0} \frac{f(a)\otimes\beta(h)}{\|h\|} \tag{12.379}$$

se calcule en prenant la norme du numérateur et en utilisant le lemme 12.130 :

$$\frac{\|f(a)\otimes\beta(h)\|}{\|h\|} = \frac{\|f(a)\|\|\beta(h)\|}{\|h\|} \to 0. \tag{12.380}$$

Tous les termes contenant $\alpha(h)$ ou $\beta(h)$ se traitent de la même manière. Le dernier terme à traiter est

$$\lim_{h\to 0} \frac{df_a(h)\otimes dg_a(h)}{\|h\|}. \tag{12.381}$$

En prenant la norme du numérateur, en utilisant encore le lemme 12.130 et en utilisant le lemme 12.17, nous avons

$$\|df_a(h)\otimes dg_a(h)\| = \|df_a(h)\|\|dg_a(h)\| \leqslant \|df_a\|\|dg_a\|\|h\|^2, \tag{12.382}$$

donc

$$\lim_{h\to 0} \frac{df_a(h)\otimes dg_a(h)}{\|h\|} = 0. \tag{12.383}$$

Notons que l'utilisation du lemme 12.17 requière que df_a soit continue, ce qui n'est pas évident en dimension infinie : une application linéaire n'est pas spécialement continue. C'est donc ici que nous utilisons le fait que E, V et W sont de dimension finie [44].

Ceci prouve que $f\tilde{\otimes}g$ est différentiable et nous donne la formule (12.374) pour appliquer sa différentielle à un élément de E. La formule (12.375) est un corollaire : elle se vérifie en l'appliquant à a puis à u.

Pour terminer nous devons prouver que $d(f\tilde{\otimes}g)$ est continue. Vu que f et g sont de classe C^1, les applications f, g, df et dg sont continues. Les applications ψ et φ sont également continues parce que linéaires sur des espaces de dimensioy finie. La proposition 12.146 appliquée à df et g montre que $df\tilde{\otimes}g$ est continue. La composition avec ψ qui est linéaire conserve la continuité.

Dons le membre de droite de (12.375) est continu et $f\tilde{\otimes}g$ est a une différentielle continue. Elle est donc de classe C^1. □

44. Il y a surement moyen de paufiner, et d'affaiblir cette hypothèse, mais je ne me lance pas là-dedans.

Il est temps de démontrer le truc difficile, à savoir que si f et g sont de classe C^p, alors $f\tilde{\otimes}g$ est également de classe C^p.

Proposition 12.149.
Nous applellons P_k la propriété suivante :

> *Pour tout $p \geqslant k$, pour tout espaces vectoriels normés E, V, W de dimension finies et pour toutes applications $f\colon E \to V$ et $g\colon E \to W$ de classe C^k, la fonction $f\tilde{\otimes}g$ est de classe C^k.*

(1) La propriété P_k est vraie pour tout k.

(2) Si $f\colon E \to V$ et $g\colon E \to W$ sont de classe C^p, alors $f\tilde{\otimes}g\colon E \to V \otimes W$ est de classe C^p.

Démonstration. Le gros de la preuve est le point (1). Le point (2) est alors une utilisation de la propriété P_p avec $p = k$.

Pour $k = 0$. Si f et g sont de classe C^p avec $p \geqslant k$, alors f et g sont a fortiori continues. La proposition 12.146 montre alors que $f\tilde{\otimes}g$ est continue.

Bien que ce ne soit pas tout à fait nécessaire, nous prouvons que P_1 est également vraie avant de passer à la récurrence. Si f et g sont de classe C^p avec $p \geqslant 1$, alors elles sont de classe C^1 et la proposition 12.148 s'applique : $f\tilde{\otimes}g$ est de classe C^1.

Nous faisons la récurrence en supposant que P_k est vraie, et en prouvant que P_{k+1} est vraie. Soit $p \geqslant k+1$ ainsi que des applications $f\colon E \to V$ et $g\colon E \to W$ de classe C^{k+1}. La proposition 12.148 dit que $f\tilde{\otimes}g$ est de classe C^1 et que

$$d(f\tilde{\otimes}g) = \psi \circ (df\tilde{\otimes}g) + \varphi \circ (f\tilde{\otimes}dg). \tag{12.384}$$

À droite, df et g sont de classe C^k parce que f et g sont de classe C^{k+1}. Donc $df\tilde{\otimes}g$ est de classe C^k par l'hypothèse de récurrence appliquée aux espaces $\mathcal{L}(E, V)$ et W. La proposition 12.142 nous assure alors que $\psi \circ (df\tilde{\otimes}g)$ est de classe C^k également.

Nous avons prouvé que $d(f\tilde{\otimes}g)$ est de classe C^k, donc $f\tilde{\otimes}g$ est de classe C^{k+1}. Cela nous fait la récurrence. □

12.9.6 Formule des accroissements finis

Proposition 12.150.
Soient $a < b$ dans $\mathbb{R}$ et deux fonctions

$$f\colon [a, b] \to E \tag{12.385a}$$
$$g\colon [a, b] \to \mathbb{R} \tag{12.385b}$$

continues sur $[a, b]$ et dérivables sur $]a, b[$. Si pour tout $t \in]a, b[$ nous avons $\|f'(t)\| \leqslant g'(t)$ alors

$$\|f(b) - f(a)\| \leqslant g(b) - g(a). \tag{12.386}$$

Démonstration. Soit $\epsilon > 0$ et la fonction

$$\begin{aligned} \varphi_\epsilon\colon [a, b] &\to \mathbb{R} \\ t &\mapsto \|f(t) - f(a)\| - g(t) - \epsilon t. \end{aligned} \tag{12.387}$$

Cela est une fonction continue réelle à variable réelle. En particulier pour tout $u \in]a, b[$ la fonction φ_ϵ est continue sur le compact $[u, b]$ et donc y atteint son minimum en un certain point $c \in [u, b]$; c'est le bon vieux théorème de Weierstrass 7.99. Nous commençons par montrer que pour tout u, ledit minimum ne peut être que b. Pour cela nous allons montrer que si $t \in [u, b[$, alors $\varphi_\epsilon(s) < \varphi_\epsilon(t)$ pour un certain $s > t$. Par continuité si s est proche de t nous avons

$$\left\| \frac{f(s) - f(t)}{s - t} \right\| - \frac{\epsilon}{2} < \|f'(t)\| < g'(t) + \frac{\epsilon}{2} = \frac{g(s) - g(t)}{s - t} + \frac{\epsilon}{2}. \tag{12.388}$$

Ces inégalités proviennent de la limite

$$\lim_{s\to t}\frac{f(s)-f(t)}{s-t}=f'(t),\tag{12.389}$$

donc si s et t sont proches,

$$\left\|\frac{f(s)-f(t)}{s-t}-f'(t)\right\|\tag{12.390}$$

est petit. Si $s>t$ nous pouvons oublier des valeurs absolues et transformer l'inégalité en

$$\|f(s)-f(t)\|<g(s)-g(t)+\epsilon(s-t).\tag{12.391}$$

Utilisant cela et l'inégalité triangulaire,

$$\begin{aligned}\varphi_\epsilon(s)&\leqslant\|f(s)-f(t)\|+\|f(t)-f(a)\|-g(s)-\epsilon s&(12.392a)\\&\leqslant g(s)-g(t)+\epsilon s-\epsilon t+\|f(t)-f(a)\|-g(s)-\epsilon s&(12.392b)\\&=\varphi_\epsilon(t).&(12.392c)\end{aligned}$$

Donc nous avons bien $\varphi_\epsilon(s)<\varphi_\epsilon(t)$ avec l'inégalité stricte. Par conséquent pour tout $u\in\ ]a,b[$ nous avons $\varphi_\epsilon(b)<\varphi_\epsilon(u)$ et en prenant la limite $u\to a$ nous avons

$$\varphi_\epsilon(b)\leqslant\varphi_\epsilon(a).\tag{12.393}$$

Cette inégalité donne immédiatement

$$\|f(b)-f(a)\|\leqslant g(b)-g(a)+\epsilon(b-a)\tag{12.394}$$

pour tout $\epsilon>0$ et donc

$$\|f(b)-f(a)\|\leqslant g(b)-g(a).\tag{12.395}$$

□

Théorème 12.151 (Théorème des accroissements finis)**.**
Soient E et F des espaces vectoriels normés, U ouvert dans E et une application différentiable $f\colon U\to F$. Pour tout segment $[a,b]\subset U$ nous avons

$$\|f(b)-f(a)\|\leqslant\left(\sup_{x\in[a,b]}\|df_x\|\right)\|b-a\|.\tag{12.396}$$

Démonstration. Nous prenons les applications

$$\begin{aligned}k\colon[0,1]&\to E\\t&\mapsto f\big((1-t)a+tb\big)\end{aligned}\tag{12.397}$$

et

$$\begin{aligned}g\colon[0,1]&\to\mathbb{R}\\t&\mapsto t\sup_{x\in[a,b]}\|df_x\|\|b-a\|.\end{aligned}\tag{12.398}$$

Pour tout t nous avons $g'(t)=M\|b-a\|$ où il n'est besoin de dire ce qu'est M. D'un autre côté nous avons aussi

$$\begin{aligned}k'(t)&=\lim_{\epsilon\to0}\frac{f\big((1-t-\epsilon)a+(t+\epsilon)b\big)-f\big((1-t)a+tb\big)}{\epsilon}\\&=\frac{d}{d\epsilon}\Big[f\big((1-t)a+tb+\epsilon(b-a)\big)\Big]_{\epsilon=0}\\&=df_{(1-t)a+tb}(b-a)\end{aligned}\tag{12.399}$$

où nous avons utilisé l'hypothèse de différentiabilité de f sur $[a,b]$ et donc en $(1-t)a+tb$. Nous avons donc

$$\|k'(t)\| \leqslant \|b-a\|\|df_{(1-t)a+tb}\| \leqslant M\|b-a\| = g'(t) \tag{12.400}$$

La proposition 12.150 est donc utilisable et

$$\|k(1)-k(0)\| = g(1)-g(0), \tag{12.401}$$

c'est-à-dire

$$\|f(b)-f(a)\| = M\|b-a\| \tag{12.402}$$

comme il se doit. □

Proposition 12.152.
Soient E et F des espaces vectoriels normés, U ouvert dans E et une application $f\colon U \to F$. Soient $a,b \in U$ tels que $[a,b] \subset U$. Nous posons $u = (b-a)/\|b-a\|$ et nous supposons que pour tout $x \in [a,b]$, la dérivée directionnelle

$$\frac{\partial f}{\partial u}(x) = \frac{d}{dt}\Big[f(x+tu)\Big]_{t=0} \tag{12.403}$$

existe. Nous supposons de plus que $\frac{\partial f}{\partial u}(x)$ est continue en $x=a$. Alors

$$\|f(b)-f(a)\| \leqslant \left(\sup_{x\in[a,b]} \|\frac{\partial f}{\partial u}(x)\|\right)\|b-a\|. \tag{12.404}$$

Démonstration. Nous posons évidemment

$$M = \sup_{x\in[a,b]} \|\frac{\partial f}{\partial u}(x)\| \tag{12.405}$$

et nous considérons les fonctions

$$k(t) = f\big((1-t)a+tb\big) \tag{12.406}$$

et

$$g(t) = tM\|b-a\|. \tag{12.407}$$

Pour alléger les notations nous posons $x = (1-t)a+tb$ et nous calculons avec un petit changement de variables dans la limite :

$$k'(t) = \frac{d}{d\epsilon}\Big[f\big(x+\epsilon(b-a)\big)\Big]_{\epsilon=0} = \|b-a\|\frac{d}{d\epsilon}\Big[f\big(x+\frac{\epsilon}{\|b-a\|}(b-a)\big)\Big]_{\epsilon=0} = \|b-a\|\frac{\partial f}{\partial u}(x), \tag{12.408}$$

et donc encore une fois nous avons

$$\|k'(t)\| \leqslant g'(t), \tag{12.409}$$

ce qui donne

$$\|k(1)-k(0)\| = g(1)-g(0), \tag{12.410}$$

c'est-à-dire

$$\|f(b)-f(a)\| \leqslant \sup_{x\in[a,b]} \|\frac{\partial f}{\partial u}(x)\|\|b-a\|. \tag{12.411}$$

□

Théorème 12.153.
Soient E,V deux espaces vectoriels normés, une application $f\colon E \to V$, un point $a \in E$ tel que pour tout $u \in E$, la dérivée

$$\frac{d}{dt}\Big[f(x+tu)\Big]_{t=0} \tag{12.412}$$

existe pour tout $x \in B(a,r)$ et est continue (par rapport à x) en $x = a$. Nous supposons de plus que

$$\frac{\partial f}{\partial u}(a) = 0 \tag{12.413}$$

pour tout $u \in E$. Alors f est différentiable en a et

$$df_a = 0 \tag{12.414}$$

Démonstration. Soit $\epsilon > 0$. Pourvu que $\|h\|$ soit assez petit pour que $a + h \in B(a,r)$, la proposition 12.152 nous donne

$$\|f(a+h) - f(a)\| \leqslant \sup_{x\in[a,a+h]} \|\frac{\partial f}{\partial u}(x)\||h| \tag{12.415}$$

où $u = h/\|h\|$. Par continuité de $\partial_u f(x)$ en $x = a$ et par le fait que cela vaut 0 en $x = a$, il existe un $\delta > 0$ tel que si $\|h\| < \delta$ alors

$$\|\frac{\partial f}{\partial u}(a+h)\| \leqslant \epsilon. \tag{12.416}$$

Pour de tels h nous avons

$$\|f(a+h) - f(a)\| \leqslant \epsilon\|h\|, \tag{12.417}$$

ce qui prouve que l'application linéaire $T(u) = 0$ convient parfaitement pour faire fonctionner la définition 12.133. □

12.9.7 Applications multilinéaires

Nous avons déjà parlé d'applications multilinéaires dans la définition 12.51.

Lemme 12.154 (Leibnitz pour les formes bilinéaires[193])**.**
Si $B\colon E \times F \to G$ est bilinéaire et continue, elle est C^∞ et

$$dB_{(x,y)}(u,v) = B(x,v) + B(u,y). \tag{12.418}$$

Démonstration. D'abord le membre de droite de (12.418) est une application linéaire et continue, donc c'est un bon candidat à être différentielle. Nous allons prouver que ça l'est, ce qui prouvera la différentiabilité de B. Avec ce candidat, le numérateur de la définition (12.133) s'écrit dans notre cas

$$B\big((x,y)+(u,v)\big) - B(x,y) - B(x,v) - B(u,y) = B(u,v). \tag{12.419}$$

Il reste à voir que

$$\lim_{(u,v)\to(0,0)} \frac{B(u,v)}{\|(u,v)\|} = 0 \tag{12.420}$$

Par l'équation (12.106) nous avons

$$\frac{\|B(u,v)\|}{\|(u,v)\|} \leqslant \frac{\|B\|\|u\|\|v\|}{\|u\|} = \|B\|\|v\| \tag{12.421}$$

parce que $\|(u,v)\| \geqslant \|u\|$. À partir de là il est maintenant clair que

$$\lim_{(u,v)\to(0,0)} \frac{\|B(u,v)\|}{\|(u,v)\|} = 0, \tag{12.422}$$

ce qu'il fallait. □

Proposition 12.155 (Règle de Leibnitz[193])**.**
Soient E, F_1, F_2 des espaces vectoriels normés, U ouvert dans E et des applications de classe C^r ($r \geqslant 1$)

$$f_1\colon U \to F_1 \tag{12.423a}$$
$$f_2\colon U \to F_2 \tag{12.423b}$$
$$\tag{12.423c}$$

et $B \in L(F_1 \times F_2, G)$. Alors l'application

$$\begin{aligned} \varphi\colon U &\to G \\ x &\mapsto B\big(f_1(x), f_2(x)\big) \end{aligned} \tag{12.424}$$

est de classe C^r et

$$d\varphi_x(u) = \varphi\big((df_1)_x(u), f_2(x)\big) + \varphi\big(f_1(x), (df_2)_x(u)\big). \tag{12.425}$$

Démonstration. Par hypothèse B est continue (c'est la définition de l'espace L), et donc C^∞ par le lemme 12.154. Par ailleurs la fonction $f_1 \times f_2$ est de classe C^r parce que f_1 et f_2 le sont et parce que la proposition 12.139 le dit. L'application composée $B \circ (f_1 \times f_2)$ est donc également de classe C^r par le théorème 12.141.

Il ne nous reste donc qu'à prouver la formule 12.425. En utilisant la différentielle du produit cartésien [45] nous avons

$$f\big(B \circ (f_1 \times f_2)\big)_x(h) = dB_{(f_1\times f_2)(x)}\big((df_1)_x(h), (df_2)_x(h)\big). \tag{12.426}$$

Nous développons cela en utilisant le lemme 12.154 :

$$\begin{aligned} d\big(B \circ (f_1 \times f_2)\big)_x(h) &= dB_{\big(f_1(x),f_2(x)\big)}\big((df_1)_x(h), (df_2)_x(h)\big) && \text{(12.427a)} \\ &= B\big(f_1(x), (df_2)_x(h)\big) + B\big((df_1)_x(h), f_2(x)\big), && \text{(12.427b)} \end{aligned}$$

comme souhaité. □

12.9.8 Différentielle partielle

Définition 12.156 (Différentielle partielle)**.**
*Soient E, F et G des espaces vectoriels normés et une fonction $f\colon E \times F \to G$. Nous définissons sa **différentielle partielle** sur l'espace E par*

$$\begin{aligned} d_1 f_{(x_0,y_0)}\colon E &\to G \\ u &\mapsto \frac{d}{dt}\Big[f(x_0 + tu, y_0\Big]_{t=0}. \end{aligned} \tag{12.428}$$

La différentielle d_2 se définit de la même façon.

Proposition 12.157 ([193])**.**
Soient E_1, E_2 et F des espaces vectoriels normés, soit un ouvert $U \subset E_1 \times E_2$ et une fonction $f\colon U \to F$.

(1) Si f est différentiable alors les différentielles partielles existent et

$$d_1 f_{(x_0,y_0)}(u) = df_{(x_0,y_0)}(u, 0) \tag{12.429a}$$
$$d_2 f_{(x_0,y_0)}(v) = df_{(x_0,y_0)}(0, v) \tag{12.429b}$$

où $u \in E_1$ et $v \in E_2$.

(2) Si f est différentiable alors

$$df_{(x_0,y_0)}(u, v) = d_1 f_{(x,y_0)}(u) + d_2 f_{(x_0,y_0)}(v). \tag{12.430}$$

Démonstration. Nous posons $\alpha = (x_0, y_0) \in U$ et

$$\begin{aligned} j_\alpha^{(1)}\colon E_1 &\to E_1 \times E_2 \\ x &\mapsto (x, y_0). \end{aligned} \tag{12.431}$$

45. Proposition 12.139.

C'est une fonction de classe C^∞ et

$$(dj_\alpha^{(1)})_{x_0}(u) = \frac{d}{dt}\Big[j_\alpha^{(1)}(x_0+tu)\Big]_{t=0} = \frac{d}{dt}\Big[(x_0+tu,y_0)\Big]_{t=0} = (u,0). \tag{12.432}$$

D'autre part

$$\begin{aligned}(d_1f)_\alpha(u) &= \frac{d}{dt}\Big[f(x_0+tu,y_0)\Big]_{t=0} && \text{(12.433a)}\\ &= \frac{d}{dt}\Big[(f\circ j_\alpha^{(1)})(x_0+tu)\Big]_{t=0} && \text{(12.433b)}\\ &= \big(d(f\circ j_\alpha^{(1)})\big)_{x_0}(u). && \text{(12.433c)}\end{aligned}$$

À ce moment nous utilisons la règle des différentielles composées 12.141 pour dire que

$$(d_1f)_\alpha(u) = df_{j_\alpha^{(1)}(x_0)}\circ(dj_\alpha^{(1)})_{x_0}(u) = df_\alpha(u,0). \tag{12.434}$$

Voila qui prouve déjà le point (1).

Pour la suite nous considérons les fonctions

$$\begin{aligned}P_1(x,y)&=x, & J_1(u)&=(u,0),\\ P_2(x,y)&=y, & J_2(v)&=(0,v)\end{aligned} \tag{12.435}$$

et nous avons l'égalité évidente

$$J_1\circ P_1 + J_2\circ P_2 = \mathbb{1} \tag{12.436}$$

sur $E_1\times E_2$. En appliquant df_α à cette dernière égalité, en appliquant à (u,v) et en utilisant la linéarité de df_α nous trouvons

$$\begin{aligned}df_\alpha(u,v) &= df_\alpha\big((J_1\circ P_1)(u,v)\big) + df_\alpha\big((J_2\circ P_2)(u,v)\big) && \text{(12.437a)}\\ &= df_\alpha(u,0)+df_\alpha(0,v) && \text{(12.437b)}\\ &= (d_1f)_\alpha(u)+(d_2f)_\alpha(v) && \text{(12.437c)}\end{aligned}$$

où nous avons utilisé le point (1) pour la dernière égalité. □

12.9.9 L'inverse, sa différentielle

Si E est un espace de Banach, nous sommes intéressés à l'espace $\mathrm{GL}(E)$ des endomorphismes inversibles de E sur E. Cet ensemble est métrique par la formule usuelle

$$\|T\| = \sup_{\|x\|=1}\|T(x)\|_E. \tag{12.438}$$

Proposition 12.158 (Thème 42)**.**
Soit E un espace de Banach (espace vectoriel normé complet). Si A est un endomorphisme de E satisfaisant $\|A\|<1$ pour la norme opérateur, alors $(\mathbb{1}-A)$ est inversible et son inverse est donné par

$$(\mathbb{1}-A)^{-1} = \sum_{k=0}^{\infty} A^k. \tag{12.439}$$

Démonstration. Étant donné que la norme opérateur est une norme algébrique (lemme 12.20), nous avons $\|A^k\|\leqslant\|A\|^k$. Par conséquent la série $\|A^k\|$ est majorée par la série géométrique qui converge [46]. Par conséquent $\sum_k A^k$ est une série absolument convergente et donc convergente par la proposition 12.62 et le fait que $\mathcal{L}(E)$ est complet (proposition 12.65).

46. Voir l'exemple 12.75.

Montrons à présent que la somme est l'inverse de $\mathbb{1} - A$ en utilisant le produit terme à terme autorisé par la proposition 12.40 :

$$\sum_{k=0}^{n} A^k(\mathbb{1} - A) = \sum_{k=0}^{n}(A^k - A^{k+1}) = \mathbb{1} - A^{n+1}. \tag{12.440}$$

Par conséquent

$$\|\mathbb{1} - \sum_{k=0}^{n} A^k(\mathbb{1} - A)\| = \|A^{n+1}\| \leqslant \|A\|^{n+1} \to 0. \tag{12.441}$$

□

Théorème 12.159 (Inverse dans GL(E)[194, 193])**.**
Soient E et F des espaces vectoriels normés.

(1) L'ensemble GL(E) *est ouvert dans* End(E).

(2) L'application inverse

$$\begin{aligned} i\colon \mathrm{GL}(E,F) &\to \mathrm{GL}(F,E) \\ u &\mapsto u^{-1} \end{aligned} \tag{12.442}$$

est de classe C^∞ et

$$di_{u_0}(h) = -u_0^{-1} \circ h \circ u_0^{-1} \tag{12.443}$$

pour tout $h \in \mathrm{End}(E)$

Démonstration. Nous supposons que GL(E,F) n'est pas vide, sinon ce n'est pas du jeu.

Cas de dimension finie Si la dimension de E et F est finie, elles doivent être égales, sinon il n'y a pas de fonctions inversibles $E \to F$. L'ensemble GL(E,F) est donc naturellement GL($n,\mathbb{R}$). Un élément de $\mathbb{M}(n,\mathbb{R})$ est dans GL($n,\mathbb{R}$) si et seulement si son déterminant est non nul. Le déterminant étant une fonction continue (polynomiale) en les entrées de la matrice, l'ensemble GL($n,\mathbb{R}$) est ouvert dans $\mathbb{M}(n,\mathbb{R})$.

Même idée pour la régularité de la fonction $i\colon \mathrm{GL}(n,\mathbb{R}) \to \mathrm{GL}(n,\mathbb{R})$, $X \mapsto X^{-1}$. Les entrées de X^{-1} sont les cofacteurs de X divisé par $\det(X)$, et donc des polynômes en les entrées de X divisés par un polynôme qui ne s'annule pas sur GL($n,\mathbb{R}$), et donc sur un ouvert autour de X et de X^{-1}. Bref, tout est C^∞.

Le reste de la preuve parle de la dimension infinie.

Ouvert autour de l'identité Nous commençons par prouver que $B(\mathbb{1},1) \subset \mathrm{GL}(E)$. Pour cela il suffit de remarquer que si $\|u\| < 1$ alors le lemme 12.158 nous donne un inverse de $(1+u)$ en la personne de $\sum_{k=0}^{\infty}(-u)^k$.

Ouvert en général Soit maintenant $u_0 \in \mathrm{GL}(E)$. Si $\|u\| < \frac{1}{\|u_0^{-1}\|}$ alors $\|u_0^{-1}u\| < 1$, ce qui signifie que

$$\mathbb{1} + u_0^{-1}u \tag{12.444}$$

est inversible. Mais $u_0 + u = u_0(\mathbb{1} + u_0^{-1}u)$, donc $u_0 + u \in \mathrm{GL}(E)$ ce qui signifie que

$$B\left(u_0, \frac{1}{\|u_0^{-1}\|}\right) \subset \mathrm{GL}(E). \tag{12.445}$$

Différentielle en l'identité Nous commençons par prouver que $di_{\mathbb{1}}(u) = -u$. Pour cela nous posons

$$\alpha(h) = \sum_{k=2}^{\infty}(-1)^k h^k \tag{12.446}$$

et nous calculons

$$di_{\mathbb{1}}(u) = \frac{d}{dt}\Big[i(\mathbb{1} + tu)\Big]_{t=0} = \frac{d}{dt}\Big[\mathbb{1} - tu + \alpha(tu)\Big]_{t=0}. \tag{12.447}$$

Il suffit de prouver que $\frac{d}{dt}\Big[\alpha(tu)\Big]_{t=0} = 0$ pour conclure que $di_{\mathbb{1}}(u) = -u$. Pour cela, nous remarquons que $\alpha(0) = 0$ et donc que

$$\frac{d}{dt}\Big[\alpha(tu)\Big]_{t=0} = \lim_{t\to 0}\frac{\alpha(tu)-\alpha(0)}{t} \tag{12.448a}$$

$$= \lim_{t\to 0}\sum_{k=2}^{\infty}(-1)^k\frac{(tu)^k}{t} \tag{12.448b}$$

$$= -\lim_{t\to 0} u\sum_{k=1}^{\infty}(-1)^k t^k u^k. \tag{12.448c}$$

La norme de ce qui est dans la limite est majorée par

$$\|u\|\sum_{k=1}^{\infty}\|tu\|^k = \|u\|\left(\frac{1}{1-\|tu\|}-1\right), \tag{12.449}$$

et cela tend vers zéro lorsque $t\to\infty$. Nous avons utilisé la somme 12.143 de la série géométrique. Nous avons bien prouvé que $di_{\mathbb{1}}(u) = -u$.

Différentielle en général Soit maintenant $u_0 \in \mathrm{GL}(E)$ et $h \in \mathrm{End}(E)$ tel que $u_0 + h \in \mathrm{GL}(E)$; par le premier point, il suffit de prendre $\|h\|$ suffisamment petit. Vu que $u_0+h = u_0(\mathbb{1}+u_0^{-1}h)$ nous avons

$$(u_0+h)^{-1} = (\mathbb{1}+u_0^{-1}h)^{-1}u_0^{-1}. \tag{12.450}$$

Nous pouvons donc calculer

$$(u_0+h)^{-1} = \big(\mathbb{1}-u_0^{-1}h+\alpha(u_0^{-1}h)\big)u_0^{-1} = u_0^{-1}-u_0^{-1}hu_0^{-1}+\alpha(u_0^{-1}h)u_0^{-1}, \tag{12.451}$$

et ensuite

$$di_{u_0}(h) = \frac{d}{dt}\Big[i(u_0+th)\Big]_{t=0} = \frac{d}{dt}\Big[u_0^{-1}-tu_0^{-1}hu_0^{-1}+\alpha(tu_0^{-1}h)u_0^{-1}\Big]_{t=0}, \tag{12.452}$$

mais nous avons déjà vu que

$$\frac{d}{dt}\Big[\alpha(th)\Big]_{t=0} = 0, \tag{12.453}$$

donc

$$di_{u_0}(h) = -u_0^{-1}hu_0^{-1} \tag{12.454}$$

Cela donne la différentielle de l'application inverse.

Continuité de l'inverse L'application i est continue parce que différentiable.

L'inverse est C^∞ Nous allons écrire la fonction inverse comme une composée. Soient les applications

$$\begin{aligned} B\colon L(F,E)\times L(F,E) &\to L\big(L(E,F),L(F,E)\big)\\ B(\psi_1,\psi_2)(A) &= -\psi_1\circ A\circ\psi_2 \end{aligned} \tag{12.455}$$

et

$$\begin{aligned} \Delta\colon L(F,E) &\to L(F,E)\times L(F,E)\\ \varphi &\mapsto (\varphi,\varphi) \end{aligned} \tag{12.456}$$

Nous avons alors

$$di = B\circ\Delta\circ i. \tag{12.457}$$

L'application Δ est de classe C^∞. Nous devons voir que B l'est aussi. Pour le voir nous commençons par prouver qu'elle est bornée :

$$\begin{aligned} \|B\| &= \sup_{\|\psi_1\|,\|\psi_2\|=1}\|B(\psi_1,\psi_2)\|_{\mathcal{L}\left(L(E,F),L(F,E)\right)}\\ &= \sup_{\|\psi_1\|,\|\psi_2\|=1}\sup_{\|A\|=1}\|\psi_1\circ A\circ\psi_2\|_{L(F,E)}\\ &\leqslant \sup_{\|\psi_1\|,\|\psi_2\|=1}\sup_{\|A\|=1}\|\psi_1\|\|A\|\|\psi_2\|\\ &\leqslant 1. \end{aligned} \tag{12.458}$$

Donc B est bien bornée et par conséquent continue. Une application bilinéaire continue est C^∞ par le lemme 12.154. La décomposition $di = B \circ \Delta \circ i$ nous donne donc que $i \in C^\infty$ dès que i est continue, ce que nous avions déjà montré.

□

12.10 Exponentielle de matrice

Proposition 12.160.
Soit V un espace vectoriel de dimension finie et $A \in \mathrm{End}(V)$. La série

$$\exp(A) = \mathbb{1} + A + \frac{A^2}{2} + \frac{A^3}{3} + \ldots = \sum_{k=1}^{\infty} \frac{A^k}{k!}. \tag{12.459}$$

*converge normalement dans $\big(\mathrm{End}(V), \|.\|_{op}\big)$. L'**exponentielle** de la matrice A est cette matrice.*

Démonstration. Vu que la norme opérateur est une norme d'algèbre par le lemme 12.20, nous avons pour tout k la majoration $\|A^k\| \leqslant \|A\|^k$. Nous avons donc

$$\sum_{k=0}^{\infty} \frac{\|A^k\|}{k!} \leqslant \sum_{k} \frac{\|A\|^k}{k!}. \tag{12.460}$$

La dernière somme converge en vertu de la convergence de la série exponentielle donnée en exemple 12.77. □

Étant donné que c'est une limite, il y a une question de convergence et donc de topologie. C'est pour cela que nous ne pouvions pas introduire l'exponentielle de matrice avant d'avoir introduit la norme des matrices. La convergence de la série pour toute matrice sera prouvée au passage dans la proposition 12.161.

La fonction exponentielle $x \mapsto e^x$ n'est pas un polynôme en x, mais nous avons le résultat marrant suivant.

Proposition 12.161.
Si u est un endomorphisme, alors $\exp(u)$ est un polynôme en u[47].

Démonstration. Nous considérons l'application

$$\begin{aligned} \varphi_u \colon \mathbb{K}[X] &\to \mathrm{End}(E) \\ P &\mapsto P(u) \end{aligned} \tag{12.461}$$

Étant donné que l'image de φ_u est un fermé dans $\mathrm{End}(E)$, il suffit de montrer que la série

$$\sum_{k=0}^{\infty} \frac{\varphi_u(X)^k}{k!} \tag{12.462}$$

converge dans $\mathrm{End}(E)$ pour qu'elle converge dans $\mathrm{Image}(\varphi_u)$. Pour ce faire nous nous rappelons de la norme opérateur[48] et de la propriété fondamentale $\|A^k\| \leqslant \|A\|^k$. En notant $A = \varphi_u(X)$,

$$\left\| \sum_{k=n}^{m} \frac{A^k}{k!} \right\| \leqslant \sum_{k=n}^{m} \frac{\|A^k\|}{k!} \leqslant \sum_{k=n}^{m} \frac{\|A\|^k}{k!}, \tag{12.463}$$

ce qui est une morceau du développement de $e^{\|A\|}$. La limite $n \to \infty$ est donc zéro par la convergence de l'exponentielle réelle. La suite des sommes partielles de e^A est donc de Cauchy. La série converge donc parce que nous sommes dans un espace vectoriel réel de dimension finie $(\mathrm{End}(E))$. □

47. Nan, mais j'te jure : exp n'est pas un polynôme, mais $\exp(u)$ est un polynôme de u.
48. Définition 12.10.

12.162.
Pourquoi $\exp(u)$ est-il un polynôme d'endomorphisme alors que exp n'est pas un polynôme ? Lorsque nous disons que la fonction $x \mapsto \exp(x)$ n'est pas un polynôme, nous sommes en train de localiser la fonction exp à l'intérieur de l'espace de toutes les fonctions $\mathbb{R} \to \mathbb{R}$, c'est-à-dire à l'intérieur d'un espace de dimension infinie. Au contraire lorsqu'on parle de $\exp(u)$ et qu'on le compare aux endomorphismes $P(u)$, nous sommes en train de repérer $\exp(u)$ à l'intérieur de l'espace des matrices qui est de dimension finie. Il n'est donc pas étonnant que l'on parvienne moins à faire la distinction.

Si par contre nous considérons exp en tant qu'application $\exp\colon \mathrm{End}(E) \to \mathrm{End}(E)$, ce n'est pas un polynôme.

Si u et v sont des endomorphismes, nous aurons des polynômes P et Q tels que $e^u = P(u)$ et $e^v = Q(v)$; mais nous n'aurons en général évidemment pas $P = Q$. En cela, exp n'est pas un polynôme.

12.11 Espace dual

Définition 12.163.
*Soit un espace vectoriel normé $(V, \|.\|)$ sur le corps $\mathbb{C}$ ou $\mathbb{R}$ (que nous nommons $\mathbb{K}$). Son **dual topologique**, noté V' est l'ensemble des applications linéaires continues $V \to \mathbb{K}$.*

12.11.1 Topologies

Il est possible de mettre sur V' (au moins) deux topologies distinctes. La première est la topologie de la norme opérateur ; rien de nouveau pour elle. La seconde est la topologie $*$-faible dont nous avons déjà un peu parlé dans la définition 9.81.

En termes de notations, nous allons noter les semi-normes de la topologie faible par

$$p_x(\varphi) = |\varphi(x)| \tag{12.464}$$

pour $x \in V$ et $\varphi \in V'$. À droite, les barres dénotent soit la valeur absolue (si $\mathbb{K} = \mathbb{R}$), soit le module (si $\mathbb{K} = \mathbb{C}$).

Lemme 12.164.
Soit $\varphi \in V'$ et $x \in V$. Alors

$$p_x(\varphi) \leqslant \frac{\|\varphi\|}{\|x\|}. \tag{12.465}$$

Si $\varphi_0 \in V'$, si $r > 0$ et si $x \in V$ nous avons aussi :

$$B(\varphi_0, r) \subset B_x(\varphi_0, \frac{r}{\|x\|}). \tag{12.466}$$

Démonstration. En posant $x' = x/\|x\|$ nous avons

$$p_x(\varphi) = |\varphi(x)| = \frac{1}{\|x\|}|\varphi(x')| \leqslant \frac{1}{\|x\|}\|\varphi\|. \tag{12.467}$$

En ce qui concerne la seconde affirmation, si $\varphi \in B(\varphi_0, r)$ alors en notant $x' = x/\|x\|$ nous avons :

$$p_x(\varphi_0 - \varphi) = |\varphi_0(x) - \varphi(x)| = \frac{1}{\|x\|}|\varphi_0(x') - \varphi(x')| \leqslant \frac{1}{\|x\|}\|\varphi_0 - \varphi\| \leqslant \frac{r}{\|x\|}. \tag{12.468}$$

Donc $\varphi \in B_x\big(\varphi_0, \frac{r}{\|x\|}\big)$. □

Proposition 12.165.
En ce qui concerne la convergence d'une suite (φ_k) dans V' mais si elle vérifie

$$\varphi_k \xrightarrow{\|.\|} \varphi \tag{12.469}$$

alors

$$\varphi_k \xrightarrow{*} \varphi. \tag{12.470}$$

Démonstration. Soit une suite (φ_k) dans V', convergente vers φ pour la topologie de la norme. Soit $x \in V$, et $x' = x/\|x\|$. Nous avons

$$p_x(\varphi_k - \varphi) = \frac{1}{\|x\|}|\varphi_k(x') - \varphi(x)| \leqslant \frac{1}{\|x\|}\|\varphi_k - \varphi\| \to 0. \tag{12.471}$$

□

Lemme 12.166.
La translation dans V' est une opération continue pour la topologie de la norme opérateur et pour celle de la topologie $*$.

Démonstration. Soit une suite φ_k tendant vers 0 ; nous devons prouver que $\tau_\sigma(\varphi_k) \to \tau_\sigma(0) = \sigma$. Et ce, pour chacune des deux topologies.

Norme opérateur L'hypothèse $\varphi_k \xrightarrow{\|.\|} 0$ signifie que $\|\varphi_k\| \to 0$, c'est-à-dire que

$$\sup_{\|v\|=1} |\varphi_k(v)| \to 0. \tag{12.472}$$

Nous avons alors

$$\|\tau_\sigma(\varphi_k) - \sigma\| = \sup_{\|v\|=1} |\tau_\sigma(\varphi_k)v - \sigma(v)| = \sup_{\|v\|=1} |\varphi_k(v)| \to 0. \tag{12.473}$$

Donc d'accord pour $\tau_\sigma(\varphi) \to \sigma$.

Topologie $*$ Nous supposons maintenant que $\varphi_k \xrightarrow{*} 0$. Pour tout $v \in V$ nous avons

$$p_v\big(\tau_\sigma(\varphi_k) - \sigma\big) = \big|\tau_\sigma(\varphi_k)v - \sigma(v)\big| = |\varphi_k(v)| = p_v(\varphi_k). \tag{12.474}$$

Mais par hypothèse, $p_v(\varphi_k) \to 0$.

□

Pour la suite, nous allons préfixer par N les concepts liés à la topologie de V' associée à la norme opérateur et par $*$, les concepts de la topologie $*$.

Proposition 12.167.
Soit un espace vectoriel normé V. Un $*$-ouvert et toujours un N-ouvert.

Démonstration. Soit un $*$-ouvert $\mathcal{O}$ de V'. Il existe donc $x \in V$ et $r > 0$ tels que $B_x(\varphi, r) \subset \mathcal{O}$. Nous avons alors, en utilisant le lemme 12.164,

$$B(\varphi, r\|x\|) \subset B_x(\varphi, r) \subset \mathcal{O}. \tag{12.475}$$

Donc $\mathcal{O}$ est un N-ouvert. □

Corollaire 12.168.
Soit un espace topologique X. Si $f\colon (V', *) \to X$ est continue, alors $f\colon (V', \|.\|) \to X$ est continue.

Démonstration. Soit un ouvert $\mathcal{O}$ de X. Vu que f est $*$-continue, la partie $f^{-1}(\mathcal{O})$ est un $*$-ouvert de V'. Il est onc un N-ouvert de V' par la proposition 12.167. □

12.11.2 Réflexivité

Pour la suite nous notons V'' le dual de $(V', \|.\|)$. Certes en tant qu'ensembles, $(V', *)$ et $(V', \|.\|)$ sont identiques, mais comme ils n'ont pas la même topologie, les duaux ne sont pas les mêmes.

Bref, V'' est l'ensemble des applications linéaires continues $(V', \|.\|) \to \mathbb{C}$. Et lorsque nous disons $\mathbb{C}$ ici, ça peut aussi bien être $\mathbb{R}$ selon le contexte.

De plus nous considérons que V'' la norme opérateur qui dérive de la norme de V', laquelle dérive de la norme vectorielle sur V.

Proposition-définition 12.169.
Soit un espace vectoriel normé V sur $\mathbb{R}$ ou $\mathbb{C}$. Nous considérons l'application

$$\begin{aligned} J\colon V &\to V'' \\ J(x)\varphi &= \varphi(x). \end{aligned} \tag{12.476}$$

(1) L'application J est bien définie : $J(x)$ est continue.

(2) L'application J est continue.

(3) Elle est injective.

*Lorsque J est bijective, l'espace V est dit **réflexif**.*

Démonstration. Point par point.

(1) Nous commençons par montrer que $J(x)\colon (V', \|.\|) \to \mathbb{C}$ est continue pour chaque $x \in V$. Soit une suite $\varphi_k \xrightarrow{\|.\|} 0$. Nous avons :

$$J(x)\varphi_k = \varphi_k(x) \leqslant \|\varphi_k\|\|x\| \to 0 \tag{12.477}$$

où vous aurez noté l'utilisation du lemme 12.17. Cela prouve que $J(x)$ est continue et donc que J est bien à valeurs dans V''.

(2) Soit une suite $x_k \xrightarrow{V} 0$, et étudions $\|J(x_k)\|$ pour la norme dans V''. Nous posons $x'_k = x_k/\|x_k\|$ et nous calculons (encore une fois, nous écrivons « $\mathbb{C}$ », mais ça pourrait être $\mathbb{R}$)

$$\|J(x_k)\| = \sup_{\|\varphi\|=1} |J(x_k)\varphi|_{\mathbb{C}} = \sup_{\|\varphi\|=1} |\varphi(x_k)| = \|x_k\| \sup_{\|\varphi\|=1} |\varphi(x'_k)| \leqslant \|x_k\| \to 0. \tag{12.478}$$

La dernière inégalité pourrait être sans doute une égalité [49], mais nous n'en avons pas besoin ici.

□

12.11.3 Module de continuité

Définition 12.170.
*Soient deux espaces topologiques normés X et Y, ainsi qu'une application $f\colon X \to Y$. Le **module de continuité** de f est la fonction*

$$\begin{aligned} \omega_f\colon \mathbb{R}^+ &\to \mathbb{R}^+ \cup \{\infty\} \\ h &\mapsto \sup_{\substack{x,y\in X \\ d_X(x,y)<h}} d_Y\big(f(x), f(y)\big). \end{aligned} \tag{12.479}$$

Nous définissons aussi $\omega_f(h) = 0$ pour $h \leqslant 0$.

Notons que le module de continuité est une fonction croissante.

Lemme 12.171.
Soit $f \in C^0\big([0,1], \mathbb{C}\big)$ et ω son module de continuité. Si λ et h sont strictement positifs avec $\lambda h \in [0,1]$ alors

$$\phi(\lambda h) \leqslant (\lambda + 1)\omega(h). \tag{12.480}$$

49. Écrivez moi si vous en êtes certain.

Démonstration. La fonction ω est décroissante, et pour $h, k > 0$ nous avons $\omega(h+k) \leqslant \omega(h)+\omega(k)$. Par récurrence pour tout $k \in \mathbb{N}$ nous avons

$$\omega(kh) \leqslant k\omega(h). \tag{12.481}$$

En écrivant cela pour $k = \lceil \lambda \rceil$, nous avons

$$\omega(\lambda h) \leqslant \omega(kh) \leqslant k\omega(h) \leqslant (\lambda + 1)\omega(h). \tag{12.482}$$

□

Lemme 12.172.
Une fonction est uniformément continue[50] *si et seulement si son module de continuité est continu en zéro*[51].

Démonstration. Nous commençons par supposer que f est uniformément continue. Soit $\epsilon > 0$. Par uniforme continuité, il existe $\delta > 0$ tel que $d\big(f(x), f(y)\big) \leqslant \epsilon$ dès que $d(x, y) \leqslant \delta$. Si $h \in B(0, \delta)$, alors

$$\omega_f(h) \leqslant \omega_f(\delta) = \sup_{\substack{x,y\in X \\ d(x,y)\leqslant\delta}} d\big(f(x), f(y)\big) \leqslant \epsilon. \tag{12.483}$$

Cela prouve que $\lim_{h\to 0} \omega_f(h) = 0$.

Dans l'autre sens, si $\epsilon > 0$ est fixé, il suffit de prendre δ tel que $\omega_f(h) \leqslant \epsilon$ pour tout $h \leqslant \delta$ pour faire fonctionner la définition de l'uniforme continuité. □

Lemme 12.173 ([195])**.**
Soient des espaces métriques E et E' et une suite de fonctions $(f_i)_{i\geqslant 0}$ qui converge uniformément vers f. Alors pour chaque $\delta > 0$ nous avons

$$\limsup_{i\to\infty} \omega_{f_i}(\delta) \leqslant \omega_f(\delta). \tag{12.484}$$

Démonstration. Soient $\delta > 0$ ainsi que $x, y \in E$ tels que $\|x - y\| \leqslant \delta$. Pour chaque i nous avons

$$\begin{aligned} |f_i(x) - f_i(y)| &\leqslant |f_i(x) - f(x)| + |f(x) - f(y)| + |f(y) - f_i(y)| && \text{(12.485a)} \\ &\leqslant |f(x) - f(y)| + 2\|f_i - f\|_\infty && \text{(12.485b)} \\ &\leqslant \omega_f(\delta) + 2\|f_i - f\|_\infty. && \text{(12.485c)} \end{aligned}$$

Nous prenons le supremum de cela sur $\{x, y \in E \text{ tel que } \|x - y\| \leqslant \delta\}$ pour obtenir :

$$\omega_{f_i}(\delta) \leqslant \omega_f(\delta) + 2\|f_i - f\|_\infty. \tag{12.486}$$

La tentation est grande à ce point de prendre la limite des deux côtés pour $i \to \infty$. Cependant, rien ne nous permet de dire que la suite $i \mapsto \omega_{f_i}(\delta)$ ait une limite. Nous pouvons cependant prendre la limite supérieures[52] et obtenir

$$\limsup_{i\to\infty} \omega_{f_i}(\delta) \leqslant \omega_f(\delta). \tag{12.487}$$

□

50. Définition 9.71.
51. Dans ce lemme, nous avons deux espaces métriques, mais nous allons noter d la distance des deux côtés.
52. Définition 8.26.

12.12 Mini introduction aux nombres p-adiques

12.12.1 La flèche d'Achille

C'est un grand classique que je donne ici juste comme introduction pour montrer que des séries infinies peuvent donner des nombres finis de manière tout à fait intuitive.

Achille tire une flèche vers un arbre situé à 10 m de lui. Disons que la flèche avance à une vitesse constante de 1 m/s. Il est clair que la flèche mettra 10 s pour toucher l'arbre. En 5 s, elle aura parcouru la moitié de son chemin. On le note :

$$\text{temps} = 5s + \dots$$

Reste 5 m à faire. En 2.5 s, elle aura fait la moitié de ce chemin chemin, soit $2.5m = \frac{10}{4}m$. On le note :

$$\text{temps} = \frac{10}{2}s + \frac{10}{4}s+$$

Reste $2.5m$ à faire. La moitié de ce trajet, soit $\frac{10}{8}m$, est parcouru en $\frac{10}{8}s$; on le note encore, mais c'est la dernière fois !

$$\text{temps} = \frac{10}{2}s + \frac{10}{4}s + \frac{10}{8}s+$$

En continuant ainsi à regarder la flèche qui parcours des demi-trajets puis des moitiés de demi-trajets et encore des moitiés de moitiés de demi-trajets, et en sachant que le temps total est $10s$, on trouve :

$$10\left(\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \dots\right) = 10.$$

On doit donc croire que la somme jusqu'à l'infini des inverses des puissances de deux vaut 1 :

$$\sum_{n=1}^{\infty} \frac{1}{2^n} = 1.$$

Cela peut être démontré à la loyale.

12.12.2 La tortue et Achille

Maintenant qu'on est convaincu que des sommes infinies peuvent représenter des nombres tout à fait normaux, passons à un truc plus marrant.

Achille, qui marche peinard à 10 m/h, part avec $1m$ d'avance sur une tortue qui avance à 1 m/h. Le temps que la tortue arrive au point de départ d'Achille, Achille aura parcouru $10m$, et le temps que la tortue mettra pour arriver à ce point, eh bien, Achille ne sera déjà plus là : il sera à $100m$. Si la tortue tient bon pendant un temps infini, et si l'on est confiant en le genre de raisonnements faits à la section 12.12.1, elle rattrapera Achille dans

$$1m + 10m + 100m + 1000m + \dots$$

Autant dire que ça ne risque pas d'arriver. Et pourtant, mettons en équations :

$$\begin{cases} x_{\text{Achile}}(t) = 1 + 10t & \text{(12.488a)} \\ x_{\text{tortue}}(t) = t. & \text{(12.488b)} \end{cases}$$

La tortue rejoint Achille au temps t tel que $x_{\text{Achille}(t)} = x_{\text{tortue}}(t)$. Un mini calcul donne $t = -1/9$. Physiquement, c'est une situation logique. Peut-on en déduire une égalité mathématique du style de

$$1 + 10 + 100 + 1000 + \dots = -\frac{1}{9} \text{ ???}$$

Là où les choses deviennent jolies, c'est quand on cherche à voir ce que peut bien être la valeur d'un hypothétique $x = 1 + 10 + 100 + 1000 + \ldots$. En effet, logiquement on devrait avoir

$$\begin{aligned}\frac{x}{10} &= \frac{1}{10} + 1 + 10 + 100 + \ldots \\ &= \frac{1}{10} + x.\end{aligned}$$

Reste à résoudre l'équation du premier degré : $\frac{x}{10} = x + \frac{1}{10}$. Ai-je besoin de donner la solution ?

12.12.3 Dans les nombres p-adiques, c'est vrai

Nous nous proposons d'apprendre sur les nombres p-adiques juste ce qu'il faut pour montrer que l'égalité

$$\sum_{k=0}^{\infty} 10^k = -\frac{1}{9} \tag{12.489}$$

est vraie dans les nombres 5-adiques. Tout ce qu'il faut est sur wikipedia.

Soit $a \in \mathbb{N}$ et p, un nombre premier. La **valuation** p-adique de a est l'exposant de p dans la décomposition de a en nombres premiers. On la note $v_p(a)$. Pour un rationnel on définit

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b) \tag{12.490}$$

La **valeur absolue** p-adique de $r \in \mathbb{Q}$ est

$$|r|_p = p^{-v_p(r)}. \tag{12.491}$$

Nous posons $|0|_p = 0$. De là nous considérons la distance

$$d_p(x, y) = |x - y|_p. \tag{12.492}$$

Lemme 12.174.
L'espace $(\mathbb{Q}, d_p)$ est un espace métrique[53].

Nous considérons maintenant $p = 5$. Étant donné que $a = 5 \cdot 2$ nous avons $v_5(10) = 1$ et

$$v_5\left(\frac{1}{9}\right) = v_5(1) - v_5(9) = 0. \tag{12.493}$$

Nous avons

$$\sum_{k=0}^{N} 10^k + \frac{1}{9} = \frac{10^{N+1}}{9} \tag{12.494}$$

mais

$$v_p\left(\frac{10^{N+1}}{9}\right) = v_5(10^{N+1}) - v_5(9) = N + 1. \tag{12.495}$$

Par conséquent

$$d_5\Big(\sum_{k=0}^{N} 10^k, -\frac{1}{9}\Big) = \Big|\frac{10^{N+1}}{9}\Big|_p = p^{-(N+1)}. \tag{12.496}$$

En passant à la limite,

$$\lim_{N\to\infty} d_5\Big(\sum_{k=0}^{N} 10^k, -\frac{1}{9}\Big) = 0, \tag{12.497}$$

ce qui signifie que[54]

$$\sum_{k=0}^{\infty} 10^k = -\frac{1}{9}. \tag{12.498}$$

53. Définition 7.87
54. Voir la définition 12.56 de la convergence d'une série dans un espace métrique.