Agrégation 2024

Plans de leçons & Développements

Document intégralement écrit par Hugo Delaunay.
Visitez `agreg.skyost.eu` pour plus de ressources et d'informations.

Une coquille ? Une correction à apporter ? Rendez-vous sur le dépôt Github "`Skyost/Agregation`" ou contactez-moi via mon site web personnel `skyost.eu`.

Table des matières

I Plans de leçons

101 Groupe opérant sur un ensemble. Exemples et applications.

Soit G un groupe.

I - Actions de groupe

Soit $X \neq \emptyset$ un ensemble.

1. Cas général

[ULM21] p. 29

Définition 1. On appelle **action** (à gauche) de G sur X toute application

$$\begin{array}{ccc} G \times X & \to & X \\ (g,x) & \mapsto & g \cdot x \end{array}$$

satisfaisant les conditions suivantes :

(i) $\forall g,h \in G, \forall x \in X, g \cdot (h \cdot x) = (gh) \cdot x$.

(ii) $\forall x \in X, e_G \cdot x = x$.

Remarque 2. On peut de même définir une action à droite de G sur X.

Exemple 3.
— Le groupe S_X des bijections de X dans X opère naturellement sur X par la relation $\sigma \cdot x = \sigma(x)$ pour tout $\sigma \in S_x$ et pour tout $x \in X$.
— Pour un espace vectoriel V, le groupe $\mathrm{GL}(V)$ opère sur V.

On supposera par la suite que G agit sur X à gauche via l'action $\cdot$.

Théorème 4. On a une correspondance bijective entre les actions de G sur X et les morphismes de G dans S_X. En effet, si $\cdot$ désigne une action de G sur X, on peut y faire correspondre le morphisme

$$\varphi : \begin{array}{ccc} G & \to & S_X \\ g & \mapsto & (x \mapsto g \cdot x) \end{array}$$

Définition 5. On définit pour tout $x \in X$:

— $G \cdot x = \{g \cdot x \mid g \in G\} \subseteq X$ l'**orbite de** x.

— $\mathrm{Stab}_G(x) = \{g \in G \mid g \cdot x = x\} < G$ le **stabilisateur de** x.

On dit que l'action de G sur X est :

— **Libre** si $\mathrm{Stab}_G(x) = \{e_G\}$ pour tout $x \in X$.

— **Transitive** si G n'admet qu'une seule orbite.

Exemple 6. L'action du groupe diédral $\mathscr{D}_3$ sur les sommets d'un triangle équilatéral est transitive mais n'est pas libre.

Proposition 7. La relation $\sim$ définie sur X par

$$x \sim y \iff x \in G \cdot y$$

est une relation d'équivalence dont les classes d'équivalence sont les orbites des éléments de X sous l'action de G.

Application 8. Toute permutation $\sigma \in S_n$ s'écrit comme produit

$$\sigma = \gamma_1 \dots \gamma_m$$

de cycles γ_i de longueur ≥ 2 dont les supports sont deux-à-deux disjoints. Cette décomposition est unique à l'ordre près.

[PER] p. 57

Définition 9. Une action $\varphi : G \to S_X$ une action de G sur X est dite **fidèle** si $\mathrm{Ker}(\varphi) = \{e_G\}$.

[ULM21] p. 33

Proposition 10. Soit $\varphi : G \to S_X$ une action de G sur X. Alors,

$$\mathrm{Ker}(\varphi) = \bigcap_{x \in X} \mathrm{Stab}_G(x)$$

Corollaire 11. Une action libre est fidèle.

Proposition 12. Soit $x \in X$. L'application

$$f : \begin{array}{ccc} G/\mathrm{Stab}_G(x) & \to & G \cdot x \\ g\,\mathrm{Stab}_G(x) & \mapsto & g \cdot x \end{array}$$

est une bijection.

p. 71

Remarque 13. Attention cependant, $G/\mathrm{Stab}_G(x)$ n'est pas un groupe en général.

2. Cas fini

On suppose ici que G et X sont finis.

Proposition 14. Soit $x \in X$. Alors :

- $|G \cdot x| = (G : \mathrm{Stab}_G(x))$.
- $|G| = |\mathrm{Stab}_G(x)||G \cdot x|$.
- $|G \cdot x| = \frac{|G|}{|\mathrm{Stab}_G(x)|}$

Théorème 15 (Formule des classes)**.** Soit Ω un système de représentants associé à la relation $\sim$ de la Théorème 7. Alors,

$$|X| = \sum_{\omega \in \Omega} |G \cdot \omega| = \sum_{\omega \in \Omega} (G : \mathrm{Stab}_G(\omega)) = \sum_{\omega \in \Omega} \frac{|G|}{|\mathrm{Stab}_G(\omega)|}$$

Définition 16. On définit :

- $X^G = \{x \in X \mid \forall g \in G,\ g \cdot x = x\}$ l'ensemble des points de X laissés fixes par tous les éléments de G.
- $X^g = \{x \in X \mid g \cdot x = x\}$ l'ensemble des points de X laissés fixes par $g \in G$.

Corollaire 17 (Formule de Burnside)**.** Le nombre r d'orbites de X sous l'action de G est donné par

$$r = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

Corollaire 18. Soit p un nombre premier. Si G est un p-groupe (ie. l'ordre de G est une puissance de p), alors,

$$|X^G| \equiv |X| \mod p$$

Corollaire 19. Soit p un nombre premier. Le centre d'un p-groupe non trivial est non trivial.

Corollaire 20. Soit p un nombre premier. Un groupe d'ordre p^2 est toujours abélien.

Application 21 (Théorème de Cauchy)**.** On suppose G non trivial et fini. Soit p un premier divisant l'ordre de G. Alors il existe un élément d'ordre p dans G.

[DEV]

Application 22 (Premier théorème de Sylow)**.** On suppose G fini d'ordre np^α avec $n, \alpha \in \mathbb{N}$ et p premier tel que $p \nmid n$. Alors, il existe un sous-groupe de G d'ordre p^α.

[GOU21] p. 44

II - Action d'un groupe sur un groupe

1. Action par translation

Proposition 23. G agit sur lui-même par translation (à gauche) via l'action

$$(g,h) \mapsto g \cdot h = gh$$

De plus, cette action est fidèle et transitive.

[ULM21] p. 34

Application 24 (Théorème de Cayley)**.** Tout groupe fini d'ordre n est isomorphe à un sous-groupe de S_n.

Proposition 25. Soit $H < G$. Alors G agit sur G/H via l'action

$$(g,hH) \mapsto g \cdot hH = (gh)H$$

De plus, cette action est transitive.

Proposition 26. Soit $H < G$. Soit $\varphi : G \to S_{G/H}$ le morphisme de l'action par translation de G sur G/H. Alors,

$$\mathrm{Ker}(\varphi) = \bigcap_{g \in G} gHg^{-1}$$

Application 27. On suppose que G est de cardinal infini et que G possède un sous-groupe d'indice fini distinct de G. Alors G n'est pas simple.

[PER] p. 17

2. Action par conjugaison

Proposition 28. G agit sur lui-même par conjugaison via l'action

$$(g,h) \mapsto g \cdot h = ghg^{-1}$$

[ULM21] p. 36

Définition 29.
- L'orbite de $g \in G$ sous l'action par conjugaison de G sur lui-même s'appelle la **classe de conjugaison de** g.
- Le stabilisateur de $g \in G$ sous l'action par conjugaison de G sur lui-même s'appelle le **centralisateur de** g.
- Deux éléments de G qui appartiennent à la même classe de conjugaison sont dits **conjugués**.

Exemple 30. — Si $\sigma = \begin{pmatrix} a_1 & \dots & a_p \end{pmatrix} \in S_n$ est un p-cycle, et si $\tau \in S_n$, alors

$$\tau\sigma\tau^{-1} = \begin{pmatrix} \tau(a_1) & \dots & \tau(a_p) \end{pmatrix}$$

— Par conséquent, dans S_n, les p-cycles sont conjugués.

— Pour $n \geq 5$, les 3-cycles sont conjugués dans A_n.

[PER] p. 15

Proposition 31. Soit $g \in G$. Alors g appartient au centre de G (noté $Z(G)$) si et seulement si sa classe de conjugaison est réduite à un seul élément.

[ULM21] p. 36

Corollaire 32. $Z(G)$ est l'union des classes de conjugaison de taille 1.

Proposition 33. Soit Ω un système de représentants associé à la relation $\sim$ de la Théorème 7 pour l'action par conjugaison. On note $\Omega' = Z(G) \smallsetminus \Omega$. Alors,

$$|G| = |Z(G)| + \sum_{\omega \in \Omega'} \frac{|G|}{|\mathrm{Stab}_G(\omega)|}$$

[GOU21] p. 24

[DEV]

Application 34 (Théorème de Wedderburn)**.** Tout corps fini est commutatif.

p. 100

Proposition 35. G agit sur ses sous-groupes par conjugaison via l'action

$$(g, H) \mapsto g \cdot H = gHg^{-1}$$

[ULM21] p. 38

Proposition 36. Soit $H < G$. Alors H est distingué dans G si et seulement si H est un point fixe pour l'action de la Théorème 35.

III - Action d'un groupe sur un espace vectoriel

1. Action par conjugaison sur les espaces de matrices

Soit E un espace vectoriel de dimension finie n sur un corps $\mathbb{K}$.

Proposition 37. L'application

$$\begin{array}{ccc} \mathrm{GL}_n(\mathbb{K}) \times \mathcal{M}_n(\mathbb{K}) & \to & \mathcal{M}_n(\mathbb{K}) \\ (P, A) & \mapsto & PAP^{-1} \end{array}$$

[ROM21] p. 199

définit une action de $\mathrm{GL}_n(\mathbb{K})$ sur $\mathscr{M}_n(\mathbb{K})$.

Définition 38. Deux matrices qui sont dans la même orbite pour cette action sont dites **semblables**.

Remarque 39. Deux matrices semblables représentes la même application linéaire dans deux bases de $\mathbb{K}^n$. [GOU21] p. 127

C'est cette remarque qui justifie que l'on va étudier l'action par conjugaison de $\mathrm{GL}_n(\mathbb{K})$ sur $\mathscr{M}_n(\mathbb{K})$.

Théorème 40. Soient A et B deux matrices semblables. Alors : [ROM21] p. 199

- $\mathrm{trace}(A) = \mathrm{trace}(B)$.
- $\det(A) = \det(B)$.
- $\mathrm{rang}(A) = \mathrm{rang}(B)$.
- $\chi_A = \chi_B$.
- $\pi_A = \pi_B$.

Contre-exemple 41. Les matrices $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ ont la même trace, le même déterminant, le même polynôme caractéristique, mais ne sont pas semblables. [D-L] p. 137

Théorème 42. Soient $\mathbb{L}$ une extension de $\mathbb{K}$ et $A, B \in \mathscr{M}_n(\mathbb{K})$. On suppose $\mathbb{K}$ infini et A, B semblables sur $\mathbb{L}$. Alors A et B sont semblables sur $\mathbb{K}$. [GOU21] p. 167

Notation 43. Soient $f \in \mathscr{L}(E)$ et $x \in E$. On note $P_{f,x}$ le polynôme unitaire engendrant l'idéal $\{P \in \mathbb{K}[X] \mid P(f)(x) = 0\}$ et $E_{f,x} = \{P(f)(x) \mid P \in \mathbb{K}[X]\}$. p. 397

Lemme 44. Soit $f \in \mathscr{L}(E)$.

(i) Si $k = \deg(\pi_f)$, alors $\mathbb{K}[f]$ est un sous-espace vectoriel de $\mathscr{L}(E)$ de dimension k, dont une base est $(f^i)_{i \in [\![0, k-1]\!]}$.

(ii) Soit $x \in E$. Si $l = \deg(P_{f,x})$, alors E_x est un sous-espace vectoriel de E de dimension l, dont une base est $(f^i(x))_{i \in [\![0, l-1]\!]}$.

Lemme 45. Soit $f \in \mathscr{L}(E)$. Il existe $x \in E$ tel que $P_{f,x} = \pi_f$.

Théorème 46 (Frobenius)**.** Soit $f \in \mathscr{L}(E)$. Il existe des sous-espaces vectoriels $F_1, \dots, F_r$ de E tous stables par f tels que :

(i) $E = \bigoplus_{i=1}^{r} F_i$.

(ii) $\forall i \in [\![1, r]\!]$, la restriction $f_i = f_{|F_i}$ est un endomorphisme cyclique de F_i.

(iii) Si $P_i = \pi_{f_i}$ est le polynôme minimal de f_i, on a $P_{i+1} \mid P_i \ \forall i \in [\![1, r-1]\!]$.

La suite $(P_i)_{i \in [\![1,r]\!]}$ ne dépend que de f et non du choix de la décomposition (elle est donc unique). On l'appelle **suite des invariants de** f.

Corollaire 47. Deux endomorphismes sont semblables si et seulement s'ils ont les mêmes invariants de similitude.

2. Représentations linéaires et caractères

Dans cette partie, on suppose que G est d'ordre fini.

[ULM21] p. 144

Définition 48.
— Une **représentation linéaire** ρ est un morphisme de G dans $\mathrm{GL}(V)$ où V désigne un espace-vectoriel de dimension finie n sur $\mathbb{C}$.
— On dit que n est le **degré** de ρ.
— On dit que ρ est **irréductible** si $V \neq \{0\}$ et si aucun sous-espace vectoriel de V n'est stable par $\rho(g)$ pour tout $g \in G$, hormis $\{0\}$ et V.

Exemple 49. Soit $\varphi : G \to S_n$ le morphisme structurel d'une action de G sur un ensemble de cardinal n. On obtient une représentation de G sur $\mathbb{C}^n = \{e_1, \dots, e_n\}$ en posant

$$\rho(g)(e_i) = e_{\varphi(g)(i)}$$

c'est la représentation par permutations de G associé à l'action. Elle est de degré n.

Définition 50. La représentation par permutations de G associée à l'action par translation à gauche de G sur lui-même est la **représentation régulière** de G, on la note ρ_G.

p. 150

Définition 51. On peut associer à toute représentation linéaire ρ, son **caractère** $\chi = \mathrm{trace} \circ \rho$. On dit que χ est **irréductible** si ρ est irréductible.

Proposition 52.
(i) Les caractères sont des fonctions constantes sur les classes de conjugaison.
(ii) Il y a autant de caractères irréductibles que de classes de conjugaisons.

Définition 53. Soit $\rho : G \to \mathrm{GL}(V)$ une représentation linéaire de G. On suppose $V = W \oplus W_0$ avec W et W_0 stables par $\rho(g)$ pour tout $g \in G$. On dit alors que ρ est **somme directe** de ρ_W et de ρ_{W_0}.

Théorème 54 (Maschke)**.** Toute représentation linéaire de G est somme directe de représentations irréductibles.

Théorème 55. Les sous-groupes distingués de G sont exactement les

$$\bigcap_{i \in I} \mathrm{Ker}(\rho_i) \text{ où } I \in \mathscr{P}(\llbracket 1, r \rrbracket)$$

[PEY] p. 231

Corollaire 56. G est simple si et seulement si $\forall i \neq 1$, $\forall g \neq e_G$, $\chi_i(g) \neq \chi_i(e_G)$.

102 Groupe des nombres complexes de module 1. Racines de l'unité. Applications.

I - Nombres complexes de module 1

1. Le groupe $\mathbb{U}$

Définition 1. On définit

$$\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$$

le groupe abélien des nombres complexes de module 1.

[ROM21] p. 36

Proposition 2. L'application

$$\exp(i\theta) \mapsto \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix}$$

(où exp est définie dans la sous-section suivante) définit un isomorphisme de $\mathbb{U}$ dans $\mathrm{SO}_2(\mathbb{R})$.

Proposition 3. Un sous-groupe additif de $\mathbb{R}$ est soit dense dans $\mathbb{R}$, soit de la forme $n\mathbb{Z}$.

[FGN3] p. 51

Corollaire 4. Un sous-groupe de $\mathbb{U}$ est soit fini, soit dense dans $\mathbb{U}$.

Corollaire 5. Soit $\theta \notin 2\pi\mathbb{Q}$. $\{e^{in\theta} \mid n \in \mathbb{N}\}$ est dense dans $\mathbb{U}$.

Application 6. $\{\sin(n) \mid n \in \mathbb{N}\}$ est dense dans $[-1, 1]$.

Proposition 7. $\mathbb{U}$ est un sous-groupe compact et connexe de $\mathbb{C}^*$.

[GOU20] p. 44

Application 8. Soit $f : \mathbb{U} \to \mathbb{R}$ continue. Alors il existe deux points diamétralement opposés de $\mathbb{U}$ qui ont la même image par f.

2. L'exponentielle complexe

Définition 9. On définit la fonction **exponentielle complexe** pour tout $z \in \mathbb{C}$ par

$$\sum_{n=0}^{+\infty} \frac{z^n}{n!}$$

on note cette somme e^z ou parfois $\exp(z)$.

[QUE] p. 4

Remarque 10. Cette somme est bien définie pour tout $z \in \mathbb{C}$ d'après le critère de d'Alembert.

Proposition 11. (i) $\forall z, z' \in \mathbb{C}$, $e^{z+z'} = e^z e^{z'}$.

(ii) exp est holomorphe sur $\mathbb{C}$, de dérivée elle-même.

(iii) exp ne s'annule jamais.

Proposition 12. La fonction $\varphi : t \mapsto e^{it}$ est un morphisme surjectif de $\mathbb{R}$ sur $\mathbb{U}$.

Proposition 13. En reprenant les notations précédentes, $\mathrm{Ker}(\varphi)$ est un sous-groupe fermé de $\mathbb{R}$, de la forme $\mathrm{Ker}(\varphi) = a\mathbb{Z}$. On note $a = 2\pi$.

3. Trigonométrie

Définition 14. Les fonctions sin et cos sont définies sur $\mathbb{R}$ par

— $\cos(t) = \mathrm{Re}(e^{it}) = \frac{e^{it}+e^{-it}}{2} = \sum_{n=0}^{+\infty}(-1)^n \frac{t^{2n}}{(2n)!}$.

— $\sin(t) = \mathrm{Im}(e^{it}) = \frac{e^{it}-e^{-it}}{2i} = \sum_{n=0}^{+\infty}(-1)^n \frac{t^{2n+1}}{(2n+1)!}$.

Proposition 15. Ces fonctions sont réelles, 2π-périodiques, et admettent un développement en série entière de rayon de convergence infini. On peut en particulier les prolonger sur le plan complexe entier.

Proposition 16. Tout nombre complexe $z \in \mathbb{C}$ peut s'écrire de la manière suivante :

$$z = |z|e^{i\theta} = \cos(\theta) + i\sin(\theta)$$

[R-R] p. 259

Proposition 17 (Formule de Moivre)**.**

$$\forall n \in \mathbb{N}, \forall \theta \in \mathbb{R}, (\cos(\theta) + i\sin(\theta))^n = \cos(n\theta) + i\sin(n\theta)$$

Application 18 (Calcul du noyau de Dirichlet)**.** [GOU20] p. 271

$$\forall n \in \mathbb{N}^*, \forall x \in \mathbb{R} \setminus 2\pi\mathbb{Z}, \sum_{k=-n}^{n} \frac{\sin\left(\frac{(2n+1)x}{2}\right)}{\sin\left(\frac{x}{2}\right)}$$

II - Le groupe des racines de l'unité

Soit $n \in \mathbb{N}^*$.

1. Racines n-ièmes de l'unité

Définition 19. Étant donnés $\alpha \in \mathbb{C}$, on appelle : [R-R] p. 259

- **Racine n-ième de** α tout nombre $z \in \mathbb{C}$ tel que $z^n = \alpha$.
- **Racine n-ième de l'unité** toute racine n-ième de 1. On note μ_n cet ensemble.

Exemple 20. Les racines cubiques de l'unité sont 1, $j = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ et $\bar{j}$.

Proposition 21. Pour tout $n \in \mathbb{N}^*$, il y a n racines n-ièmes de l'unité, données par

$$e^{\frac{2ik\pi}{n}} = \cos\left(\frac{2ik\pi}{n}\right) + i\sin\left(\frac{2ik\pi}{n}\right)$$

où k parcourt les entiers de 0 à $n-1$.

Corollaire 22. Pour tout $n \in \mathbb{N}^*$,

$$X^n - 1 = \prod_{k=0}^{n-1} (X - e^{\frac{2ik\pi}{n}})$$

Corollaire 23. Tout nombre complexe non nul α écrit $\alpha = re^{i\theta}$ admet exactement n racines n-ièmes données par

$$\sqrt[n]{r}e^{i\frac{\theta}{n}}e^{\frac{2ik\pi}{n}}$$

où k parcourt les entiers de 0 à $n-1$.

[GOZ] p. 67

Proposition 24. μ_n est un groupe, et l'application

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \to & \mu_n \\ k & \mapsto & e^{\frac{2ik\pi}{n}} \end{array}$$

est un isomorphisme.

Proposition 25. $\mathbb{C}^*$ admet exactement un sous-groupe d'ordre n : μ_n. [ROM21] p. 36

2. Générateurs et polynômes cyclotomiques

Définition 26. L'ensemble des générateurs de μ_n, noté μ_n^*, est formé des **racines primitives n-ièmes de l'unité**. [GOZ] p. 67

Proposition 27. (i) $\mu_n^* = \{e^{\frac{2ik\pi}{n}} \mid k \in [\![0, n-1]\!], \operatorname{pgcd}(k,m) = 1\}$.
(ii) $|\mu_n^*| = \varphi(n)$, où φ désigne l'indicatrice d'Euler.

Définition 28. On appelle **n-ième polynôme cyclotomique** le polynôme

$$\Phi_n = \prod_{\xi \in \mu_n^*} (X - \xi)$$

Théorème 29. (i) $X^n - 1 = \prod_{d|n} \Phi_d$.
(ii) $\Phi_n \in \mathbb{Z}[X]$.
(iii) Φ_n est irréductible sur $\mathbb{Q}$.

Corollaire 30. Le polynôme minimal sur $\mathbb{Q}$ de tout élément ξ de μ_n^* est Φ_n. En particulier,

$$[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(m)$$

Application 31 (Théorème de Wedderburn)**.** Tout corps fini est commutatif.

[DEV]

Application 32 (Dirichlet faible)**.** Pour tout entier n, il existe une infinité de nombres premiers congrus à 1 modulo n. [GOU21] p. 99

III - Applications en algèbre

1. Une application géométrique

Proposition 33 (Déterminant circulant)**.** Soient $n \in \mathbb{N}^*$ et $a_1, \dots, a_n \in \mathbb{C}$. On pose $\omega = e^{\frac{2i\pi}{n}}$. Alors

$$\begin{vmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \dots & a_0 \end{vmatrix} = \prod_{j=0}^{n-1} P(\omega^j)$$

où $P = \sum_{k=0}^{n-1} a_k X^k$.

p. 153

Application 34 (Suite de polygones)**.** Soit P_0 un polygone dont les sommets sont $\{z_{0,1}, \dots, z_{0,n}\}$. On définit la suite de polygones (P_k) par récurrence en disant que, pour tout $k \in \mathbb{N}^*$, les sommets de P_{k+1} sont les milieux des arêtes de P_k.

Alors la suite (P_k) converge vers l'isobarycentre de P_0.

[I-P] p. 389

2. Racines de polynômes

[DEV]

Théorème 35 (Kronecker)**.** Soit $P \in \mathbb{Z}[X]$ unitaire tel que toutes ses racines complexes appartiennent au disque unité épointé en l'origine (que l'on note D). Alors toutes ses racines sont des racines de l'unité.

p. 279

Corollaire 36. Soit $P \in \mathbb{Z}[X]$ unitaire et irréductible sur $\mathbb{Q}$ tel que toutes ses racines complexes soient de module inférieur ou égal à 1. Alors $P = X$ ou P est un polynôme cyclotomique.

3. Dual d'un groupe

Soit G un groupe fini de cardinal n.

Définition 37. Un **caractère** est un morphisme de G dans $\mathbb{C}^*$. On note $\widehat{G}$ l'ensemble des caractères, qu'on appelle **dual** de G.

[PEY] p. 2

Proposition 38. $\widehat{G}$ est un groupe pour la multiplication.

Proposition 39. (i) $\widehat{G}$ est constitué des morphismes de G dans μ_n.
(ii) $\forall g \in G, |\chi(g)| = 1$.
(iii) $\forall g \in G, \chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)}$.

Proposition 40. Si $G = \langle g_0 \rangle$, en notant ω une racine primitive n-ième de l'unité, les éléments de $\widehat{G}$ sont de la forme $g_0^k \mapsto (\omega^j)^k$ pour $j \in [\![0, n-1]\!]$.

Corollaire 41. Si G est cyclique, $G \cong \widehat{G}$.

4. Transformée de Fourier discrète

Soit $N \in \mathbb{N}^*$.

p. 64

Notation 42. Soit f un vecteur de $\mathbb{C}^N$. On note $f[k]$ sa k-ième composante pour tout $k \in [\![1, N]\!]$.

Définition 43. Soit f un vecteur de $\mathbb{C}^N$.La **transformée de Fourier discrète** de f est

$$\widehat{f} = \sum_{n=0}^{N-1} f[n]\omega_N^{-nk}$$

pour $k \in [\![0, N-1]\!]$ où l'on a noté $\omega_N = e^{\frac{2i\pi}{N}}$ une racine primitive N-ième de l'unité.On note

$$\mathscr{F} : \begin{array}{ccc} \mathbb{C}^N & \to & \mathbb{C}^N \\ f & \mapsto & \widehat{f} \end{array}$$

Proposition 44 (Transformée de Fourier inverse)**.**

$$\forall n \in [\![0, N-1]\!], f[n] = \frac{1}{N} \sum_{k=0}^{N-1} \widehat{f}[k]\omega_N^{nk}$$

Corollaire 45. Soit f un vecteur de $\mathbb{C}^N$. En notant f_1 le vecteur défini par

$$f_1[0] = \frac{1}{N} f[0] \text{ et } \forall n \in [\![1, \dots, N-1]\!], f_1[n] = \frac{1}{N} f[N-n]$$

on a

$$\mathscr{F}^{-1}(f) = \mathscr{F}(f_1)$$

Annexes

[I-P]
p. 389

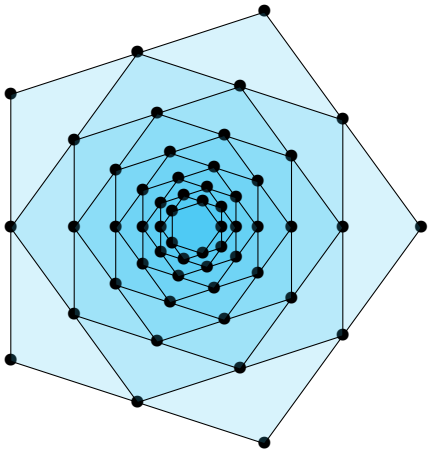


FIGURE I.1 – La suite de polygones.

103 Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications.

Soit G un groupe.

I - Conjugaison dans un groupe

1. Action de conjugaison

Lemme 1. On a une action de G sur lui-même :

$$\forall g, h \in G,\ g \cdot h = ghg^{-1}$$

[ROM21] p. 19

Définition 2. L'action précédente est appelée **action de conjugaison**. Le morphisme structurel de G dans $S(G)$ est noté Int :

$$\forall g, h \in G,\ \mathrm{Int}(g)(h) = ghg^{-1}$$

L'image de G par ce morphisme $\mathrm{Int}(G)$ est le groupe des **automorphismes intérieurs** de G.

Exemple 3. Le groupe additif d'un espace vectoriel est un groupe abélien dont le seul automorphisme intérieur est l'identité.

[ULM21] p. 20

Proposition 4. Muni de la composition, l'ensemble des automorphismes intérieurs de G est un groupe.

[GOU21] p. 21

2. Orbites et stabilisateurs

Définition 5. On considère l'action de conjugaison de G.

- Ses orbites sont les **classes de conjugaison** de G.
- Le stabilisateur d'un élément est le **centralisateur** de celui-ci.
- Deux éléments sont dits **conjugués** s'ils appartiennent à la même classe de conjugaison.

[PER] p. 15

Exemple 6. Les cycles de même ordre sont conjugués dans S_n.

Définition 7. On définit le **centre** de G noté $Z(G)$ par

$$Z(G) = \{g \in G \mid \forall h \in H, gh = hg\}$$

Autrement dit, $Z(G)$ est l'intersection des centralisateurs des éléments de G.

p. 12

Exemple 8. Si G est abélien, alors $Z(G) = G$.

Proposition 9. Soit $g \in G$. Alors, $g \in Z(G)$ si et seulement si sa classe de conjugaison est réduite à un élément.

Ainsi, $Z(G)$ est l'union des classes de conjugaison de taille 1.

[ULM21] p. 36

II - Sous-groupes distingués et groupes quotients

1. Classes à gauche et à droite

Proposition 10. Soit $H < G$. On définit la relation $\sim_H$ sur G par $g_1 \sim_H g_2 \iff g_1^{-1} g_2 \in H$. Alors :

(i) $\sim_H$ est une relation d'équivalence.

(ii) La classe d'équivalence d'un élément $g \in G$ pour $\sim_H$ est $\overline{g} = gH = \{gh \mid h \in H\}$ appelée **classe à gauche** de g modulo H.

p. 24

Remarque 11. On définit de la même manière la **classe à droite** d'un élément $g \in G$ modulo H que l'on note Hg.

Exemple 12. Soit $n > 2$. On considère $\mathscr{D}_n = \langle r, s \rangle$ le groupe diédral d'ordre $2n$. Alors,

$$r\langle s \rangle = \{r, rs\} \neq \{r, sr\} = \langle s \rangle r$$

Proposition 13. Soit $H < G$. Alors,

$$\forall g \in G, |hG| = |Gh| = |H|$$

2. Sous-groupes distingués

Définition 14. Soit $H < G$. On dit que H est **distingué** dans G si,

$$\forall g \in G,\ gH = Hg$$

On note cela $H \triangleleft G$.

[ROM21] p. 3

Exemple 15.
- $\{e_G\} \triangleleft G, G \triangleleft G$ et $Z(G) \triangleleft G$.
- L'intersection de deux sous-groupes distingués dans G est distinguée dans G.
- Si G est abélien, tout sous-groupe de G est distingué dans G.

Remarque 16. Le symbole $\triangleleft$ n'est pas transitif.

[GOU21] p. 20

Proposition 17.

$$H \triangleleft G \iff \forall g \in G,\ gHg^{-1} \subseteq H$$

Proposition 18. Soient G_1 et G_2 deux groupes, et soient H_1 et H_2 deux sous-groupes respectivement de G_1 et de G_2. Soit $\varphi : G_1 \to G_2$ un morphisme. Alors :

(i) Si $H_1 \triangleleft G_1$, alors $\varphi(H_1) \triangleleft \varphi(G_1)$.

(ii) Si $H_2 \triangleleft G_2$, alors $\varphi^{-1}(H_2) \triangleleft G_1$.

En particulier, $\mathrm{Ker}(\varphi) \triangleleft G_1$.

[ULM21] p. 16

Proposition 19. Soient $K < H < G$ une suite de sous-groupes. Alors,

$$K \triangleleft G \implies K \triangleleft H$$

p. 43

Proposition 20. Soit $H < G$. Si $(G : H) = 2$ (voir sous-section suivante), alors $H \triangleleft G$.

p. 25

3. Groupes quotients

Définition 21. Soit $H < G$.
- On appelle **ensemble quotient** de G par la relation d'équivalence $\sim_H$ de la Théorème 10, et on note G/H, l'ensemble des classes à gauche de G modulo H.
- On appelle **indice** de G dans H, et on note $(G : H)$, le cardinal de G/H.

Proposition 22. Soit $H < G$. L'ensemble des classes à droite de G modulo H est aussi de cardinal égal à $(G : H)$.

Théorème 23. Un sous-groupe H de G est distingué si et seulement si $*$ définit une loi de groupe sur G/H par : p. 44

$$\forall g_1, g_2 \in G,\ g_1 H * g_2 H = (g_1 g_2) H$$

telle que la surjection canonique

$$\pi_H : \begin{array}{ccc} G & \to & G/H \\ g & \mapsto & gH \end{array}$$

soit un morphisme de groupes. Dans ce cas, π_H est un morphisme surjectif de noyau H.

Définition 24. Soit $H \triangleleft G$. On appelle **groupe quotient** le groupe $(G/H, *)$ définit dans le théorème précédent.

Exemple 25. Soit $m \in \mathbb{N}^*$. $m\mathbb{Z}$ est un sous-groupe du groupe abélien $\mathbb{Z}$. On peut définir le groupe quotient $\mathbb{Z}/m\mathbb{Z}$: c'est un groupe cyclique d'ordre m.

4. Théorèmes d'isomorphisme

Théorème 26 (Premier théorème d'isomorphisme)**.** Soient G_1 et G_2 deux groupes et soit $\varphi : G_1 \to G_2$ un morphisme. Alors φ induit un isomorphisme **[ULM21]** p. 51

$$\overline{\varphi} : \begin{array}{ccc} G_1/\mathrm{Ker}(\varphi) & \to & \varphi(G_1) \\ g\mathrm{Ker}(\varphi) & \mapsto & \varphi(g) \end{array}$$

Exemple 27.
— Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
— $G/Z(G) \cong \mathrm{Int}(G)$.

Théorème 28 (Deuxième théorème d'isomorphisme)**.** Soient $H < G$ et $K \triangleleft G$. On pose $N = H \cap K$. Alors, p. 80

$$N \triangleleft H \text{ et } H/N \cong HK/K$$

Exemple 29. On note V le sous-groupe de S_4 d'ordre 4 isomorphe au groupe de Klein. Alors,

$$V/S_4 \cong S_3$$

p. 51

Théorème 30 (Troisième théorème d'isomorphisme)**.** Soient $H, K \triangleleft G$ tels que $H \subset K$. Alors,

$$K/H \triangleleft G/H \text{ et } (G/H)/(K/H) \cong G/K$$

Exemple 31.

$$(\mathbb{Z}/10\mathbb{Z})/(2\mathbb{Z}/10\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$$

III - Applications

1. Application aux p-groupes

Soit G un groupe fini opérant sur un ensemble fini X.

[ROM21] p. 22

Définition 32. On dit que G est un **p-groupe** s'il est d'ordre une puissance d'un nombre premier p.

Théorème 33 (Formule des classes)**.** Soit Ω un système de représentants des orbites de l'action de G sur X. Alors,

$$|X| = \sum_{\omega \in \Omega} |G \cdot \omega| = \sum_{\omega \in \Omega} (G : \mathrm{Stab}_G(\omega)) = \sum_{\omega \in \Omega} \frac{|G|}{|\mathrm{Stab}_G(\omega)|}$$

Corollaire 34. Soit p un nombre premier. Si G est un p-groupe opérant sur X, alors,

$$|X^G| \equiv |X| \mod p$$

où X^G désigne l'ensemble des points fixes de X sous l'action de G.

Corollaire 35. On note $G \cdot h_1, \dots, G \cdot h_r$ les classes de conjugaison de G. Alors,

$$\begin{aligned} |G| &= |Z(G)| + \sum_{\substack{i=1 \\ |G \cdot h_i| = 2}}^{r} |G \cdot h_i| \\ &= |Z(G)| + \sum_{\substack{i=1 \\ |G \cdot h_i| = 2}}^{r} \frac{|G|}{|\mathrm{Stab}_G(h_i)|} \end{aligned}$$

Corollaire 36. Soit p un nombre premier. Le centre d'un p-groupe non trivial est non trivial.

Corollaire 37. Soit p un nombre premier. Un groupe d'ordre p^2 est toujours abélien.

Application 38 (Théorème de Cauchy)**.** On suppose G non trivial et fini. Soit p un premier divisant l'ordre de G. Alors il existe un élément d'ordre p dans G.

[DEV]

Application 39 (Premier théorème de Sylow)**.** On suppose G fini d'ordre np^α avec $n, \alpha \in \mathbb{N}$ et p premier tel que $p \nmid n$. Alors, il existe un sous-groupe de G d'ordre p^α.

[GOU21] p. 44

2. Application au groupe symétrique

Lemme 40. Les 3-cycles sont conjugués dans A_n pour $n \geq 5$.

[PER] p. 15

Lemme 41. Le produit de deux transpositions est un produit de 3-cycles.

[ROM21] p. 49

Proposition 42. A_n est engendré par les 3-cycles pour $n \geq 3$.

[DEV]

Théorème 43. A_n est simple pour $n \geq 5$.

[PER] p. 28

Corollaire 44. Pour $n \geq 5$, les sous-groupes distingués de S_n sont S_n, A_n et $\{\mathrm{id}\}$.

Application 45. A_5 est le seul groupe simple d'ordre 60 à isomorphisme près.

[ULM21] p. 92

3. Application au groupe linéaire d'un espace vectoriel

Dans cette partie, E désignera un espace vectoriel sur un corps $\mathbb{K}$ de dimension finie n.

a. Centre

Définition 46. Soit H un hyperplan de E et soit $u \in \mathrm{SL}(E) \setminus \{\mathrm{id}_E\}$. Posons $D = \mathrm{Im}(u - \mathrm{id}_E)$. On dit que u est une **transvection** d'hyperplan H et de droite D si $u_{|H} = \mathrm{id}_H$ (et dans ce cas, $D \subset H$).

[PER] p. 97

Proposition 47. $u \in \mathrm{GL}(E)$ est une transvection de droite D si et seulement si $u_{|D} = \mathrm{id}_D$ et le morphisme induit $\overline{u} : E/D \to E/D$ est l'identité.

Proposition 48. Soit τ une transvection de droite D et d'hyperplan H et soit $u \in \mathrm{GL}(E)$. Alors $u\tau u^{-1}$ est une transvection de droite $u(D)$ et d'hyperplan $u(H)$.

Corollaire 49. (i) $Z(\mathrm{GL}(E)) = \{\lambda \mathrm{id}_E \mid \lambda \in \mathbb{K}^*\}$.
(ii) $Z(\mathrm{SL}(E)) = Z(\mathrm{GL}(E)) \cap \mathrm{SL}(E) \cong \mu_n(\mathbb{K})$.

b. Conjugaison

Définition 50. Soit H un hyperplan de E et soit $u \in \mathrm{GL}(E) \setminus \mathrm{SL}(E)$. Posons $D = \mathrm{Im}(u - \mathrm{id}_E)$. On dit que u est une **dilatation de droite** D **et d'hyperplan** H si $u_{|H} = \mathrm{id}_H$.Le **rapport** de cette dilatation est le scalaire $\det(u)$.

Proposition 51. Deux dilatations sont conjuguées dans $\mathrm{GL}(E)$ si et seulement si elles ont le même rapport.

Proposition 52. Deux transvections sont toujours conjuguées dans $\mathrm{GL}(E)$. Si $n \geq 3$, elles le sont aussi dans $\mathrm{SL}(E)$.

c. Groupe projectif

Définition 53. Le quotient de $\mathrm{GL}(E)$ par son centre est appelé **groupe projectif linéaire** et est noté $\mathrm{PGL}(E)$. De même, le quotient de $\mathrm{SL}(E)$ par son centre est noté $\mathrm{PSL}(E)$.

Remarque 54. Soit $h_\lambda : x \mapsto \lambda x$, on a $\det h_\lambda = \lambda^n$, de sorte qu'on a une suite exacte :

$$\{\overline{\mathrm{id}_E}\} \to \mathrm{PSL}(E) \to \mathrm{PGL}(E) \xrightarrow{\overline{\det}} \mathbb{K}^*/\mathbb{K}^{*n} \to \{\overline{\mathrm{id}_E}\}$$

où on a posé $\mathbb{K}^{*n} = \{\lambda \in \mathbb{K}^* \mid \exists \mu \in \mathbb{K}^*, \lambda = \mu^n\}$. En particulier, si $\mathbb{K}$ est algébriquement clos, $\mathrm{PSL}(E) \cong \mathrm{PGL}(E)$.

Théorème 55. Le groupe $\mathrm{PSL}(E)$ est simple sauf si $n = 2$ et $\mathbb{K} = \mathbb{F}_2$ ou $\mathbb{F}_3$.

4. Représentations linéaires de groupes finis

Dans cette partie, on suppose que G est d'ordre fini.

[ULM21] p. 144

Définition 56. — Une **représentation linéaire** ρ est un morphisme de G dans $\mathrm{GL}(V)$ où V désigne un espace-vectoriel de dimension finie n sur $\mathbb{C}$.
— On dit que n est le **degré** de ρ.
— On dit que ρ est **irréductible** si $V \neq \{0\}$ et si aucun sous-espace vectoriel de V n'est

stable par $\rho(g)$ pour tout $g \in G$, hormis $\{0\}$ et V.

Exemple 57. Soit $\varphi : G \to S_n$ le morphisme structurel d'une action de G sur un ensemble de cardinal n. On obtient une représentation de G sur $\mathbb{C}^n = \{e_1, \dots, e_n\}$ en posant

$$\rho(g)(e_i) = e_{\varphi(g)(i)}$$

c'est la représentation par permutations de G associé à l'action. Elle est de degré n.

Définition 58. La représentation par permutations de G associée à l'action par translation à gauche de G sur lui-même est la **représentation régulière** de G, on la note ρ_G.

Définition 59. On peut associer à toute représentation linéaire ρ, son **caractère** $\chi = \text{trace} \circ \rho$. On dit que χ est **irréductible** si ρ est irréductible.

p. 150

Proposition 60. (i) Les caractères sont des fonctions constantes sur les classes de conjugaison.

(ii) Il y a autant de caractères irréductibles que de classes de conjugaisons.

Définition 61. Soit $\rho : G \to \text{GL}(V)$ une représentation linéaire de G. On suppose $V = W \oplus W_0$ avec W et W_0 stables par $\rho(g)$ pour tout $g \in G$. On dit alors que ρ est **somme directe** de ρ_W et de ρ_{W_0}.

Théorème 62 (Maschke)**.** Toute représentation linéaire de G est somme directe de représentations irréductibles.

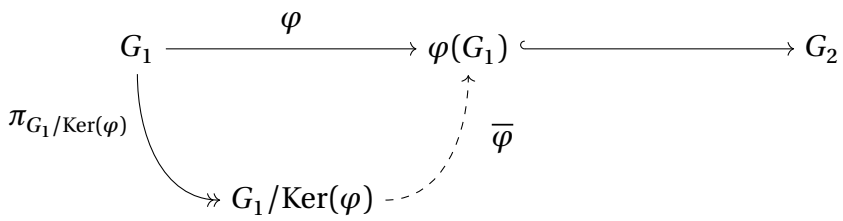
Théorème 63. Les sous-groupes distingués de G sont exactement les

$$\bigcap_{i \in I} \text{Ker}(\rho_i) \text{ où } I \in \mathscr{P}(\llbracket 1, r \rrbracket)$$

[PEY] p. 231

Corollaire 64. G est simple si et seulement si $\forall i \neq 1, \forall g \neq e_G, \chi_i(g) \neq \chi_i(e_G)$.

Annexes



[ULM21] p. 51

FIGURE I.2 – Illustration du premier théorème d'isomorphisme par un diagramme.

104 Groupes finis. Exemples et applications.

I - Outils d'étude de groupes finis

Soit G un groupe.

1. Ordre d'un groupe, ordre d'un élément

Définition 1. L'ordre du groupe G, noté $|G|$ est le cardinal de l'ensemble sous-jacent G. Si G est fini de cardinal n, on dit que G est **d'ordre** n. Sinon, on dit que G est **d'ordre infini**. [ULM21] p. 1

Exemple 2. Les multiplicatifs des corps $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont d'ordre infini.

Définition 3. On appelle **ordre** d'un élément $g \in G$, l'ordre du sous-groupe $\langle g \rangle$ qu'il engendre. p. 6

Exemple 4. L'élément i est d'ordre 4 dans $\mathbb{C}^*$.

Proposition 5. Soit $g \in G$ d'ordre n. Alors,

(i) n est le plus petit entier strictement positif ayant la propriété $g^n = e_G$.

(ii) $\langle g \rangle = \{e_G, g, \dots, g^{n-1}\}$.

(iii) Pour $k \in \mathbb{Z}$, $g^k = e_G$ si et seulement si $n \mid k$.

Exemple 6. Pour $n \in \mathbb{Z}$, on a $\langle n \rangle = \{nk \mid k \in \mathbb{Z}\}$ et on note ce groupe $n\mathbb{Z}$.

Théorème 7. Soit $g \in G$. Alors, p. 18

(i) g est d'ordre infini si et seulement si $\langle g \rangle$ est isomorphe à $(\mathbb{Z}, +)$. Dans ce cas $g^i \neq g^j$ dès que $i \neq j$ et $\langle g \rangle = \{\dots, g^{-1}, e_G, g, \dots\}$.

(ii) g est d'ordre fini si et seulement si $g, \dots, g^{n-1}$ sont tous distincts et si $g^n = e_G$.

Théorème 8 (Lagrange)**.** On suppose G fini. Soit $H < G$. Alors, p. 25

$$|H| \mid |G|$$

En particulier, l'ordre d'un élément de G divise toujours l'ordre de G.

2. Groupes cycliques

Définition 9. On dit que G est **cyclique** s'il est engendré par un seul élément. p. 6

Proposition 10. Un groupe fini d'ordre premier est cyclique. p. 26

Théorème 11. On suppose G fini d'ordre n. Alors,

(i) Si G est abélien et s'il existe au plus un sous-groupe d'ordre d pour tout diviseur d de n, alors G est cyclique.

(ii) Si G est cyclique, tous ses sous-groupes le sont aussi.

(iii) G est cyclique si et seulement si pour tout diviseur d de n, G admet exactement un sous-groupe d'ordre d.

Théorème 12. Tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique. **[ROM21]** p. 25

Corollaire 13. L'ensemble des racines n-ièmes de l'unité d'un corps est un sous-groupe cyclique de son groupe multiplicatif.

3. Actions de groupes

Soit X un ensemble. **[ULM21]** p. 29

Définition 14. On appelle **action** (à gauche) de G sur X toute application

$$\begin{array}{ccc} G \times X & \to & X \\ (g,x) & \mapsto & g \cdot x \end{array}$$

satisfaisant les conditions suivantes :

(i) $\forall g,h \in G, \forall x \in X, g \cdot (h \cdot x) = (gh) \cdot x$.

(ii) $\forall x \in X, e_G \cdot x = x$.

Remarque 15. On peut de même définir une action à droite de G sur X.

Définition 16. On définit pour tout $x \in X$:

— $G \cdot x = \{g \cdot x \mid g \in G\} \subseteq X$ l'**orbite de** x.

— $\mathrm{Stab}_G(x) = \{g \in G \mid g \cdot x = x\} < G$ le **stabilisateur de** x.

On suppose ici que G et X sont finis.

Proposition 17. Soit $x \in X$. Alors :
- $|G \cdot x| = (G : \mathrm{Stab}_G(x))$.
- $|G| = |\mathrm{Stab}_G(x)||G \cdot x|$.
- $|G \cdot x| = \frac{|G|}{|\mathrm{Stab}_G(x)|}$

p. 71

Théorème 18 (Formule des classes)**.** Soit Ω un système de représentants des orbites de l'action de G sur X. Alors,

$$|X| = \sum_{\omega \in \Omega} |G \cdot \omega| = \sum_{\omega \in \Omega} (G : \mathrm{Stab}_G(\omega)) = \sum_{\omega \in \Omega} \frac{|G|}{|\mathrm{Stab}_G(\omega)|}$$

Définition 19. On définit :
- $X^G = \{x \in X \mid \forall g \in G,\ g \cdot x = x\}$ l'ensemble des points de X laissés fixes par tous les éléments de G.
- $X^g = \{x \in X \mid g \cdot x = x\}$ l'ensemble des points de X laissés fixes par $g \in G$.

Corollaire 20 (Formule de Burnside)**.** Le nombre r d'orbites de X sous l'action de G est donné par

$$r = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

Corollaire 21. Soit p un nombre premier. Si G est un p-groupe (ie. l'ordre de G est une puissance de p), alors,

$$|X^G| \equiv |X| \mod p$$

où X^G désigne l'ensemble des points fixes de X sous l'action de G.

Corollaire 22. Soit p un nombre premier. Le centre d'un p-groupe non trivial est non trivial.

Corollaire 23. Soit p un nombre premier. Un groupe d'ordre p^2 est toujours abélien.

Application 24 (Théorème de Cauchy)**.** On suppose G non trivial et fini. Soit p un premier divisant l'ordre de G. Alors il existe un élément d'ordre p dans G.

[DEV]

Application 25 (Premier théorème de Sylow)**.** On suppose G fini d'ordre np^α avec $n, \alpha \in \mathbb{N}$ et p premier tel que $p \nmid n$. Alors, il existe un sous-groupe de G d'ordre p^α.

[GOU21] p. 44

II - Groupes abéliens finis

1. Un exemple fondamental : $\mathbb{Z}/n\mathbb{Z}$

Proposition 26. $n\mathbb{Z}$ est un sous-groupe distingué de $(\mathbb{Z},+)$, si bien que l'on peut définir le quotient $\mathbb{Z}/n\mathbb{Z}$. [ULM21] p. 45

Proposition 27. $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre n.

Proposition 28. On peut définir une structure d'anneau sur $\mathbb{Z}/n\mathbb{Z}$. Le groupe multiplicatif de cet anneau est alors d'ordre $\varphi(n)$.

Corollaire 29. $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est premier.

Proposition 30. Dans le cas du Théorème 7 Point (ii), $\langle g\rangle$ est alors isomorphe à $\mathbb{Z}/n\mathbb{Z}$. [ROM21] p. 14

Exemple 31.

$$\mu_n \cong \mathbb{Z}/n\mathbb{Z}$$

où μ_n désigne le groupe cyclique des racines de l'unité de $\mathbb{C}^*$.

2. Décomposition cyclique

Théorème 32 (Chinois)**.** Soient n et m deux entiers premiers entre eux. Alors, [ULM21] p. 81

$$\mathbb{Z}/nm\mathbb{Z} \equiv \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

Théorème 33 (Kronecker)**.** Soit G un groupe abélien d'ordre $n \geq 2$. Il existe une suite d'entiers $n_1 \geq 2$, n_2 multiple de n_1, …, n_k multiple de n_{k-1} telle que G est isomorphe au groupe produit p. 112

$$\prod_{i=1}^{k} \mathbb{Z}/n_i\mathbb{Z}$$

Exemple 34. Soit $G = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z}$. Alors,

$$\begin{aligned} G &\cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \\ &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \end{aligned}$$

III - Groupes non abéliens finis

Les groupes qui suivent sont, sauf cas particuliers, des groupes non abéliens.

1. Groupes symétrique et alterné

Définition 35. L'ensemble des permutations de $[\![1,n]\!]$ est un groupe pour la composition des applications : c'est le **groupe symétrique**, noté S_n.

p. 55

Remarque 36. S_n est fini, d'ordre $n!$.

Théorème 37 (Cayley)**.** Tout groupe fini d'ordre n est isomorphe à un sous-groupe de S_n.

Définition 38. Soient $l \in \mathbb{N}^*$ et $i_1, \dots, i_l \in [\![1,n]\!]$ des éléments distincts. La permutation $\gamma \in S_n$ définie par

$$\gamma(j) = \begin{cases} j & \text{si } j \notin \{i_1, \dots, i_l\} \\ i_{k+1} & \text{si } j = i_k \text{ avec } k < l \\ i_1 & \text{si } j = i_l \end{cases}$$

et notée $\begin{pmatrix} i_1 & \dots & i_l \end{pmatrix}$ est appelée **cycle** de longueur l et de **support** $\{i_1, \dots, i_l\}$. Un cycle de longueur 2 est une **transposition**.

Exemple 39. $\gamma = \begin{pmatrix} 1 & 4 & 2 & 5 \end{pmatrix} = \begin{pmatrix} 4 & 2 & 5 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 5 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 5 & 1 & 4 & 2 \end{pmatrix}$ est un cycle de S_5 de longueur 4.

Théorème 40. Toute permutation de S_n s'écrit de manière unique (à l'ordre près) comme produit de cycles dont les supports sont deux à deux disjoints.

Exemple 41.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 3 & 5 \end{pmatrix}$$

Définition 42. On appelle **type** d'une permutation $\sigma \in S_n$ et on note $[l_1, \dots, l_m]$ la liste des cardinaux l_i des orbites dans $[\![1,n]\!]$ de l'action du groupe $\langle \sigma \rangle$ sur $[\![1,n]\!]$, rangée dans l'ordre croissant.

Proposition 43. Une permutation de type $[l_1, \dots, l_m]$ a pour ordre $\text{ppcm}(l_1, \dots, l_m)$.

Exemple 44. La permutation de l'Théorème 41 est d'ordre 6.

Définition 45.
— Soit $\sigma \in S_n$. On appelle **signature** de σ, notée $\epsilon(\sigma)$ l'entier $\epsilon(\sigma) = \prod_{i \neq j} \frac{\sigma(i)-\sigma(j)}{i-j}$.
— $\sigma \mapsto \epsilon(\sigma)$ est un morphisme de S_n dans $\{\pm 1\}$, on note A_n son noyau.

Lemme 46. Les 3-cycles sont conjugués dans A_n pour $n \geq 5$. **[PER]** p. 15

Lemme 47. Le produit de deux transpositions est un produit de 3-cycles. **[ROM21]** p. 49

Proposition 48. A_n est engendré par les 3-cycles pour $n \geq 3$.

[DEV]

Théorème 49. A_n est simple pour $n \geq 5$. **[PER]** p. 28

2. Groupe linéaire sur un corps fini

Soit V un espace vectoriel de dimension finie n sur un corps $\mathbb{K}$. **[ULM21]** p. 119

Définition 50.
— Le **groupe linéaire** de V, $\mathrm{GL}(V)$ est le groupe des applications linéaires de V dans lui-même qui sont inversibles.
— Le **groupe spécial linéaire** de V, $\mathrm{SL}(V)$ est le sous-groupe de $\mathrm{GL}(V)$ constitué des applications de déterminant 1.
— Les quotients de ces groupes par leur centre sont respectivement notés $\mathrm{PGL}(V)$ et $\mathrm{PSL}(V)$.

Proposition 51. On se place dans le cas où $\mathbb{K} = \mathbb{F}_q$. Alors, les groupes précédents sont finis, et : p. 124

(i) $|\mathrm{GL}(V)| = q^{\frac{n(n-1)}{2}}((q^n-1)\dots(q-1))$.
(ii) $|\mathrm{PGL}(V)| = |\mathrm{SL}(V)| = \frac{|\mathrm{GL}(V)|}{q-1}$.
(iii) $|\mathrm{PSL}(V)| = |\mathrm{SL}(V)| = \frac{|\mathrm{GL}(V)|}{(q-1)\mathrm{pgcd}(n,q-1)}$.

3. Groupe diédral

Définition 52. Pour un entier $n \geq 1$, le **groupe diédral** D_n est le sous-groupe, de $\mathrm{GL}_2(\mathbb{R})$ engendré par la symétrie axiale s et la rotation d'angle $\theta = \frac{2\pi}{n}$ définies respectivement par les matrices

$$S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ et } R = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

p. 8

Exemple 53. $D_1 = \{\mathrm{id}, s\}$.

Proposition 54. (i) D_n est un groupe d'ordre $2n$.
(ii) $r^n = s^2 = \mathrm{id}$ et $sr = r^{-1}s$.

Proposition 55. Un groupe non cyclique d'ordre 4 est isomorphe à D_2.

p. 28

Exemple 56. S_2 est isomorphe à D_2.

p. 65

Proposition 57. Un groupe fini d'ordre $2p$ avec p premier est soit cyclique, soit isomorphe à D_p.

p. 28

Exemple 58. S_3 est isomorphe à D_3.

Proposition 59. Les sous-groupes de D_n sont soit cyclique, soit isomorphes à un D_m où $m \mid n$.

p. 47

IV - Représentations linéaires de groupes finis

Dans cette partie, G désigne un groupe d'ordre fini.

p. 144

Définition 60.
— Une **représentation linéaire** ρ est un morphisme de G dans $\mathrm{GL}(V)$ où V désigne un espace-vectoriel de dimension finie n sur $\mathbb{C}$.
— On dit que n est le **degré** de ρ.
— On dit que ρ est **irréductible** si $V \neq \{0\}$ et si aucun sous-espace vectoriel de V n'est stable par $\rho(g)$ pour tout $g \in G$, hormis $\{0\}$ et V.

Exemple 61. Soit $\varphi : G \to S_n$ le morphisme structurel d'une action de G sur un ensemble de cardinal n. On obtient une représentation de G sur $\mathbb{C}^n = \{e_1, \dots, e_n\}$ en posant

$$\rho(g)(e_i) = e_{\varphi(g)(i)}$$

c'est la représentation par permutations de G associé à l'action. Elle est de degré n.

Définition 62. La représentation par permutations de G associée à l'action par translation à gauche de G sur lui-même est la **représentation régulière** de G, on la note ρ_G.

Définition 63. On peut associer à toute représentation linéaire ρ, son **caractère** $\chi = \text{trace} \circ \rho$. On dit que χ est **irréductible** si ρ est irréductible.

p. 150

Proposition 64. (i) Les caractères sont des fonctions constantes sur les classes de conjugaison.

(ii) Il y a autant de caractères irréductibles que de classes de conjugaisons.

Définition 65. Soit $\rho : G \to \text{GL}(V)$ une représentation linéaire de G. On suppose $V = W \oplus W_0$ avec W et W_0 stables par $\rho(g)$ pour tout $g \in G$. On dit alors que ρ est **somme directe** de ρ_W et de ρ_{W_0}.

Théorème 66 (Maschke)**.** Toute représentation linéaire de G est somme directe de représentations irréductibles.

Théorème 67. Les sous-groupes distingués de G sont exactement les

$$\bigcap_{i \in I} \text{Ker}(\rho_i) \text{ où } I \in \mathscr{P}([\![1, r]\!])$$

[PEY] p. 231

Corollaire 68. G est simple si et seulement si $\forall i \neq 1, \forall g \neq e_G, \chi_i(g) \neq \chi_i(e_G)$.

105 Groupe des permutations d'un ensemble fini. Applications.

Pour toute cette leçon, on fixe un entier $n \geq 1$.

I - Généralités

1. Définitions

Définition 1. Soit E un ensemble. On appelle **groupe des permutations** de E le groupe des bijections de E dans lui-même. On le note $S(E)$.

[ROM21] p. 37

Notation 2. Si $E = [\![1, n]\!]$, on note $S(E) = S_n$, le groupe symétrique à n éléments.

Notation 3. Soit $\sigma \in S_n$. On note :

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

pour signifier que σ est la bijection $\sigma : k \mapsto \sigma(k)$.

Le théorème suivant justifie que, pour un ensemble à n éléments, on peut se contenter d'étudier S_n en lieu et place de $S(E)$.

Théorème 4. (i) Soient E et F deux ensembles en bijection. Alors $S(E)$ et $S(F)$ sont isomorphes.

(ii)
$$|S_n| = n!$$

Théorème 5 (Cayley)**.** Tout groupe G est isomorphe à un sous-groupe de $S(G)$.

p. 53

2. Orbites et cycles

Définition 6. Soit $\sigma \in [\![1, n]\!]$. On a une action naturelle de $H = \langle \sigma \rangle$ sur $[\![1, n]\!]$ définie par

$$\forall k \in \mathbb{Z}, \forall j \in [\![1, n]\!], \sigma^k \cdot j = \sigma^k(j)$$

Les orbites pour cette action sont les $H \cdot j = \{\sigma(j) \mid j \in [\![1, n]\!]\}$. On les note $\mathcal{O}_\sigma(j)$.

p. 41

Remarque 7. — Les orbites selon σ sont décrites par la relation

$$x \sim y \iff \exists k \in \mathbb{Z} \text{ tel que } y = \sigma^k(x)$$

— Une orbite $\mathcal{O}_\sigma(j)$ est réduite à un point si et seulement si $\sigma(j) = j$.

Définition 8. Soient $l \leq n$ et $i_1, \dots, i_l \in [\![1, n]\!]$ des éléments distincts. La permutation $\gamma \in S_n$ définie par

$$\gamma(j) = \begin{cases} j & \text{si } j \notin \{i_1, \dots, i_l\} \\ i_{k+1} & \text{si } j = i_k \text{ avec } k < l \\ i_1 & \text{si } j = i_l \end{cases}$$

et notée $\begin{pmatrix} i_1 & \dots & i_l \end{pmatrix}$ est appelée **cycle** de longueur l et de **support** $\{i_1, \dots, i_l\}$. Un cycle de longueur 2 est une **transposition**.

p. 37

Proposition 9. Une permutation σ est cycle si et seulement s'il n'y a qu'une seule orbite $\mathcal{O}_\sigma(j)$ non réduite à un point.

p. 42

Remarque 10. La composée de deux cycles n'est pas un cycle en général.

Exemple 11. Avec $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix} \in S_4$, on a $\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ qui n'est pas un cycle.

Proposition 12. L'ordre d'un cycle est égal à sa longueur.

Proposition 13. Soient σ et τ deux cycles de S_n dont on note respectivement $\text{Supp}(\sigma)$ et $\text{Supp}(\tau)$ les supports. Si $\text{Supp}(\sigma) \cap \text{Supp}(\tau) = \emptyset$, alors $\text{Supp}(\sigma\tau) = \text{Supp}(\sigma) \cup \text{Supp}(\tau)$ et dans ce cas :

(i) $\sigma\tau = \tau\sigma$.

(ii) $\sigma\tau = \text{id} \implies \sigma = \tau = \text{id}$.

[ULM21] p. 56

Théorème 14. Toute permutation de S_n s'écrit de manière unique (à l'ordre près) comme produit de cycles dont les supports sont deux à deux disjoints.

Exemple 15.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 \end{pmatrix}\begin{pmatrix} 3 & 5 \end{pmatrix}$$

Définition 16. On appelle **type** d'une permutation $\sigma \in S_n$ et on note $[l_1, \dots, l_m]$ la liste des cardinaux l_i des orbites dans $[\![1, n]\!]$ de l'action du groupe $\langle\sigma\rangle$ sur $[\![1, n]\!]$, rangée dans l'ordre croissant.

Proposition 17. Une permutation de type $[l_1, \dots, l_m]$ a pour ordre $\text{ppcm}(l_1, \dots, l_m)$.

Exemple 18. La permutation de l'Théorème 15 est d'ordre 6.

3. Signature

Définition 19. Soit $\sigma \in S_n$. On appelle **signature** de σ, notée $\epsilon(\sigma)$ le nombre rationnel

$$\epsilon(\sigma) = \prod_{i \neq j} \frac{\sigma(i) - \sigma(j)}{i - j}$$

Exemple 20.

$$\epsilon(\begin{pmatrix} 1 & 2 \end{pmatrix}) = -1$$

Proposition 21. $\epsilon : S_n \to \mathbb{Q}^*$ est un morphisme de groupes. Pour une permutation $\sigma \in S_n$, on a les propriétés suivantes :

(i) Si σ est un transposition, $\epsilon(\sigma) = -1$.

(ii) Si l est le nombre de transpositions qui apparaît dans une décomposition de σ en produit de transpositions, alors $\epsilon(\sigma) = (-1)^l$.

(iii) Si σ est de type $[l_1, \dots, l_m]$, alors $\epsilon(\sigma) = (-1)^{l_1 + \dots + l_m - m}$.

En particulier, si $n \geq 2$, l'image de ϵ est le sous-groupe $\{\pm 1\}$ de $\mathbb{Q}^*$.

Proposition 22. Le seul morphisme non trivial de S_n dans $\mathbb{C}^*$ est ϵ. **[PEY]** p. 20

Définition 23. — Soit $\sigma \in S_n$. Si $\epsilon(\sigma) = 1$, on dit que σ est **paire**. Sinon, on dit qu'elle est **impaire**. **[ULM21]** p. 64

— Le noyau de ϵ (constitué donc des permutations paires) est un sous-groupe distingué de S_n appelé **groupe alterné** et noté A_n.

Proposition 24. Pour $n \geq 2$,

$$|A_n| = \frac{n!}{2}$$

II - Structure

1. Conjugaison

Proposition 25. Deux permutations σ et τ de S_n sont conjuguées si et seulement si elles sont du même type. En particulier, pour $\omega \in S_n$ et tout cycle $\begin{pmatrix} i_1 & \dots & i_l \end{pmatrix} \in S_n$, on a :

$$\omega \begin{pmatrix} i_1 & \dots & i_l \end{pmatrix} \omega^{-1} = \begin{pmatrix} \omega(i_1) & \dots & \omega(i_l) \end{pmatrix}$$

p. 60

Exemple 26. Les types possibles d'une permutation de S_4 sont [1] (l'identité), [2] (les transpositions), [2,2] (les doubles transpositions), [3] (les 3-cycles) et [4] (les 4-cycles) : on a 5 classes de conjugaison de tailles respectives 1, 6, 3, 8 et 6.

Proposition 27. Pour tout $n \geq 3$, $Z(S_n) = \{\sigma \in S_n \mid \forall \tau \in S_n, \sigma\tau = \tau\sigma\} = \{\mathrm{id}\}$.

[PER] p. 13

Lemme 28. Les 3-cycles sont conjugués dans A_n pour $n \geq 5$.

p. 15

2. Générateurs

Proposition 29. (i) S_n est engendré par les transpositions. On peut même se limiter aux transpositions de la forme $\begin{pmatrix} 1 & k \end{pmatrix}$ ou encore $\begin{pmatrix} k & k+1 \end{pmatrix}$ (pour $k \leq n$).

(ii) S_n est engendré par $\begin{pmatrix} 1 & 2 \end{pmatrix}$ et $\begin{pmatrix} 1 & \dots & n \end{pmatrix}$.

[ROM21] p. 44

Exemple 30. Pour $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \end{pmatrix}\begin{pmatrix} 6 & 7 \end{pmatrix}$, on a $\sigma = \begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 2 & 3 \end{pmatrix}\begin{pmatrix} 3 & 4 \end{pmatrix}\begin{pmatrix} 4 & 5 \end{pmatrix}\begin{pmatrix} 6 & 7 \end{pmatrix}$.

Proposition 31. A_n est engendré par les 3-cycles pour $n \geq 3$.

3. Simplicité

Lemme 32. Les 3-cycles sont conjugués dans A_n pour $n \geq 5$.

[PER] p. 15

Lemme 33. Le produit de deux transpositions est un produit de 3-cycles.

[ROM21] p. 49

[DEV]

Théorème 34. A_n est simple pour $n \geq 5$.

[PER] p. 28

Corollaire 35. Le groupe dérivé de A_n est A_n pour $n \geq 5$, et le groupe dérivé de S_n est A_n pour $n \geq 2$.

Corollaire 36. Pour $n \geq 5$, les sous-groupes distingués de S_n sont S_n, A_n et $\{\mathrm{id}\}$.

Corollaire 37. Soit H un sous-groupe d'indice n de S_n. Alors, H est isomorphe à S_{n-1}.

III - Applications

1. Déterminant

Soit $\mathbb{K}$ un corps et soit E un espace vectoriel de dimension n sur $\mathbb{K}$.

[GOU21] p. 140

Définition 38. Soient $E_1, \dots, E_p$ et F des espaces vectoriels sur $\mathbb{K}$ et $f : E_1, \dots, E_p \to F$.

- f est dite **p-linéaire** si en tout point les p applications partielles sont linéaires.
- Si f est p-linéaire et si $E_1 = \cdots = E_p$ ainsi que $F = \mathbb{K}$, f est une **forme p-linéaire**. On note $\mathscr{L}_p(E, \mathbb{K})$ l'ensemble des formes p-linéaires sur E.
- Si de plus $f(x_1, \dots, x_p) = 0$ dès que deux vecteurs parmi les x_i sont égaux, alors f est dite **alternée**.

Exemple 39. En reprenant les notations précédentes, pour $p = 2$, f est bilinéaire.

Proposition 40. $\mathscr{L}_p(E, \mathbb{K})$ est un espace vectoriel et, $\dim(\mathscr{L}_p(E, \mathbb{K})) = |\dim(E)|^p$.

Théorème 41. L'ensemble des formes p-linéaires alternées sur E est un $\mathbb{K}$-espace vectoriel de dimension 1. De plus, il existe une unique forme p-linéaire alternée f prenant la valeur 1 sur une base $\mathscr{B}$ de E. On note $f = \det_{\mathscr{B}}$.

Définition 42. $\det_{\mathscr{B}}$ est l'application **déterminant** dans la base $\mathscr{B}$. En l'absence d'ambiguïté, on s'autorise à noter $\det = \det_{\mathscr{B}}$.

Proposition 43. Soit $\mathscr{B} = (e_1, \dots, e_n)$ une base de E. Si $x_1, \dots, x_n \in E$ ($\forall i \in [\![1, n]\!]$, on peut écrire $x_i = \sum_{j=1}^{n} x_{i,j} e_j$), on a la formule $\det_{\mathscr{B}}(x_1, \dots, x_n) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^{n} x_{i,\sigma(i)}$.

Corollaire 44. Soit $\mathscr{B}$ une base de E.

(i) Si $\mathscr{B}'$ est une autre base de E, alors $\det_{\mathscr{B}'} = \det_{\mathscr{B}'}(\mathscr{B})\det_{\mathscr{B}}$.

(ii) Une famille de vecteurs est liée si et seulement si son déterminant est nul dans une base quelconque de E.

(iii) Soient $A, B \in \mathscr{M}_n(\mathbb{K})$, alors $\det_{\mathscr{B}}(AB) = \det_{\mathscr{B}}(A)\det_{\mathscr{B}}(B)$.

(iv) Soit $A \in \mathscr{M}_n(\mathbb{K})$, alors $\det_{\mathscr{B}}(A) = \det_{\mathscr{B}}({}^tA)$ et pour tout $\lambda \in \mathbb{K}$, $\det_{\mathscr{B}}(\lambda A) = \lambda^n \det_{\mathscr{B}}(A)$.

(v) Si on effectue une permutation $\sigma \in S_n$ sur les colonnes d'une matrice A, alors le déterminant de A est multiplié par $\epsilon(\sigma)$.

Notation 45. Soit $a \in \mathbb{F}_p$. On note $\left(\frac{a}{p}\right)$ le symbole de Legendre de a modulo p.

[I-P] p. 203

Lemme 46. Soient $p \geq 3$ un nombre premier et V un espace vectoriel sur $\mathbb{F}_p$ de dimension finie. Les dilatations engendrent $\mathrm{GL}(V)$.

[DEV]

Théorème 47 (Frobenius-Zolotarev)**.** Soient $p \geq 3$ un nombre premier et V un espace vectoriel sur $\mathbb{F}_p$ de dimension finie.

$$\forall u \in \mathrm{GL}(V), \epsilon(u) = \left(\frac{\det(u)}{p}\right)$$

où u est vu comme une permutation des éléments de V.

2. Matrices de permutation

Soit $\mathbb{K}$ un corps et soit E un espace vectoriel de dimension n sur $\mathbb{K}$.

[ROM21] p. 54

Définition 48. À tout $\sigma \in S_n$ on associe la matrice de passage de la base canonique $(e_i)_{i\in[\![1,n]\!]}$ à la base $(e_{\sigma}(i))_{i\in[\![1,n]\!]}$ que l'on note P_σ : c'est la **matrice de permutation** associée à σ.

Remarque 49. En reprenant les notations précédentes, $\forall j \in [\![1,n]\!]$, $P_\sigma e_j = \sigma(e_j)$.

Proposition 50. $\sigma \mapsto P_\sigma$ est un morphisme de groupes injectif de S_n dans $\mathrm{GL}_n(\mathbb{K})$. De plus, on a

$$\det(P_\sigma) = \epsilon(\sigma)$$

Corollaire 51. Tout groupe fini d'ordre n est isomorphe à un sous groupe de $\mathrm{GL}_n(\mathbb{F}_p)$ pour un premier $p \geq 2$.

3. Polynômes symétriques

Soit $\mathbb{K}$ un corps de caractéristique différente de 2.

[GOU21] p. 83

Définition 52. Soit $P \in \mathbb{K}[X_1, \dots, X_n]$. On dit que P est **symétrique** si

$$\forall \sigma \in S_n, P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$$

Exemple 53. Dans $\mathbb{R}[X]$, le polynôme $XY + YZ + ZX$ est symétrique.

Définition 54. On appelle **polynômes symétriques élémentaires** de $A[X_1, \dots, X_n]$ les polynômes noté Σ_p où $p \in [\![1, n]\!]$ définis par

$$\Sigma_p = \sum_{1 \leq i_1 < \cdots < i_p \leq n} X_{i_1} \dots X_{i_p}$$

Exemple 55.
- $\Sigma_1 = X_1 + \cdots + X_n$.
- $\Sigma_2 = \sum_{1 \leq i < j \leq n} X_i X_j$.
- $\Sigma_n = X_1 \dots X_n$.

Remarque 56. Si $P \in A[X_1, \dots, X_n]$, alors $P(\Sigma_1(X_1, \dots, X_n), \dots, \Sigma_n(X_1, \dots, X_n))$ est symétrique. Et la réciproque est vraie.

Théorème 57 (Théorème fondamental des polynômes symétriques)**.** Soit $P \in A[X_1, \dots, X_n]$ un polynôme symétrique. Alors,

$$\exists ! \Phi \in A[X_1, \dots, X_n] \text{ tel que } \Phi(\Sigma_1, \dots, \Sigma_n)$$

Exemple 58. $P = X^3 + Y^3 + Z^3$ s'écrit $P = \Sigma_1^3 - 3\Sigma_1\Sigma_2 + 3\Sigma_3$.

Application 59 (Relations coefficients - racines)**.** Soit $P = a_0 X^n + \cdots + a_n \in \mathbb{K}[X]$ avec $a_0 \neq 0$ scindé sur $\mathbb{K}$, dont les racines (comptées avec leur ordre de multiplicité) sont $x_1, \dots, x_n$. Alors

p. 64

$$\forall p \in [\![1, n]\!], \Sigma_p(x_1, \dots, x_n) = (-1)^p \frac{a_p}{a_0}$$

En particulier,

— $\Sigma_1(x_1,\dots,x_n) = \sum_{i=1}^n x_i = -\frac{a_1}{a_0}$.

— $\Sigma_n(x_1,\dots,x_n) = \prod_{i=1}^n x_i = (-1)^n \frac{a_n}{a_0}$.

Application 60 (Théorème de Kronecker)**.** Soit $P \in \mathbb{Z}[X]$ unitaire tel que toutes ses racines complexes appartiennent au disque unité épointé en l'origine (que l'on note D). Alors toutes ses racines sont des racines de l'unité.

[I-P] p. 279

Corollaire 61. Soit $P \in \mathbb{Z}[X]$ unitaire et irréductible sur $\mathbb{Q}$ tel que toutes ses racines complexes soient de module inférieur ou égal à 1. Alors $P = X$ ou P est un polynôme cyclotomique.

106 Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $\mathrm{GL}(E)$. Applications.

Soit E un espace vectoriel de dimension finie $n \geq 1$ sur un corps $\mathbb{K}$.

I - Étude du groupe linéaire

1. $\mathrm{GL}(E)$ et son lien avec l'algèbre des matrices

Définition 1. Le **groupe linéaire** de E est le groupe des applications $\mathbb{K}$-linéaires bijectives de E dans E.

[ROM21] p. 139

Remarque 2. Le choix d'une base de E permet de réaliser un isomorphisme d'algèbre de $\mathscr{L}(E)$ sur $\mathscr{M}_n(\mathbb{K})$ et cet isomorphisme induit un isomorphisme de $\mathrm{GL}(E)$ sur $\mathrm{GL}_n(\mathbb{K})$.Cet isomorphisme se définit à l'aide du choix d'une base, il n'est donc pas canonique.

[PER] p. 95

Pour cette raison, on pourra par la suite confondre $\mathrm{GL}(E)$ et $\mathrm{GL}_n(\mathbb{K})$.

Proposition 3. $\det : \mathrm{GL}(E) \to \mathbb{K}^*$ est un morphisme surjectif.

Théorème 4. Soit $u \in \mathscr{L}(E)$. Les assertions suivantes sont équivalentes :

(i) $u \in \mathrm{GL}(E)$.
(ii) $\mathrm{Ker}(u) = \{0\}$.
(iii) $\mathrm{Im}(u) = E$.
(iv) $\mathrm{rang}(u) = n$.
(v) $\det(u) = 0$.
(vi) u transforme toute base de E en une base de E.
(vii) Il existe $v \in \mathscr{L}(E)$ tel que $u \circ v = \mathrm{id}_E$.
(viii) Il existe $w \in \mathscr{L}(E)$ tel que $w \circ u = \mathrm{id}_E$.

[ROM21] p. 140

2. Centre

Proposition 5. Soit $u \in \mathrm{GL}(E)$ un endomorphisme laissant invariantes toutes les droites vectorielles de E. Alors u est une homothétie.

[PER] p. 98

Théorème 6.

$$\mathrm{GL}(E) = \mathbb{K}^* \cdot \mathrm{id}_E$$

3. Sous-groupes notables

a. Groupe orthogonal

Définition 7. Un endomorphisme $u \in \mathscr{L}(E)$ est dit **orthogonal** (ou est une **isométrie**) s'il est tel que $\langle u(x), u(y)\rangle = \langle x, y\rangle$ pour tout $x, y \in E$. On note $\mathscr{O}(E)$ l'ensemble des endomorphismes orthogonaux de E. [ROM21] p. 720

Exemple 8.
— Les seules homothéties qui sont des isométries sont $-\mathrm{id}_E$ et id_E.
— Si $n = 1$, on a $\mathscr{O}(E) = \{\pm \mathrm{id}_E\}$.

Proposition 9. Soit $u \in \mathscr{L}(E)$. p. 743

$$u = \mathscr{O}(E) \iff \forall x \in E,\ \|u(x)\| \iff u \in \mathrm{GL}(E) \text{ et } u^{-1} = u^*$$

Théorème 10. Les isométries sont des automorphismes. Il en résulte que $\mathscr{O}(E)$ est un sous-groupe de $\mathrm{GL}(E)$. p. 721

Remarque 11. Ce n'est pas vrai en dimension infinie.

Théorème 12. Un endomorphisme de E est une isométrie si et seulement s'il transforme toute base orthonormée de E en une base orthonormée.

Théorème 13. Un endomorphisme de E est une isométrie si et seulement si sa matrice A dans une base orthonormée est inversible, d'inverse ${}^tA$.

On dit alors que A est **orthogonale**.

Notation 14. On note $\mathscr{O}_n(\mathbb{R})$ le groupe des matrices orthogonales.

Théorème 15.

$$\forall u \in \mathscr{O}(E),\ \det(u) = \pm 1$$

Remarque 16. On a des résultats équivalents pour les matrices.

Théorème 17 (Réduction des endomorphismes orthogonaux)**.** Soit $u \in \mathscr{O}(E)$. Alors, il existe

$\mathscr{B}$ une base orthonormée de E telle que la matrice de u dans $\mathscr{B}$ est

$$\begin{pmatrix} I_p & 0 & 0 & \dots & 0 \\ 0 & -I_q & 0 & \dots & 0 \\ 0 & 0 & R_1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & R_r \end{pmatrix}$$

où $R_i = \begin{pmatrix} \cos(\theta_i) & -\sin(\theta_i) \\ \sin(\theta_i) & \cos(\theta_i) \end{pmatrix}$ avec $\forall i \in [\![1, r]\!], \theta_i \in]0, 2\pi[$.

b. Groupe spécial linéaire

Définition 18. On définit $\mathrm{SL}(E) = \mathrm{Ker}(\det)$ le **groupe spécial linéaire** de E.

p. 141

Remarque 19. On peut définir de manière analogue $\mathrm{SL}_n(\mathbb{K})$, et on a encore un isomorphisme entre ces deux groupes.

Théorème 20. $\mathrm{SL}(E)$ est un sous-groupe distingué de $\mathrm{GL}(E)$. Le groupe quotient $\mathrm{GL}(E)/\mathrm{SL}(E)$ est isomorphe à $\mathbb{K}^*$ et on a la suite exacte :

$$\{\mathrm{id}_E\} \to \mathrm{SL}(E) \to \mathrm{GL}(E) \xrightarrow{\det} \mathbb{K}^* \to \{\mathrm{id}_E\}$$

Théorème 21.

$$Z(\mathrm{SL}(E)) = \mu_n(\mathbb{K}) \cdot \mathrm{id}_E$$

où $\mu_n(\mathbb{K})$ désigne le groupe des racines de l'unité de $\mathbb{K}$.

Proposition 22. Soit $u \in \mathrm{GL}(E) \setminus \{\mathrm{id}_E\}$. Soit H un hyperplan de E tel que $u_{|H} = \mathrm{id}_H$. Les assertions suivantes sont équivalentes :

[PER] p. 97

(i) $\det(u) = 1$.

(ii) u n'est pas diagonalisable.

(iii) $\mathrm{Im}(u - \mathrm{id}_E) \subseteq H$.

(iv) Le morphisme induit $\overline{u} : E/H \to E/H$ est l'identité de E/H.

(v) En notant $H = \mathrm{Ker}(f)$ (où f désigne une forme linéaire sur E), il existe $a \in H \setminus \{0\}$ tel que

$$u = \mathrm{id}_E + f \cdot a$$

(vi) Dans une base adaptée, la matrice de u s'écrit

$$\begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Définition 23. En reprenant les notations précédentes, on dit que u est une **transvection** d'hyperplan H et de droite $\mathrm{Vect}(a)$.

Proposition 24. Soient $u \in \mathrm{GL}(E)$ et τ une transvection d'hyperplan H et de droite D. Alors, $u\tau u^{-1}$ est une transvection d'hyperplan $u(H)$ et de droite $u(D)$.

Théorème 25. Si $n \geq 2$, les transvections engendrent $\mathrm{SL}(E)$.

4. Générateurs

Proposition 26. Soit $u \in \mathrm{GL}(E)$. Soit H un hyperplan de E tel que $u_{|H} = \mathrm{id}_H$. Les assertions suivantes sont équivalentes :

(i) $\det(u) = \lambda \neq 1$.

(ii) u admet une valeur propre $\lambda \neq 1$.

(iii) $\mathrm{Im}(u - \mathrm{id}_E) \subsetneq H$.

(iv) Dans une base adaptée, la matrice de u s'écrit

$$\begin{pmatrix} I_{n-1} & 0 \\ 0 & \lambda \end{pmatrix}$$

avec $\lambda \neq 1$.

Définition 27. En reprenant les notations précédentes, on dit que u est une **dilatation** de rapport λ.

Théorème 28. Si $n \geq 2$, les transvections et les dilatations engendrent $\mathrm{GL}(E)$.

Notation 29. Soit $a \in \mathbb{F}_p$. On note $\left(\frac{a}{p}\right)$ le symbole de Legendre de a modulo p.

[I-P] p. 203

Lemme 30. Soient $p \geq 3$ un nombre premier et V un espace vectoriel sur $\mathbb{F}_p$ de dimension finie. Les dilatations engendrent $\mathrm{GL}(V)$.

[DEV]

Application 31 (Théorème de Frobenius-Zolotarev)**.** Soient $p \geq 3$ un nombre premier et V un espace vectoriel sur $\mathbb{F}_p$ de dimension finie.

$$\forall u \in \mathrm{GL}(V), \epsilon(u) = \left(\frac{\det(u)}{p}\right)$$

où u est vu comme une permutation des éléments de V.

5. Groupes projectifs

Définition 32. On définit $\mathrm{PGL}(E)$ (resp. $\mathrm{PSL}(E)$) le quotient de $\mathrm{GL}(E)$ (resp. $\mathrm{SL}(E)$) par son centre.

[ROM21] p. 141

Proposition 33.

$$Z(\mathrm{PGL}(E)) = Z(\mathrm{PSL}(E)) = \{\mathrm{id}_E\}$$

On se place pour la suite de cette sous-section dans le cas où $\mathbb{K} = \mathbb{F}_q$.

[ULM21] p. 124

Proposition 34. Les groupes précédents sont finis, et :

(i) $|\mathrm{GL}(E)| = q^{\frac{n(n-1)}{2}}((q^n-1)\dots(q-1))$.

(ii) $|\mathrm{PGL}(E)| = |\mathrm{SL}(E)| = \frac{|\mathrm{GL}(E)|}{q-1}$.

(iii) $|\mathrm{PSL}(E)| = |\mathrm{SL}(E)| = \frac{|\mathrm{GL}(E)|}{(q-1)\mathrm{pgcd}(n,q-1)}$.

Application 35. Pour tout entier $p \in [\![1, n]\!]$, il y a

$$\frac{\prod_{k=n-(p-1)}^{n}(q^k-1)}{\prod_{k=1}^{p}(q^k-1)}$$

sous-espaces vectoriels de dimension p dans E.

[ROM21] p. 157

II - Actions sur l'algèbre des matrices

1. Action par translation

Proposition 36. Les applications

$$\begin{array}{ccc} \mathrm{GL}_n(\mathbb{K}) \times \mathcal{M}_n(\mathbb{K}) & \to & \mathcal{M}_n(\mathbb{K}) \\ (P, A) & \mapsto & PA \end{array}$$

[ROM21] p. 184

et

$$\begin{array}{ccc} \mathrm{GL}_n(\mathbb{K}) \times \mathcal{M}_n(\mathbb{K}) & \to & \mathcal{M}_n(\mathbb{K}) \\ (P, A) & \mapsto & AP^{-1} \end{array}$$

définissent une action de $\mathrm{GL}_n(\mathbb{K})$ sur $\mathcal{M}_n(\mathbb{K})$.

Remarque 37. Pour la première action, deux matrices sont dans la même orbite si et seulement si elles ont même noyau. Pour la seconde, deux matrices sont dans la même orbite si et seulement si elles ont même image.

Lemme 38. [C-G] p. 376

$$\forall A \in \mathcal{S}_n^{++}(\mathbb{R}) \, \exists! B \in \mathcal{S}_n^{++}(\mathbb{R}) \text{ telle que } B^2 = A$$

[DEV]

Théorème 39 (Décomposition polaire)**.** L'application

$$\mu : \begin{array}{ccc} \mathcal{O}_n(\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R}) & \to & \mathrm{GL}_n(\mathbb{R}) \\ (O, S) & \mapsto & OS \end{array}$$

est un homéomorphisme.

Remarque 40. Ainsi, pour toute matrice $A \in \mathrm{GL}_n(\mathbb{R})$, il existe un représentant de $\mathcal{O}_n(\mathbb{R})$ pour l'action par translation à gauche.

2. Action par conjugaison

Proposition 41. L'application [ROM21] p. 199

$$\begin{array}{ccc} \mathrm{GL}_n(\mathbb{K}) \times \mathcal{M}_n(\mathbb{K}) & \to & \mathcal{M}_n(\mathbb{K}) \\ (P, A) & \mapsto & PAP^{-1} \end{array}$$

définit une action de $\mathrm{GL}_n(\mathbb{K})$ sur $\mathcal{M}_n(\mathbb{K})$.

Définition 42. Deux matrices qui sont dans la même orbite pour cette action sont dites **semblables**.

Remarque 43. Deux matrices semblables représentes la même application linéaire dans deux bases de $\mathbb{K}^n$. [GOU21] p. 127

[ROM21] p. 199

Théorème 44. Soient A et B deux matrices semblables. Alors :

— $\mathrm{trace}(A) = \mathrm{trace}(B)$.

— $\det(A) = \det(B)$.

— $\mathrm{rang}(A) = \mathrm{rang}(B)$.

— $\chi_A = \chi_B$.

— $\pi_A = \pi_B$.

Contre-exemple 45. Les matrices $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ ont la même trace, le même déterminant, le même polynôme caractéristique, mais ne sont pas semblables.

[D-L] p. 137

Théorème 46. Soient $\mathbb{L}$ une extension de $\mathbb{K}$ et $A, B \in \mathcal{M}_n(\mathbb{K})$. On suppose $\mathbb{K}$ infini et A, B semblables sur $\mathbb{L}$. Alors A et B sont semblables sur $\mathbb{K}$.

[GOU21] p. 167

3. Action par congruence

On suppose $\mathbb{K}$ de caractéristique différente de 2.

[ROM21] p. 206

Proposition 47. L'application

$$\begin{array}{ccc} \mathrm{GL}_n(\mathbb{K}) \times \mathcal{S}_n(\mathbb{K}) & \to & \mathcal{S}_n(\mathbb{K}) \\ (P, A) & \mapsto & PA^tP \end{array}$$

définit une action de $\mathrm{GL}_n(\mathbb{K})$ sur $\mathcal{S}_n(\mathbb{K})$.

Définition 48. Deux matrices qui sont dans la même orbite pour cette action sont dites **congruentes**.

Remarque 49. Deux matrices congruentes représentent la même forme quadratique dans deux bases de $\mathbb{K}^n$.

Théorème 50 (Spectral)**.** Toute matrice symétrique est congruente à une matrice diagonale.

Théorème 51. (i) Si $\mathbb{K} = \mathbb{C}$: deux matrices symétriques A et B sont congruentes si et seulement si elles ont même rang. Les orbites pour cette action sont les ensembles

$$\mathcal{O}_r = \{A \in \mathcal{S}_n(\mathbb{C}) \mid \mathrm{rang}(A) = r\}$$

pour $r \in [\![1, n]\!]$.

(ii) Si $\mathbb{K} = \mathbb{R}$: deux matrices symétriques A et B sont congruentes si et seulement si elles ont même signature. Les orbites pour cette action sont les ensembles

$$\mathcal{O}_{(s,r)} = \{A \in \mathcal{S}_n(\mathbb{C}) \mid \text{sign}(\Phi_A) = (s,t)\}$$

où Φ_A désigne la forme quadratique associée à une matrice $A \in \mathcal{S}_n(\mathbb{R})$.

(iii) Si $\mathbb{K} = \mathbb{F}_q$: deux matrices symétriques A et B sont congruentes si et seulement si elles même déterminant modulo q.

III - Topologie

On se place pour la suite de cette sous-section dans le cas où $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. On munit E d'une norme $\|.\|$ et on note $|||.|||$ la norme subordonnée associée. p. 159

Proposition 52. L'espace $(\mathcal{L}(E), |||.|||)$ des applications continues de E dans E est une algèbre de Banach.

Théorème 53. $\text{GL}(E)$ est un ouvert dense de $\mathcal{L}(E)$ et l'application $u \mapsto u^{-1}$ est continue sur $\text{GL}(E)$.

Proposition 54. (i) $\text{SO}_n(\mathbb{R})$ est compact (et connexe). [C-G] p. 62

(ii) $\mathcal{O}_n(\mathbb{R})$ est compact (non-connexe).

Proposition 55. Tout sous-groupe compact de $\text{GL}_n(\mathbb{R})$ qui contient $\mathcal{O}_n(\mathbb{R})$ est $\mathcal{O}_n(\mathbb{R})$. p. 379

Proposition 56. $\text{GL}_n(\mathbb{R})^+$ est connexe. p. 401

108 Exemples de parties génératrices d'un groupe. Applications.

I - Généralités

Soit G un groupe.

1. Définitions

Lemme 1. Une intersection (quelconque) de sous-groupes de G est un sous-groupe de G. [ROM21] p. 10

Définition 2. Soit $X \subseteq G$. On appelle **sous-groupe engendré** par X, le plus petit sous-groupe (pour l'inclusion) de G contenant X. C'est l'intersection des sous-groupes de G contenant X. On le note $\langle X \rangle$ ou $\langle x_1, \dots, x_n$ si $X = \{x_1, \dots, x_n\}$.

Proposition 3. Soit $X \subseteq G$. On pose $X^{-1} = \{x^{-1} \mid x \in X\}$. Alors,

$$\langle X \rangle = \{x_1 \dots x_n \mid (x_1 \dots x_n) \in X \cup X^{-1},\ n \in \mathbb{N}^*\}$$

Définition 4. Une **partie génératrice** de G est un sous-ensemble $X \subseteq G$ tel que $G = \langle X \rangle$.

Exemple 5. Soit D_G l'ensemble des commutateurs de G (ie. éléments de la forme ghg^{-1} pour $g, h \in G$). On pose $D(G) = \langle D_G \rangle$: $D(G)$ est le groupe dérivé de G, c'est le plus grand sous-groupe tel que $G/D(G)$ est abélien.

2. Groupes monogènes

Définition 6. On dit que G est **monogène** s'il existe $g \in G$ tel que $G = \langle g \rangle$, et on dit que G est cyclique s'il est monogène et fini.

Exemple 7. (i) $\mathbb{Z}$ est monogène, l'ensemble de ses générateurs est $\mathbb{Z}^\times = \{\pm 1\}$.
(ii) $\mathbb{Z}/n\mathbb{Z}$, l'ensemble de ses générateurs est $(\mathbb{Z}/n\mathbb{Z})^\times = \{k \in \mathbb{Z}/n\mathbb{Z} \mid \text{pgcd}(k, n) = 1\}$.

Théorème 8. (i) Si G est monogène infini, alors $G \cong \mathbb{Z}$.
(ii) Si G est cyclique d'ordre n, alors $G \cong \mathbb{Z}/n\mathbb{Z}$.

Corollaire 9. Si $G = \langle g \rangle$ est cyclique d'ordre n, alors l'ensemble de ses générateurs est $\{g^k \mid \text{pgcd}(k,n) = 1\}$.

Définition 10. L'ordre d'un élément $g \in G$ est le cardinal de l'ensemble $\langle g \rangle$. p. 6

Remarque 11. $g \in G$ est d'ordre n si et seulement si $g^n = e_G$ et $g^k \neq e_G$ pour tout $k \in [\![1, n-1]\!]$.

Proposition 12. Un groupe de cardinal premier est cyclique. p. 14

Théorème 13. On suppose $G = \langle g \rangle$ cyclique d'ordre n.

(i) Les sous-groupes de G sont cycliques d'ordre divisant n.

(ii) Pour tout diviseur d de n, il existe un unique sous-groupe d'ordre d : $\langle g^{\frac{n}{d}} \rangle$.

Remarque 14. Le résultat précédent est en fait caractéristique des groupes cycliques.

3. Structure des groupes abéliens de type fini

On suppose dans cette sous-section que G est abélien.

[ULM21] p. 105

Définition 15. G est dit de **type fini** s'il existe une partie génératrice finie de G.

Théorème 16 (Kronecker)**.** On suppose G abélien de type fini. Il existe $r \in \mathbb{N}$ et une suite d'entiers $n_1 \geq 2$, n_2 multiple de n_1, …, n_k multiple de n_{k-1} telle que G est isomorphe au groupe produit

$$\prod_{i=1}^{k} \mathbb{Z}/n_i\mathbb{Z} \times Z^r$$

p. 112

Exemple 17. Si $G = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z}$. Alors,

$$\begin{aligned} G &\cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \\ &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \end{aligned}$$

II - Exemples de parties génératrices

1. Groupe symétrique

Définition 18. Soit E un ensemble. On appelle **groupe des permutations** de E le groupe des bijections de E dans lui-même. On le note $S(E)$.

[ROM21] p. 37

Notation 19. Si $E = [\![1, n]\!]$, on note $S(E) = S_n$, le groupe symétrique à n éléments.

Notation 20. Soit $\sigma \in S_n$. On note :

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

pour signifier que σ est la bijection $\sigma : k \mapsto \sigma(k)$.

Définition 21. Soient $l \leq n$ et $i_1, \dots, i_l \in [\![1, n]\!]$ des éléments distincts. La permutation $\gamma \in S_n$ définie par

$$\gamma(j) = \begin{cases} j & \text{si } j \notin \{i_1, \dots, i_l\} \\ i_{k+1} & \text{si } j = i_k \text{ avec } k < l \\ i_1 & \text{si } j = i_l \end{cases}$$

et notée $\begin{pmatrix} i_1 & \dots & i_l \end{pmatrix}$ est appelée **cycle** de longueur l et de **support** $\{i_1, \dots, i_l\}$. Un cycle de longueur 2 est une **transposition**.

Proposition 22. (i) S_n est engendré par les transpositions. On peut même se limiter aux transpositions de la forme $\begin{pmatrix} 1 & k \end{pmatrix}$ ou encore $\begin{pmatrix} k & k+1 \end{pmatrix}$ (pour $k \leq n$).

(ii) S_n est engendré par $\begin{pmatrix} 1 & 2 \end{pmatrix}$ et $\begin{pmatrix} 1 & \dots & n \end{pmatrix}$.

p. 44

Définition 23. — Soit $\sigma \in S_n$. On appelle **signature** de σ, notée $\epsilon(\sigma)$ l'entier $\epsilon(\sigma) = \prod_{i \neq j} \frac{\sigma(i) - \sigma(j)}{i - j}$.

— $\sigma \mapsto \epsilon(\sigma)$ est un morphisme de S_n dans $\{\pm 1\}$, on note A_n son noyau.

p. 48

Lemme 24. Les 3-cycles sont conjugués dans A_n pour $n \geq 5$.

[PER] p. 15

Lemme 25. Le produit de deux transpositions est un produit de 3-cycles.

[ROM21] p. 49

Proposition 26. A_n est engendré par les 3-cycles pour $n \geq 3$.

[DEV] **Théorème 27.** A_n est simple pour $n \geq 5$. [PER] p. 28

Corollaire 28. Le groupe dérivé de A_n est A_n pour $n \geq 5$, et le groupe dérivé de S_n est A_n pour $n \geq 2$.

2. Groupe diédral

Définition 29. Pour un entier $n \geq 1$, le **groupe diédral** D_n est le sous-groupe, de $\mathrm{GL}_2(\mathbb{R})$ engendré par la symétrie axiale s et la rotation d'angle $\theta = \frac{2\pi}{n}$ définies respectivement par les matrices [ULM21] p. 8

$$S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ et } R = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

Exemple 30. $D_1 = \{\mathrm{id}, s\}$.

Proposition 31. (i) D_n est un groupe d'ordre $2n$.
(ii) $r^n = s^2 = \mathrm{id}$ et $sr = r^{-1}s$.

Proposition 32. Un groupe non cyclique d'ordre 4 est isomorphe à D_2. p. 28

Exemple 33. S_2 est isomorphe à D_2. p. 65

Proposition 34. Un groupe fini d'ordre $2p$ avec p premier est soit cyclique, soit isomorphe à D_p. p. 28

Exemple 35. S_3 est isomorphe à D_3.

Proposition 36. Les sous-groupes de D_n sont soit cyclique, soit isomorphes à un D_m où $m \mid n$. p. 47

III - Applications en algèbre linéaire

1. Groupe linéaire

[PER] p. 97

Proposition 37. Soit $u \in \mathrm{GL}(E) \setminus \{\mathrm{id}_E\}$. Soit H un hyperplan de E tel que $u_{|H} = \mathrm{id}_H$. Les assertions suivantes sont équivalentes :

(i) $\det(u) = 1$.

(ii) u n'est pas diagonalisable.

(iii) $\mathrm{Im}(u - \mathrm{id}_E) \subseteq H$.

(iv) Le morphisme induit $\overline{u} : E/H \to E/H$ est l'identité de E/H.

(v) En notant $H = \mathrm{Ker}(f)$ (où f désigne une forme linéaire sur E), il existe $a \in H \setminus \{0\}$ tel que
$$u = \mathrm{id}_E + f \cdot a$$

(vi) Dans une base adaptée, la matrice de u s'écrit
$$\begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Définition 38. En reprenant les notations précédentes, on dit que u est une **transvection** d'hyperplan H et de droite $\mathrm{Vect}(a)$.

Proposition 39. Soient $u \in \mathrm{GL}(E)$ et τ une transvection d'hyperplan H et de droite D. Alors, $u\tau u^{-1}$ est une transvection d'hyperplan $u(H)$ et de droite $u(D)$.

Théorème 40. Si $n \geq 2$, les transvections engendrent $\mathrm{SL}(E)$.

Proposition 41. Soit $u \in \mathrm{GL}(E)$. Soit H un hyperplan de E tel que $u_{|H} = \mathrm{id}_H$. Les assertions suivantes sont équivalentes :

(i) $\det(u) = \lambda \neq 1$.

(ii) u admet une valeur propre $\lambda \neq 1$.

(iii) $\mathrm{Im}(u - \mathrm{id}_E) \not\subseteq H$.

(iv) Dans une base adaptée, la matrice de u s'écrit
$$\begin{pmatrix} I_{n-1} & 0 \\ 0 & \lambda \end{pmatrix}$$
avec $\lambda \neq 1$.

Théorème 42. Si $n \geq 2$, les transvections et les dilatations engendrent $\mathrm{GL}(E)$.

Notation 43. Soit $a \in \mathbb{F}_p$. On note $\left(\frac{a}{p}\right)$ le symbole de Legendre de a modulo p.

[I-P] p. 203

Lemme 44. Soient $p \geq 3$ un nombre premier et V un espace vectoriel sur $\mathbb{F}_p$ de dimension finie. Les dilatations engendrent $\mathrm{GL}(V)$.

[DEV]

Application 45 (Théorème de Frobenius-Zolotarev)**.** Soient $p \geq 3$ un nombre premier et V un espace vectoriel sur $\mathbb{F}_p$ de dimension finie.

$$\forall u \in \mathrm{GL}(V), \epsilon(u) = \left(\frac{\det(u)}{p}\right)$$

où u est vu comme une permutation des éléments de V.

2. Groupe orthogonal

Soit E un espace vectoriel réel de dimension n. Soit φ une forme bilinéaire, symétrique, non dégénérée sur E. On note q la forme quadratique associée.

[PER] p. 123

Définition 46. — On appelle **isométries** de E (relativement à q), les endomorphismes $u \in \mathrm{GL}(E)$ qui vérifient :

$$\forall x, y \in E,\ q(x,y) = q(u(x), u(y))$$

- L'ensemble des isométries de E forme un groupe, appelé **groupe orthogonal** de E, et noté $\mathcal{O}_q(E)$.
- Le sous-groupe des isométries de E de déterminant 1 est appelé **groupe spécial orthogonal** de E, et est noté $\mathrm{SO}_q(E)$.

Définition 47. Soit $u \in \mathrm{SO}_q(E)$ tel que $u^2 = \mathrm{id}_E$.

- On dit que u est une **réflexion** si $\dim(\mathrm{Ker}(u + \mathrm{id}_E)) = 1$ (ie. u est une symétrie par rapport à un hyperplan).
- On dit que u est un **retournement** si $\dim(\mathrm{Ker}(u + \mathrm{id}_E)) = 2$ (ie. u est une symétrie par rapport à un plan).

On suppose désormais de plus que φ est définie positive (ie. φ est un produit scalaire).

Théorème 48. On suppose $n \geq 3$. Alors :

(i) $\mathcal{O}_q(E)$ est engendré par les réflexions.

(ii) $\mathrm{SO}_q(E)$ est engendré par les retournements.

Application 49. On suppose $n \geq 3$. Alors :

(i) $D(\mathcal{O}_q(E)) = \mathrm{SO}_q(E)$.

(ii) $D(\mathrm{SO}_q(E)) = \mathrm{SO}_q(E)$.

120 Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.

Soit $n \geq 2$ un entier.

I - L'anneau $\mathbb{Z}/n\mathbb{Z}$

1. Construction

Théorème 1 (Division euclidienne dans $\mathbb{Z}$)**.** [GOU21] p. 9

$$\forall (a,b) \in \mathbb{Z}^2, \exists ! (q,r) \in \mathbb{Z}^2 \text{ tel que } a = bq + r \text{ et } r \in [\![0, |b|]\!]$$

Définition 2. Soient $a, b \in \mathbb{Z}$. On dit que a est **congru** à b modulo n si $n \mid b - a$. On note cela $a \equiv b \mod n$. [ROM21] p. 279

Proposition 3. Soient $a, b, c, d \in \mathbb{Z}$ tels que $a \equiv b \mod n$ et $c \equiv d \mod n$. Alors :

(i) $a + c \equiv b + d \mod n$.

(ii) $ac \equiv bd \mod n$

Lemme 4. Tout idéal de $\mathbb{Z}$ est principal, de la forme $(n) = n\mathbb{Z}$.

Définition 5. Le quotient de l'anneau $\mathbb{Z}$ par son idéal $n\mathbb{Z}$ est l'anneau noté $\mathbb{Z}/n\mathbb{Z}$. On note $\overline{a} = \{a + qn \mid q \in \mathbb{Z}\}$ l'image d'un élément $a \in \mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$.

Remarque 6. Soient $a, b \in \mathbb{Z}$.

$$\overline{a} = \overline{b} \iff a \equiv b \mod n$$

Proposition 7. (i) $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \dots, \overline{n-1}\}$.

(ii) La compatibilité de $\equiv$ avec les lois $+$ et $\times$ sur $\mathbb{Z}$ conjuguée à la remarque précédente transporte la structure d'anneau à $\mathbb{Z}/n\mathbb{Z}$ en posant, pour tout $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$:

— $\overline{a} + \overline{b} = \overline{a+b}$.

— $\overline{a}\,\overline{b} = \overline{ab}$.

2. Le groupe multiplicatif

a. Générateurs

Théorème 8. Soit $a \in \mathbb{Z}$. Les assertions suivantes sont équivalentes : p. 283

(i) $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

(ii) $\text{pgcd}(a,n) = 1$.

(iii) a est un générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$.

Exemple 9. $(\mathbb{Z}/4\mathbb{Z})^\times = \{\pm\overline{1}\}$. p. 301

Proposition 10. (i) $\mathbb{Z}$ est monogène, l'ensemble de ses générateurs est $\mathbb{Z}^\times = \{\pm 1\}$. p. 14

(ii) $\mathbb{Z}/n\mathbb{Z}$, l'ensemble de ses générateurs est $(\mathbb{Z}/n\mathbb{Z})^\times$.

Corollaire 11. Soit G un groupe.

(i) Si G est monogène infini, alors $G \cong \mathbb{Z}$.

(ii) Si G est cyclique d'ordre n, alors $G \cong \mathbb{Z}/n\mathbb{Z}$.

Exemple 12. Le groupe des racines n-ièmes de l'unité, μ_n, est isomorphe $\mathbb{Z}/n\mathbb{Z}$ via

$$\overline{k} \mapsto e^{\frac{2ik\pi}{n}}$$

b. Sous-groupes additifs et idéaux

Théorème 13. Les sous-groupes additifs de $\mathbb{Z}/n\mathbb{Z}$ sont cycliques d'ordre divisant n. Réciproquement, pour tout diviseur d de n, il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$, c'est le groupe cyclique engendré par $\overline{\frac{n}{d}}$. p. 281

Théorème 14. (i) Les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont ses sous-groupes additifs. p. 255

(ii) Les idéaux premiers de $\mathbb{Z}/n\mathbb{Z}$ sont les idéaux maximaux de $\mathbb{Z}/n\mathbb{Z}$: ce sont les idéaux engendrés par $(\overline{p})$ où p est un diviseur premier de n.

3. Indicatrice d'Euler

Définition 15. L'indicatrice d'Euler φ est la fonction qui à un entier k, associe le nombre d'entiers compris entre 1 et n qui sont premiers avec k. p. 283

Remarque 16. D'après le Théorème 8, $\varphi(n)$ est le nombre de générateurs de $\mathbb{Z}/n\mathbb{Z}$ et est également le cardinal de $(\mathbb{Z}/n\mathbb{Z})^\times$.

Exemple 17.
— Si n est premier, $\varphi(n) = n-1$.
— $\varphi(4) = 2$ d'après l'Théorème 9.

Proposition 18. Pour tout p premier et pour tout entier n, [GOZ] p. 4

$$\varphi(p^n) = p^n - p^{n-1}$$

[DEV]

Théorème 19 (Chinois)**.** Soient n et m deux entiers premiers entre eux. Alors,

$$\mathbb{Z}/nm\mathbb{Z} \equiv \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

Corollaire 20. $\forall m, n \in \mathbb{Z}$ premiers entre eux,

$$\varphi(mn) = \varphi(m)\varphi(n)$$

Proposition 21 (Théorème Euler)**.** Pour tout entier relatif a premier avec n, $a^{\varphi(n)} \equiv 1 \mod n$.

Proposition 22 (Petit théorème de Fermat)**.** Pour tout entier relatif a, pour tout p premier, $a^{p-1} \equiv 1 \mod p$.

Proposition 23. Pour tout entier naturel n,

$$\sum_{d|n} \varphi(d) = n$$

II - Cas où n est premier

1. Structure de corps

Proposition 24. Les assertions suivantes sont équivalentes.

(i) n est un nombre premier.

(ii) $\mathbb{Z}/n\mathbb{Z}$ est intègre.

(iii) $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Théorème 25. Tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique. p. 83

Corollaire 26. Si p désigne un nombre premier, $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.

Remarque 27. On a un résultat encore plus fort : $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si $n = 2, 4, p^\alpha$ ou $2p^\alpha$ avec p premier impair et $\alpha \geq 1$. **[ROM21]** p. 294

2. Carrés

Remarque 28. Tout élément de $\mathbb{Z}/2\mathbb{Z}$ est un carré. p. 427

Soit p un nombre premier impair.

Théorème 29. (i) Il y a $\frac{p-1}{2}$ carrés et autant de non carrés dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

(ii) Les carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$ sont les racines de $X^{\frac{p-1}{2}} - 1$ et les non carrés celles de $X^{\frac{p-1}{2}} + 1$.

Corollaire 30. -1 est un carré dans $(\mathbb{Z}/p\mathbb{Z})^\times$ si et seulement si $p \equiv 1 \mod 4$.

III - Applications

1. Systèmes de congruences

Proposition 31. Soit a un entier non nul. L'équation p. 289

$$ax \equiv 1 \mod n$$

admet des solutions si et seulement si $\text{pgcd}(a, n) = 1$.

Corollaire 32. Soient a un entier non nul et b un entier relatif. L'équation

$$ax \equiv b \mod n$$

a des solutions si et seulement si $d = \text{pgcd}(a,n) \mid b$. Dans ce cas, l'ensemble des solutions est

$$\left\{\frac{b}{d}x_0 + k\frac{n}{d} \mid k \in \mathbb{Z}\right\}$$

où x_0 est une solution de l'équation $\frac{a}{n}x \equiv 1 \mod n$.

Pour résoudre des systèmes de congruences, on va préciser le Théorème 19.

p. 285

Théorème 33 (Chinois)**.** Soient $n_1, \dots, n_r \geq 2$ des entiers. On note $n = \prod_{i=1}^r n_i$ et $\pi_k = \pi_{n_k\mathbb{Z}}$ la surjection canonique de $\mathbb{Z}$ sur $\mathbb{Z}/k\mathbb{Z}$ pour tout $k \in [\![1,r]\!]$.

Les entiers $n_1, \dots, n_r$ sont premiers entre eux si et seulement si les anneaux $\mathbb{Z}/n\mathbb{Z}$ et $\prod_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}$ sont isomorphes. Dans ce cas, l'isomorphisme est explicité par l'application

$$\psi : \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \to & \prod_{i=1}^r \mathbb{Z}/n_i\mathbb{Z} \\ \pi_n(k) & \mapsto & (\pi_i(k))_{i\in[\![1,r]\!]} \end{array}$$

p. 291

Exemple 34.

$$\begin{cases} k \equiv 2 \mod 4 \\ k \equiv 3 \mod 5 \\ k \equiv 1 \mod 9 \end{cases}$$

admet pour ensemble de solutions $\{838 + 180q \mid q \in \mathbb{Z}\}$.

2. Étude d'équations diophantiennes

a. Entiers sommes de deux carrés

Notation 35. On note

$$N : \begin{array}{ccc} \mathbb{Z}[i] & \to & \mathbb{N} \\ a+ib & \mapsto & a^2+b^2 \end{array}$$

et Σ l'ensemble des entiers qui sont somme de deux carrés.

[I-P] p. 137

Remarque 36. $n \in \Sigma \iff \exists z \in \mathbb{Z}[i]$ tel que $N(z) = n$.

Théorème 37 (Deux carrés de Fermat)**.** Soit $n \in \mathbb{N}^*$. Alors $n \in \Sigma$ si et seulement si $v_p(n)$ est pair pour tout p premier tel que $p \equiv 3 \mod 4$ (où $v_p(n)$ désigne la valuation p-adique de

n).

b. Premiers congrus à 1 modulo n

Notation 38. On note Φ_n le n-ième polynôme cyclotomique. [GOU21] p. 99

Lemme 39. Soient $a \in \mathbb{N}$ et p premier tels que $p \mid \Phi_n(a)$ mais $p \nmid \Phi_d(a)$ pour tout diviseur strict d de n. Alors $p \equiv 1 \mod n$.

[DEV]

Théorème 40 (Dirichlet faible)**.** Pour tout entier n, il existe une infinité de nombres premiers congrus à 1 modulo n.

3. Irréductibilité de polynômes

Lemme 41 (Gauss)**.** [GOZ] p. 10

(i) Le produit de deux polynômes primitifs est primitif (ie. dont le PGCD des coefficients est égal à 1).

(ii) $\forall P, Q \in \mathbb{Z}[X] \setminus \{0\}$, $\gamma(PQ) = \gamma(P)\gamma(Q)$ (où $\gamma(P)$ est le contenu du polynôme P).

Théorème 42 (Critère d'Eisenstein)**.** Soit $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ de degré $n \geq 1$. On suppose qu'il existe p premier tel que :

(i) $p \mid a_i$, $\forall i \in [\![0, n-1]\!]$.

(ii) $p \nmid a_n$.

(iii) $p^2 \nmid a_0$.

Alors P est irréductible dans $\mathbb{Q}[X]$.

Application 43. Soit $n \in \mathbb{N}^*$. Il existe des polynômes irréductibles de degré n sur $\mathbb{Z}$. [PER] p. 67

Théorème 44 (Critère d'irréductibilité modulo p)**.** Soit $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ de degré $n \geq 1$. Soit p un premier. On suppose $p \nmid a_n$. [GOZ] p. 12

Si $\overline{P}$ est irréductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$, alors P est irréductible dans $\mathbb{Q}[X]$.

Exemple 45. Le polynôme $X^3 - 127X^2 + 3608X + 19$ est irréductible dans $\mathbb{Z}[X]$.

4. Chiffrement RSA

[ULM18] p. 62

Définition 46. Afin de chiffrer un **message** (tout entier découpé en séquence d'entiers de taille bornée) en utilisant RSA, on doit a besoin de deux clés :

— Une **clé privée**, qui est un couple de nombres premiers (p,q).

— La **clé publique** correspondante, qui est le couple (n,e) où $n = pq$ et e est l'inverse de d modulo $\phi(n)$ où d désigne un nombre premier à $\phi(n)$.

Nous conserverons ces notations pour la suite.

Théorème 47 (Chiffrement RSA)**.** Soit $m = (m_i)_{i\in[\![1,r]\!]}$ un message où pour tout i, $m_i < n$.

(i) Possédant la clé publique, on peut *chiffrer* ce message en un message m' :

$$m' = (m_i^e)_{i\in[\![1,r]\!]}$$

(ii) Possédant la clé privée, on peut *déchiffrer* le message m' pour reconstituer m :

$$\forall i \in [\![1,r]\!],\ (m_i^e)^d \equiv d \mod n$$

Remarque 48. — L'intérêt vient pour des premiers p et q très grands : il devient alors très compliqué de factoriser n et d'obtenir la clé privée.

— Les inverses peuvent se calculer à l'aide de l'algorithme de Bézout.

121 Nombres premiers. Applications.

I - Généralités

1. Nombres premiers et premiers entre eux

Définition 1. Soient $a, b \in \mathbb{Z}$. On dit que a **divise** b (ou que b est un **multiple** de a), et on note $a \mid b$ s'il existe $n \in \mathbb{Z}$ tel que $b = an$. Dans le cas contraire, on note $a \nmid b$. [GOU21] p. 9

Théorème 2 (Division euclidienne dans $\mathbb{Z}$)**.**

$$\forall (a,b) \in \mathbb{Z}^2,\ \exists !(q,r) \in \mathbb{Z}^2 \text{ tel que } a = bq + r \text{ et } r \in [\![0, |b|]\!]$$

Définition 3. Soient $a_1, \dots, a_n \in \mathbb{Z}$. Par principalité de $\mathbb{Z}$, il existe un unique $d \in \mathbb{N}$ tel que

$$a_1\mathbb{Z} + \cdots + a_n\mathbb{Z} = d\mathbb{Z}$$

Ainsi défini, d s'appelle le **pgcd** de $a_1, \dots, a_n$ et on note $d = \text{pgcd}(a_1, \dots, a_n)$.

Remarque 4. Dans la définition précédente, d est le plus entier naturel divisant tous les a_i.

Définition 5. Soient $a_1, \dots, a_n \in \mathbb{Z}$. Lorsque $\text{pgcd}(a_1, \dots, a_n) = 1$, on dit que $a_1, \dots, a_n$ sont **premiers entre eux** *dans leur ensemble*. Lorsque $\text{pgcd}(a_i, a_j) = 1$ dès que $i \neq j$, on dit que $a_1, \dots, a_n$ sont **premiers entre eux** *deux à deux*.

Théorème 6 (Bézout)**.** Soient $a_1, \dots, a_n \in \mathbb{Z}$.

$$\text{pgcd}(a_1, \dots, a_n) = 1 \iff \exists u_1, \dots, u_n \in \mathbb{Z} \text{ tels que } \sum_{i=1}^{n} u_i a_i = 1$$

Théorème 7 (Gauss)**.** Soient $a, b, c \in \mathbb{Z}$.

$$a \mid bc \text{ et } \text{pgcd}(a,b) = 1 \implies a \mid c$$

Définition 8. On dit qu'un entier naturel p est **premier** s'il est supérieur ou égal à 2 et si ses seuls diviseurs positifs sont 1 et p. [ROM21] p. 304

Exemple 9. Les nombres de Fermat $F_n = 2^{2^n} + 1$ sont premiers pour $n \in [\![0,4]\!]$, mais pas pour $n \in [\![5,32]\!]$.

Théorème 10 (Euclide)**.** L'ensemble $\mathscr{P}$ des nombres premiers est infini.

Théorème 11 (Fondamental de l'arithmétique)**.** Tout entier naturel $n \geq 2$ se décompose de manière unique sous la forme :

$$n = \prod_{k=1}^{r} p_k^{\alpha_k}$$

où les p_k sont des nombres premiers distincts et où les α_k sont des entiers naturels non nuls.

Proposition 12. (i) Si $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ et $m = \prod_{i=1}^{k} p_i^{\beta_i}$, alors $\text{pgcd}(n,m) = \prod_{i=1}^{k} p_i^{\inf(\alpha_i,\beta_i)}$.

(ii) Soient $p \in \mathscr{P}$ et $k \in [\![1, p-1]\!]$. Alors $p \mid \binom{p}{k}$.

[GOU21] p. 11

Théorème 13 (Fermat)**.** Soient $p \in \mathscr{P}$ et $a \in \mathbb{Z}$. Alors :

(i) $a^p \equiv a \mod p$.

(ii) $p \nmid a \implies a^{p-1} \equiv 1 \mod p$.

2. Fonctions arithmétiques

Définition 14. On définit :

— L'**indicatrice d'Euler** φ est la fonction qui à un entier k, associe le nombre d'entiers compris entre 1 et n qui sont premiers avec k.

— La **fonction de Möbius**, notée μ, par

$$\mu : \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z} \\ n & \mapsto & \begin{cases} 1 & \text{si } n = 1 \\ (-1)^k & \text{si } n = p_1 \dots p_k \text{ avec } p_1, \dots, p_k \text{ premiers distincts} \\ 0 & \text{sinon} \end{cases} \end{array}$$

[GOZ] p. 3

Proposition 15. (i) $\forall m, n \in \mathbb{Z}$ premiers entre eux, $\varphi(mn) = \varphi(m)\varphi(n)$.

(ii) Pour tout entier relatif a premier avec n, $a^{\varphi(n)} \equiv 1 \mod n$.

(iii) Pour tout entier naturel n, $\sum_{d \mid n} \varphi(d) = n$.

p. 89

Théorème 16 (Formule d'inversion de Möbius)**.** Soient f et g des fonctions de $\mathbb{N}^*$ dans $\mathbb{C}$ telles que $\forall n \in \mathbb{N}^*, f(n) = \sum_{d|n} g(d)$. Alors,

$$\forall n \in \mathbb{N}^*, g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$$

Corollaire 17.

$$\forall n \in \mathbb{N}^*, \varphi(n) = \sum_{d|n} d\mu\left(\frac{n}{d}\right)$$

3. Répartition des nombres premiers

Définition 18. L'ensemble des générateurs de μ_n, noté μ_n^*, est formé des **racines primitives n-ièmes de l'unité**. p. 67

Proposition 19. (i) $\mu_n^* = \{e^{\frac{2ik\pi}{n}} \mid k \in [\![0, n-1]\!], \operatorname{pgcd}(k, m) = 1\}$.
(ii) $|\mu_n^*| = \varphi(n)$, où φ désigne l'indicatrice d'Euler.

Définition 20. On appelle **n-ième polynôme cyclotomique** le polynôme

$$\Phi_n = \prod_{\xi \in \mu_n^*} (X - \xi)$$

Théorème 21. (i) $X^n - 1 = \prod_{d|n} \Phi_d$.
(ii) $\Phi_n \in \mathbb{Z}[X]$.
(iii) Φ_n est irréductible sur $\mathbb{Q}$.

Corollaire 22. Le polynôme minimal sur $\mathbb{Q}$ de tout élément ξ de μ_n^* est Φ_n. En particulier,

$$[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(m)$$

[DEV]

Théorème 23 (Dirichlet faible)**.** Pour tout entier n, il existe une infinité de nombres premiers congrus à 1 modulo n. **[GOU21]** p. 99

Remarque 24. La version forte de ce théorème est que, pour tout entiers naturels a, b non nuls, il existe une infinité de nombres premiers de la forme $ak + b$, $k \in \mathbb{N}$.

p. 16

Théorème 25 (des nombres premiers)**.** Si $x > 0$, on note $\pi(x)$ le nombre de nombres premiers inférieurs à x. Alors,

$$\pi(x) \sim \frac{x}{\ln(x)}$$

II - Théorie des corps

1. Corps finis

Proposition 26. Les conditions suivantes sont équivalentes : [GOZ] p. 3

(i) n est un nombre premier.

(ii) $\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre.

(iii) $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Notation 27. On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Définition 28. Soit A un anneau. L'application p. 7

$$f_A : \begin{array}{ccc} \mathbb{Z} & \to & A \\ n & \mapsto & \underbrace{1+\cdots+1}_{n \text{ fois}} \end{array}$$

On note $\text{car}(A)$ l'unique $n \in \mathbb{N}$ tel que $\text{Ker}(f_A) = n\mathbb{Z}$: c'est la **caractéristique** de A.

Proposition 29. (i) Soit A un anneau intègre. Alors, $\text{car}(A) = 0$ ou p avec p premier.

(ii) Soit A un anneau fini. Alors, $\text{car}(A) \neq 0$ et $\text{car}(A) \mid |A|$.

(iii) Un anneau et un quelconque de ses sous-anneaux ont la même caractéristique.

Remarque 30. — Le Point (i) est en particulier vrai pour un corps.

— Si $\text{car}(A) = 0$, A est infini.

Proposition 31. Soit $\mathbb{K}$ un corps fini. p. 81

(i) $\text{car}(\mathbb{K})$ est un nombre premier p.

(ii) Le sous-corps premier de $\mathbb{K}$ est isomorphe à $\mathbb{F}_p$.

(iii) $|\mathbb{K}| = p^n$ pour $n \geq 2$.

Proposition 32. Soit $\mathbb{K}$ un corps de caractéristique p. L'application

$$\text{Frob} : \begin{array}{ccc} \mathbb{K} & \to & \mathbb{K} \\ x & \mapsto & x^p \end{array}$$

est un morphisme de corps.

(i) Si $\mathbb{K}$ est fini, c'est un automorphisme.

(ii) Si $\mathbb{K} = \mathbb{F}_p$, c'est l'identité.

Théorème 33. Soient $p \in \mathscr{P}$ et $n \in \mathbb{N}^*$. On pose $q = p^n$. Alors :

(i) Il existe un corps $\mathbb{K}$ à q éléments : c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.

(ii) $\mathbb{K}$ est unique à isomorphisme près : on le note $\mathbb{F}_q$.

Corollaire 34 (Théorème de Wilson)**.** Soit $n \geq 2$ un entier. Alors,

$$n \text{ est premier} \iff (n-1)! + 1 \equiv 0 \mod n$$

Théorème 35. $\mathbb{F}_q^*$ est cyclique, isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$.

[PER] p. 74

Remarque 36. En fait, tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique.

Théorème 37 (Wedderburn)**.** Tout corps fini est commutatif.

[GOU21] p. 100

2. Carrés dans les corps finis

Soit $q = p^n$ avec p premier et $n \geq 2$.

[GOZ] p. 93

Proposition 38. On note $\mathbb{F}_q^2 = \{x^2 \mid x \in \mathbb{F}_q\}$ et $\mathbb{F}_q^{*2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$. Alors $\mathbb{F}_q^{*2}$ est un sous-groupe de $\mathbb{F}_q^*$.

Proposition 39. (i) Si $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$, donc $\mathbb{F}_q^{*2} = \mathbb{F}_q^*$.

(ii) Si $p > 2$, alors :

- $\mathbb{F}_q^{*2}$ est le noyau de l'endomorphisme de $\mathbb{F}_q^*$ défini par $x \mapsto x^{\frac{q-1}{2}}$.
- $\mathbb{F}_q^{*2}$ est un sous-groupe d'indice 2 de $\mathbb{F}_q^*$.
- $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$ et $|\mathbb{F}_q^2| = \frac{q+1}{2}$.
- $(-1) \in \mathbb{F}_q^{*2} \iff q \equiv 1 \mod 4$.

Notation 40. Soit $a \in \mathbb{F}_p$. On note $\left(\frac{a}{p}\right)$ le symbole de Legendre de a modulo p. On a ainsi $\left(\frac{a}{p}\right) = \pm 1$ avec $\left(\frac{a}{p}\right) = 1$ si et seulement si $a \in \mathbb{F}_p^2$.

[I-P] p. 203

Application 41 (Frobenius-Zolotarev)**.** Soient $p \geq 3$ un nombre premier et V un espace vectoriel sur $\mathbb{F}_p$ de dimension finie.

$$\forall u \in \mathrm{GL}(V), \epsilon(u) = \left(\frac{\det(u)}{p}\right)$$

où u est vu comme une permutation des éléments de V.

3. Réduction modulo p

Le résultat suivant justifie que l'on s'intéresse aux polynômes irréductibles en théorie des corps.

Théorème 42. Soit $P \in \mathbb{K}[X]$ un polynôme irréductible sur un corps $\mathbb{K}$.

- Il existe un corps de rupture de P.
- Si $\mathbb{L} = \mathbb{K}[\alpha]$ et $\mathbb{L}' = \mathbb{K}[\beta]$ sont deux corps de rupture de P, alors il existe un unique $\mathbb{K}$-isomorphisme $\varphi : \mathbb{L} \to \mathbb{L}'$ tel que $\varphi(\alpha) = \beta$.
- $\mathbb{K}[X]/(P)$ est un corps de rupture de P.

[GOZ] p. 57

Lemme 43 (Gauss)**.** (i) Le produit de deux polynômes primitifs est primitif (ie. dont le PGCD des coefficients est égal à 1).

(ii) $\forall P, Q \in \mathbb{Z}[X] \setminus \{0\}, \gamma(PQ) = \gamma(P)\gamma(Q)$ (où $\gamma(P)$ est le contenu du polynôme P).

p. 10

[DEV]

Théorème 44 (Critère d'Eisenstein)**.** Soit $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ de degré $n \geq 1$. On suppose qu'il existe p premier tel que :

(i) $p \mid a_i, \forall i \in [\![0, n-1]\!]$.

(ii) $p \nmid a_n$.

(iii) $p^2 \nmid a_0$.

Alors P est irréductible dans $\mathbb{Q}[X]$.

Application 45. Soit $n \in \mathbb{N}^*$. Il existe des polynômes irréductibles de degré n sur $\mathbb{Z}$.

[PER] p. 67

[GOZ] p. 12

Théorème 46 (Critère d'irréductibilité modulo p)**.** Soit $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ de degré $n \geq 1$. Soit p un premier. On suppose $p \nmid a_n$.

Si $\overline{P}$ est irréductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$, alors P est irréductible dans $\mathbb{Q}[X]$.

Exemple 47. Le polynôme $X^3 - 127X^2 + 3608X + 19$ est irréductible dans $\mathbb{Z}[X]$.

III - Autres applications en algèbre

1. Entiers sommes de deux carrés

Notation 48. On note

$$N : \begin{array}{ccc} \mathbb{Z}[i] & \to & \mathbb{N} \\ a+ib & \mapsto & a^2+b^2 \end{array}$$

et Σ l'ensemble des entiers qui sont somme de deux carrés.

[I-P] p. 137

Remarque 49. $n \in \Sigma \iff \exists z \in \mathbb{Z}[i]$ tel que $N(z) = n$.

Théorème 50 (Deux carrés de Fermat)**.** Soit $n \in \mathbb{N}^*$. Alors $n \in \Sigma$ si et seulement si $v_p(n)$ est pair pour tout p premier tel que $p \equiv 3 \mod 4$ (où $v_p(n)$ désigne la valuation p-adique de n).

2. En théorie des groupes

Soit G un groupe fini opérant sur un ensemble fini X.

[ROM21] p. 22

Définition 51. On dit que G est un **p-groupe** s'il est d'ordre une puissance d'un nombre premier p.

Théorème 52 (Formule des classes)**.** Soit Ω un système de représentants des orbites de l'action de G sur X. Alors,

$$|X| = \sum_{\omega \in \Omega} |G \cdot \omega| = \sum_{\omega \in \Omega} (G : \mathrm{Stab}_G(\omega)) = \sum_{\omega \in \Omega} \frac{|G|}{|\mathrm{Stab}_G(\omega)|}$$

Corollaire 53. Soit p un nombre premier. Si G est un p-groupe opérant sur X, alors,

$$|X^G| \equiv |X| \mod p$$

où X^G désigne l'ensemble des points fixes de X sous l'action de G.

Corollaire 54. On note $G \cdot h_1, \dots, G \cdot h_r$ les classes de conjugaison de G. Alors,

$$\begin{aligned} |G| &= |Z(G)| + \sum_{\substack{i=1 \\ |G \cdot h_i| = 2}}^{r} |G \cdot h_i| \\ &= |Z(G)| + \sum_{\substack{i=1 \\ |G \cdot h_i| = 2}}^{r} \frac{|G|}{|\mathrm{Stab}_G(h_i)|} \end{aligned}$$

Corollaire 55. Soit p un nombre premier. Le centre d'un p-groupe non trivial est non trivial.

Corollaire 56. Soit p un nombre premier. Un groupe d'ordre p^2 est toujours abélien.

Application 57 (Théorème de Cauchy)**.** On suppose G non trivial et fini. Soit p un premier divisant l'ordre de G. Alors il existe un élément d'ordre p dans G.

Application 58 (Premier théorème de Sylow)**.** On suppose G fini d'ordre np^α avec $n, \alpha \in \mathbb{N}$ et p premier tel que $p \nmid n$. Alors, il existe un sous-groupe de G d'ordre p^α.

[GOU21] p. 44

3. RSA

Définition 59. Afin de chiffrer un **message** (tout entier découpé en séquence d'entiers de taille bornée) en utilisant RSA, on doit a besoin de deux clés :

- Une **clé privée**, qui est un couple de nombres premiers (p, q).
- La **clé publique** correspondante, qui est le couple (n, e) où $n = pq$ et e est l'inverse de d modulo $\phi(n)$ où d désigne un nombre premier à $\phi(n)$.

[ULM18] p. 62

Nous conserverons ces notations pour la suite.

Théorème 60 (Chiffrement RSA)**.** Soit $m = (m_i)_{i \in [\![1,r]\!]}$ un message où pour tout i, $m_i < n$.

(i) Possédant la clé publique, on peut *chiffrer* ce message en un message m' :

$$m' = (m_i^e)_{i \in [\![1,r]\!]}$$

(ii) Possédant la clé privée, on peut *déchiffrer* le message m' pour reconstituer m :

$$\forall i \in [\![1, r]\!], (m_i^e)^d \equiv d \mod n$$

Remarque 61. — L'intérêt vient pour des premiers p et q très grands : il devient alors très compliqué de factoriser n et d'obtenir la clé privée.

— Les inverses peuvent se calculer à l'aide de l'algorithme de Bézout.

122 Anneaux principaux. Exemples et applications.

Soit A un anneau unitaire.

I - Structures algébriques

1. Idéaux

Définition 1. Un sous ensemble $I \subseteq A$ est un **idéal** de A si : [ULM18] p. 5

(i) $(I,+)$ est un sous groupe de $(A,+)$.

(ii) Les produits ai et ia appartiennent à I pour tout a dans A et $i \in I$ (propriété d'absorption). p. 11

Si I est un idéal de A. Alors,

$$A/I = \{\overline{a} = a + I \mid a \in A\}$$

est un anneau, muni des lois $\overline{a} + \overline{b} = \overline{a+b}$ et $\overline{a}\overline{b} = \overline{ab}$, et est appelé **anneau quotient** de A par I.

Remarque 2. — Un anneau non nul possède toujours les deux idéaux 0 et lui-même. p. 5

— Un idéal contenant 1 est égal à l'anneau entier (à cause de la propriété d'absorption). Par conséquent, un idéal différent de l'anneau ambiant n'est jamais un sous-anneau de celui-ci.

Exemple 3. Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ pour $n \in \mathbb{Z}$.

Proposition 4. Soient $\varphi : A \to B$ un morphisme d'anneaux et $I \subseteq A$, $J \subseteq B$ deux idéaux.

(i) L'ensemble $\varphi^{-1}(J)$ est un idéal de A. En particulier, $\mathrm{Ker}(\varphi)$ est un idéal de A.

(ii) Si φ est surjectif, alors $\varphi(I)$ est un idéal de B.

Définition 5. Soit $S \subseteq A$.

— $\bigcap\{I\text{I} \text{ idéal de } \text{A} \mid S \subseteq I\}$ est un idéal de A noté (S) est appelé **idéal engendré** par S.

— On a $(S) = \{\sum_{i=1}^{n} a_i s_i b_i \mid a_i, b_i \in A, s_i \in S, n \in \mathbb{N}\}$. Si A est commutatif, $(S) = \{\sum_{i=1}^{n} a_i s_i \mid a_i \in A, s_i \in S, n \in \mathbb{N}\}$.

Définition 6. Soit I un idéal de A. p. 31

— I est dit **maximal** si $I \subsetneq A$ et si A et I sont les seuls idéaux de A qui le contiennent.

— On suppose A commutatif. I est dit **premier** si $I \subsetneq A$ et

$$\forall a, b \in A,\ ab \in I \implies a \in I \text{ ou } b \in I$$

Proposition 7. On suppose A commutatif. Soit I un idéal de A.

(i) I est maximal si et seulement si A/I est un corps.

(ii) I est premier si et seulement si A/I est un anneau intègre.

Corollaire 8. Dans un anneau commutatif, un idéal maximal est premier.

Contre-exemple 9. $\{0\}$ est un idéal premier de $\mathbb{Z}$ mais non maximal.

2. Anneaux principaux

Définition 10. — Un idéal est dit **principal** s'il est engendré par un seul élément. p. 39

— Un anneau est dit **principal** s'il est intègre (donc commutatif) et si tous ses idéaux sont principaux.

Exemple 11. Comme dit dans l'Théorème 3, $\mathbb{Z}$ est un anneau principal.

Définition 12. On suppose A commutatif. Un élément a de A est dit **irréductible** si p. 45

$$a \notin A^\times, a \neq 0 \text{ et } a = bc \implies b \in A^\times \text{ ou } b \in A^\times$$

où $A^\times$ désigne le groupe des inversibles de A.

Théorème 13. On suppose A principal. Soit $a \in A$.

(i) (a) est premier si et seulement si a est irréductible.

(ii) En supposant $a \neq 0$, (a) est premier si et seulement si (a) est maximal.

3. Anneaux euclidiens

Définition 14. — A est dit **euclidien** s'il est intègre et s'il existe une fonction $\nu : A^* \to \mathbb{N}$ telle que

$$\forall a, b \in A^*, \exists q, r \in A \text{ tels que } a = bq + r \text{ avec } (r = 0 \text{ ou } \nu(r) < \nu(b))$$

— L'élément q est le **quotient** et l'élément r est le **reste** de la division.

— La fonction ν est appelée **stathme euclidien** pour A.

p. 43

Exemple 15. $\mathbb{Z}$ est un anneau euclidien pour le stathme $\nu : n \mapsto |n|$.

Proposition 16. Un anneau euclidien est principal.

Contre-exemple 17. $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal mais n'est pas euclidien.

[PER] p. 53

Théorème 18. Si $\mathbb{K}$ est un corps commutatif, alors $\mathbb{K}[X]$ est un anneau euclidien de stathme le degré. De plus, le quotient et le reste sont uniques.

[ULM18] p. 47

Corollaire 19. On suppose A commutatif. Les assertions suivantes sont équivalentes :

(i) A est un corps commutatif.

(ii) $A[X]$ est un anneau euclidien.

(iii) $A[X]$ est un anneau principal.

Corollaire 20. Soient $\mathbb{K}$ un corps commutatif et $f \in \mathbb{K}[X]$. Alors $\mathbb{K}[X]/(f)$ est un corps si et seulement si P est irréductible dans $\mathbb{K}[X]$.

II - Arithmétique dans les anneaux

On suppose A commutatif dans toute cette section.

1. Divisibilité dans un anneau principal

Définition 21. Soient $a, b \in A$. p. 39

- On dit que a **divise** b (ou que b est un multiple de a), noté $a \mid b$ s'il existe $c \in A$ tel que $b = ac$.
- On dit que a et b sont **associés**, noté $a \sim b$ si $a \mid b$ et si $b \mid a$.

Remarque 22. Soient $a, b \in A$.

- $a \mid b \iff (b) \subseteq (a)$.
- $a \sim b \iff (b) = (a)$. Ainsi, $\sim$ est une relation d'équivalence sur A.

Proposition 23. Soient $a, b \in A$. Alors,

$$a \sim b \iff \exists u \in A^\times \text{ tel que } b = ua$$

Définition 24. Soient $a_1, \dots, a_n \in A^*$.

- $d \in A$ est un **plus grand commun diviseur** "PGCD" de $a_1, \dots, a_m$ si d satisfait les deux propriétés suivantes :
  (i) $d \mid a_i, \forall i \in [\![1, n]\!]$.
  (ii) Si $\exists d' \in A$ tel que $d' \mid a_i, \forall i \in [\![1, n]\!]$, alors $d' \mid d$.
- $m \in A$ est un **plus petit commun multiple** "PPCM" de $a_1, \dots, a_n$ si m satisfait les deux propriétés suivantes :
  (i) $a_i \mid m, \forall i \in [\![1, n]\!]$.
  (ii) Si $\exists m' \in A$ tel que $a_i \mid m', \forall i \in [\![1, n]\!]$, alors $m \mid m'$.

Remarque 25. Un PGCD (resp. un PPCM), lorsqu'il existe, n'est pas toujours unique. Dans un anneau intègre, deux PGCD (resp. PPCM) sont toujours associés puisqu'ils se divisent l'un l'autre. Dans un anneau intègre, on peut donc noter $d \sim \text{pgcd}(a, b)$ (resp. $m \sim \text{pgcd}(a, b)$) lorsque d est un pgcd (resp. m est un ppcm) de a et de b.

Exemple 26. Soient $\mathbb{K}$ un corps commutatif. On pose $P_n = X^n - 1 \in \mathbb{K}[X]$ pour $n \in \mathbb{N}^*$. Alors, pour $a, b \in \mathbb{N}^*$, le PGCD unitaire de P_a et P_b est égal à $P_{\text{pgcd}(a,b)}$. **[GOU21]** p. 60

[ULM18] p. 40

Proposition 27. Soient $a, b \in A^*$. Un élément $c \in A$ est un PPCM de a et b si et seulement si $(a) \cap (b) = (c)$. En particulier, a et b admettent un PPCM si et seulement si $(a) \cap (b)$ est un idéal principal.

Proposition 28. Soient $a, b \in A^*$. Soit $d \in A$. Les assertions suivantes sont équivalentes.

(i) $d \mid a$, $d \mid b$ et il existe $u, v \in A$ tels que $d = au + bv$.

(ii) $d \sim \text{pgcd}(a, b)$ et il existe $u, v \in A$ tels que $d = au + bv$.

(iii) $(d) = (a, b)$.

Théorème 29 (Décomposition de Bézout)**.** On suppose A principal. Soient $a_1, \dots, a_n \in A^*$. Alors :

(i) Il existe d un pgcd de $a_1, \dots, a_n$. d est tel que $(d) = (a_1, \dots, a_n)$. En particulier, d est de la forme $d = b_1 a_1 + \cdots + b_n a_n$ avec $\forall i \in [\![1, n]\!]$, $b_i \in A$.

(ii) Il existe m un ppcm de $a_1, \dots, a_n$. m est tel que $(m) = (a_1) \cap \cdots \cap (a_n)$.

Remarque 30. Une façon d'obtenir ces coefficients si A est euclidien est d'utiliser l'algorithme d'Euclide généralisé.

Exemple 31. Dans $\mathbb{F}_2[X]$: p. 52

$$-X(X^3 + X^2 + 1) + (1 + X^2)(X^2 + X + 1) = 1$$

Application 32. $\overline{X}^2 + 1$ est inversible dans $\mathbb{F}_2[X]/(X^3 + X^2 + 1)$ d'inverse $\overline{X}^2 + X + 1$.

Définition 33. Deux éléments a et b de A sont dits **premiers entre eux** s'ils admettent un PGCD et $\text{pgcd}(a, b) \sim 1$. p. 41

Exemple 34. 2 et X sont premiers entre eux dans $\mathbb{Z}[X]$.

Lemme 35 (Gauss)**.** On suppose A principal. Soient $a, b, c \in A$ avec a et b premiers entre eux. Alors,

$$a \mid bc \implies a \mid c$$

et

$$a \mid c \text{ et } b \mid c \implies ab \mid c$$

2. Anneaux factoriels

Définition 36. A est dit **factoriel** s'il est intègre et si, pour tout élément $a \in A^*$ non inversible, les conditions suivantes sont satisfaites : p. 63

(i) $a = q_1 q_2 \dots q_s$ avec $\forall i \in [\![1, s]\!]$, q_i irréductible (existence d'une décomposition en produit d'irréductibles).

(ii) Si $a = q_1 q_2 \dots q_s = \widetilde{q_1}\widetilde{q_2} \dots \widetilde{q_m}$ avec $\forall i \in [\![1, s]\!]$, q_i irréductible et $\forall i \in [\![1, s]\!]$, q_i irréductible, alors $s = m$ et pour toute permutation π d'indice, $q_i \widetilde{q_{\pi(i)}}$, $\forall i \in [\![1, s]\!]$ ("unicité" de la décomposition).

Proposition 37. Si A vérifie le Point (i), alors les assertions suivantes sont équivalentes : **[PER]** p. 48

(i) A vérifie le Point (ii).

(ii) A vérifie le lemme d'Euclide : si $p \in A$ est irréductible, alors $p \mid ab \implies p \mid a$ ou $p \mid b$.

(iii) Pour tout $p \in A$, p est irréductible si et seulement si (p) premier.

(iv) A vérifie le lemme de Gauss : si $p \in A$ est irréductible, alors $a \mid bc \implies a \mid c$ pour tout $a, b, c \in A$ avec a et b premiers entre eux.

Proposition 38. On suppose A factoriel. Tout élément $a \neq 0$ peut s'écrire de manière unique **[ULM18]** p. 65

$$a = u_a \prod_{p \in \mathcal{S}} p^{v_p(a)}$$

où $\mathcal{S}$ est un **système de représentants d'éléments premiers** de A (pour le relation $\sim$), u_a est inversible et $v_p(a) \in \mathbb{N}$ tous nuls sauf un nombre fini.

Exemple 39. Dans l'anneau principal (donc factoriel, voir Théorème 41) $\mathbb{Z}$, un choix standard pour $\mathcal{S}$ est l'ensemble des nombres premiers positifs.

Proposition 40. On suppose A factoriel. Soient $a, b \in A^*$. Alors, en reprenant les notations précédentes :

(i) $a \mid b \iff v_p(a) \leq v_p(b)$ pour tout $p \in \mathcal{S}$.

(ii) $\prod_{p \in \mathcal{S}} p^{\min(v_p(a), v_p(b))}$ est un PGCD de a et de b.

(iii) $\prod_{p \in \mathcal{S}} p^{\max(v_p(a), v_p(b))}$ est un PPCM de a et de b.

Théorème 41. Tout anneau principal est factoriel.

Contre-exemple 42. $\mathbb{Z}[i\sqrt{5}]$ est principal mais n'est pas factoriel.

Lemme 43 (Gauss)**.** On suppose A factoriel. Alors : [GOZ] p. 10

(i) Le produit de deux polynômes primitifs est primitif (ie. dont le PGCD des coefficients est associé à 1).

(ii) $\forall P, Q \in A[X] \setminus \{0\}$, $\gamma(PQ) = \gamma(P)\gamma(Q)$ (où $\gamma(P)$ est le contenu du polynôme P).

Théorème 44 (Critère d'Eisenstein)**.** Soient $\mathbb{K}$ le corps des fractions de A et $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ de degré $n \geq 1$. On suppose que A est factoriel et qu'il existe $p \in A$ irréductible tel que :

(i) $p \mid a_i$, $\forall i \in [\![0, n-1]\!]$.

(ii) $p \nmid a_n$.

(iii) $p^2 \nmid a_0$.

Alors P est irréductible dans $\mathbb{K}[X]$.

Application 45. Soit $n \in \mathbb{N}^*$. Il existe des polynômes irréductibles de degré n sur $\mathbb{Z}$. [PER] p. 67

3. Théorème chinois

[DEV]

Théorème 46 (Chinois)**.** Soient $I_1, \dots I_n$ des idéaux de A tels que $\forall i \neq j$, $I_i + I_j = A$. Alors, [ULM18] p. 56

$$\varphi : \begin{array}{ccc} A & \to & A/I_1 \times \cdots \times A/I_n \\ a & \mapsto & (a + I_1, \dots, a + I_n) \end{array}$$

est un morphisme surjectif de noyau $I = \bigcap_{i=1}^{n} I_i$. En particulier, A/I est isomorphe à $A/I_1 \times \cdots \times A/I_n$.

Corollaire 47. On suppose A principal. Pour tout $\beta_1, \dots, \beta_n \in A$ et $m_1, \dots, m_n \in A$ premiers entre eux deux à deux, le système de congruences

$$\begin{cases} u \equiv \beta_1 \mod m_1 \\ \vdots \\ u \equiv \beta_n \mod m_n \end{cases}$$

admet une unique solution $u + (m_1 m_2 \dots m_n)$ dans $A/(m_1 m_2 \dots m_n)$. Il existe donc dans A une unique solution u unique à multiples de $m_1 m_2 \dots m_n$ près.

Exemple 48. Le système

$$\begin{cases} u \equiv 1 \mod 3 \\ u \equiv 3 \mod 5 \\ u \equiv 0 \mod 7 \end{cases}$$

admet une unique solution dans $\mathbb{Z}/105\mathbb{Z}$: $\overline{28}$. Les solutions dans $\mathbb{Z}$ sont donc de la forme $28 + 105k$ avec $k \in \mathbb{Z}$.

Application 49 (Polynômes d'interpolation de Lagrange)**.** Soit $\mathbb{K}$ un corps commutatif, $\alpha_1, \dots, \alpha_n$ des éléments distincts de $\mathbb{K}$ et $\beta_1, \dots, \beta_n$ des éléments de $\mathbb{K}$. Alors, il existe un unique polynôme $g \in \mathbb{K}[X]$ de degré inférieur ou égal à n tel que $g(\alpha_i) = \beta_i$ pour tout $i \in [\![1, n]\!]$.

III - Applications

1. Équations diophantiennes

Définition 50. L'anneau $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ est **l'anneau des entiers de Gauss**. On définit

$$N : \begin{array}{ccc} \mathbb{Z}[i] & \to & \mathbb{N} \\ x + iy & \mapsto & x^2 + y^2 \end{array}$$

p. 69

Notation 51. On note Σ l'ensemble des entiers qui sont somme de deux carrés.

[I-P] p. 137

Lemme 52. Soit $p \geq 3$ un nombre premier. Alors $x \in \mathbb{F}_p^*$ est un carré si et seulement si $x^{\frac{p-1}{2}} = 1$.

Lemme 53. (i) N est multiplicative.

(ii) $\mathbb{Z}[i]^* = \{z \in \mathbb{Z}[i] \mid N(z) = 1\} = \{\pm 1, \pm i\}$.

(iii) $\mathbb{Z}[i]$ est euclidien de stathme N.

Lemme 54. Soit p un nombre premier. Si p n'est pas irréductible dans $\mathbb{Z}[i]$, alors $p \in \Sigma$.

[DEV]

Théorème 55 (Deux carrés de Fermat)**.** Soit $n \in \mathbb{N}^*$. Alors $n \in \Sigma$ si et seulement si $v_p(n)$ est pair pour tout p premier tel que $p \equiv 3 \mod 4$ (où $v_p(n)$ désigne la valuation p-adique de n).

2. En algèbre linéaire

Soit E un espace vectoriel de dimension finie n sur un corps $\mathbb{K}$. Soit $f : E \to E$ un endomorphisme de E.

Application 56. Il existe un unique polynôme de $\mathbb{K}[X]$ unitaire qui engendre l'idéal $\{P \in \mathbb{K}[X] \mid P(f) = 0\}$: c'est le **polynôme minimal** de f, noté π_f. Il s'agit du polynôme unitaire de plus bas degré annulant f. Il divise tous les autres polynômes annulateurs de f.

[GOU21] p. 186

Théorème 57 (Lemme des noyaux)**.** Soit $P = P_1 \dots P_k \in \mathbb{K}[X]$ où les polynômes $P_1, \dots, P_k$ sont premiers entre eux deux à deux. Alors,

$$\operatorname{Ker}(P(f)) = \bigoplus_{i=1}^{k} \operatorname{Ker}(P_i(f))$$

Application 58. f est diagonalisable si et seulement si π_f est scindé à racines simples.

123 Corps finis. Applications.

Soient p un nombre premier, n un nombre entier, et $q = p^n$.

I - Construction

1. Caractéristique, sous-corps premier

[GOZ] p. 7

Définition 1. Soit A un anneau. L'application

$$f_A : \begin{array}{ccc} \mathbb{Z} & \to & A \\ n & \mapsto & \underbrace{1+\cdots+1}_{n \text{ fois}} \end{array}$$

On note $\text{car}(A)$ l'unique $n \in \mathbb{N}$ tel que $\text{Ker}(f_A) = n\mathbb{Z}$: c'est la **caractéristique** de A.

Exemple 2. La caractéristique de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est n.

Proposition 3. (i) Soit A un anneau intègre. Alors, $\text{car}(A) = 0$ ou p avec p premier.

(ii) Soit A un anneau fini. Alors, $\text{car}(A) \neq 0$ et $\text{car}(A) \mid |A|$.

(iii) Un anneau et un quelconque de ses sous-anneaux ont la même caractéristique.

Remarque 4. — Le Point (i) est en particulier vrai pour un corps.

— Si $\text{car}(A) = 0$, A est infini.

Définition 5. Soit $\mathbb{K}$ un corps.

— $\mathbb{K}$ est dit **premier** s'il n'a pas d'autre sous-corps que lui-même.

— Le **sous-corps premier** de $\mathbb{K}$ est le sous-corps de $\mathbb{K}$ engendré par 1 (ie. l'intersection de tous les sous-corps de $\mathbb{K}$) : c'est un corps premier.

Remarque 6. Un corps et l'un de ses sous-corps ont le même sous-corps premier.

Proposition 7. Soient $\mathbb{K}$ un corps et $\mathbb{P}$ son corps premier. Alors, si $\text{car}(\mathbb{K}) = 0$, $\mathbb{P} \cong \mathbb{Q}$.

2. Construction de $\mathbb{F}_p$

Proposition 8. Les conditions suivantes sont équivalentes :
(i) n est un nombre premier.
(ii) $\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre.
(iii) $\mathbb{Z}/n\mathbb{Z}$ est un corps.

p. 3

Notation 9. On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Proposition 10. Soit $\mathbb{K}$ un corps fini.
(i) $\text{car}(\mathbb{K})$ est un nombre premier p.
(ii) Le sous-corps premier de $\mathbb{K}$ est isomorphe à $\mathbb{F}_p$.
(iii) $|\mathbb{K}| = p^m$ pour $m \geq 2$.

p. 81

Exemple 11. — Il n'existe pas de corps fini à 6 éléments.
— $\mathbb{F}_p(X)$, est un corps infini de caractéristique p.

Proposition 12. Tout corps fini à p éléments est isomorphe à $\mathbb{F}_p$.

p. 8

3. Construction de $\mathbb{F}_q$

Proposition 13. Soit $\mathbb{K}$ un corps de caractéristique p. L'application

$$\text{Frob} : \begin{array}{ccc} \mathbb{K} & \to & \mathbb{K} \\ x & \mapsto & x^p \end{array}$$

est un morphisme de corps.
(i) Si $\mathbb{K}$ est fini, c'est un automorphisme.
(ii) Si $\mathbb{K} = \mathbb{F}_p$, c'est l'identité.

p. 85

Corollaire 14. Dans un corps fini de caractéristique p, chaque élément admet exactement une racine p-ième.

Application 15 (Petit théorème de Fermat)**.**

$$\forall x \in \mathbb{Z},\ x^p \equiv x \mod p$$

Théorème 16. (i) Il existe un corps $\mathbb{K}$ à q éléments : c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.

(ii) $\mathbb{K}$ est unique à isomorphisme près : on le note $\mathbb{F}_q$.

Corollaire 17. Le produit des éléments de $\mathbb{F}_q^*$ vaut -1.

Application 18 (Théorème de Wilson)**.** Soit $n \geq 2$ un entier. Alors,

$$n \text{ est premier} \iff (n-1)! + 1 \equiv 0 \mod n$$

II - Propriétés

1. Commutativité

Définition 19. L'ensemble des générateurs de μ_n, noté μ_n^*, est formé des **racines primitives n-ièmes de l'unité**. p. 67

Proposition 20. (i) $\mu_n^* = \{e^{\frac{2ik\pi}{n}} \mid k \in [\![0, n-1]\!], \text{pgcd}(k, m) = 1\}$.

(ii) $|\mu_n^*| = \varphi(n)$, où φ désigne l'indicatrice d'Euler.

Définition 21. On appelle **n-ième polynôme cyclotomique** le polynôme

$$\Phi_n = \prod_{\xi \in \mu_n^*} (X - \xi)$$

Théorème 22. (i) $X^n - 1 = \prod_{d|n} \Phi_d$.

(ii) $\Phi_n \in \mathbb{Z}[X]$.

(iii) Φ_n est irréductible sur $\mathbb{Q}$.

[DEV]

Théorème 23 (Wedderburn)**.** Tout corps fini est commutatif. [GOU21] p. 100

2. Sous-corps

Théorème 24. Tout sous-corps de $\mathbb{F}_q$ est de cardinal p^d avec $d \mid n$. Réciproquement, pour tout $d \mid n$, $\mathbb{F}_q$ admet un unique sous-corps de cardinal p^d. [ULM18] p. 122

Exemple 25. Les sous-corps de $\mathbb{F}_{2^{12}}$ sont $\mathbb{F}_{2^6}$, $\mathbb{F}_{2^4}$, $\mathbb{F}_{2^3}$, $\mathbb{F}_{2^2}$ et $\mathbb{F}_2$.

Corollaire 26. Le polynôme $X^q - X \in \mathbb{F}_p[X]$ est produit de tous les polynômes irréductibles unitaires de $\mathbb{F}_p[X]$ dont le degré divise n.

Corollaire 27. Il existe des polynômes irréductibles de tout degré dans $\mathbb{F}_q[X]$.

Corollaire 28. Un corps de rupture d'un polynôme irréductible de $\mathbb{F}_q[X]$ sur $\mathbb{F}_q$ est aussi un corps de décomposition pour ce polynôme sur $\mathbb{F}_q$.

3. Groupe multiplicatif

Théorème 29. Tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique. [GOZ] p. 83

Corollaire 30. Le groupe multiplicatif d'un corps fini est cyclique.

Corollaire 31.

$$\mathbb{F}_q^* \cong \mathbb{Z}/(q-1)\mathbb{Z}$$

4. Groupe des automorphismes

Théorème 32. Le groupe des automorphismes de $\mathbb{F}_q$ est cyclique, engendré par Frob, et d'ordre n.

Proposition 33. Pour chaque application $f : \mathbb{F}_q \to \mathbb{F}_q$, il existe un unique polynôme $P \in \mathbb{F}_q[X]$ de degré inférieur ou égal à $q-1$ tel que

$$P = \sum_{u \in \mathbb{F}_q} f(u)(1-(X-u)^{q-1})$$

Proposition 34. Les sous-groupes additifs de $\mathbb{F}_q$ sous les sous-$\mathbb{F}_q$-espaces vectoriels. Ils sont au nombre de

$$\sum_{s=0}^{n} \frac{(p^n-1)(p^{n-1}-1)\dots(p^{n-s+1}-1)}{(p^s-1)(p^{s-1}-1)\dots(p-1)}$$

5. Carrés

Proposition 35. On note $\mathbb{F}_q^2 = \{x^2 \mid x \in \mathbb{F}_q\}$ et $\mathbb{F}_q^{*2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$. Alors $\mathbb{F}_q^{*2}$ est un sous-groupe de $\mathbb{F}_q^*$.

p. 93

Proposition 36. (i) Si $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$, donc $\mathbb{F}_q^{*2} = \mathbb{F}_q^*$.

(ii) Si $p > 2$, alors :

- $\mathbb{F}_q^{*2}$ est le noyau de l'endomorphisme de $\mathbb{F}_q^*$ défini par $x \mapsto x^{\frac{q-1}{2}}$.
- $\mathbb{F}_q^{*2}$ est un sous-groupe d'indice 2 de $\mathbb{F}_q^*$.
- $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$ et $|\mathbb{F}_q^2| = \frac{q+1}{2}$.
- $(-1) \in \mathbb{F}_q^{*2} \iff q \equiv 1 \mod 4$.

On suppose, pour la suite de cette sous-section, $p > 2$.

p. 155

Définition 37. On définit le **symbole de Legendre** $\left(\frac{x}{p}\right)$ pour $x \in \mathbb{F}_p^*$ par :

$$\left(\frac{x}{p}\right) = \pm 1 \text{ avec } \left(\frac{x}{p}\right) = 1 \iff x \in \mathbb{F}_p^{*2}$$

Proposition 38. $x \mapsto \left(\frac{x}{p}\right)$ est un morphisme de groupes non constant et,

$$\forall x \in \mathbb{F}_p^{*2}, \left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$$

Théorème 39 (Loi de réciprocité quadratique)**.** Soit $q \neq p$ un premier impair. Alors,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

Remarque 40. Cela signifie qu'il est équivalent d'avoir p résidu quadratique modulo q ou q résidu quadratique modulo p, sauf si $p \equiv q \equiv 3 \mod 4$ auquel cas ces propositions s'excluent mutuellement.

Proposition 41.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{(p-1)^2}{8}}$$

Exemple 42.

$$\left(\frac{17}{41}\right) = (-1)^{8\times 20}\left(\frac{41}{27}\right) = \left(\frac{7}{17}\right) = (-1)^{3\times 8}\left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = (-1)^3\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

III - Applications

1. Irréductibilité de polynômes

Théorème 43. Soit $P \in \mathbb{K}[X]$ un polynôme irréductible sur un corps $\mathbb{K}$. p. 57

- Il existe un corps de rupture de P.
- Si $\mathbb{L} = \mathbb{K}[\alpha]$ et $\mathbb{L}' = \mathbb{K}[\beta]$ sont deux corps de rupture de P, alors il existe un unique $\mathbb{K}$-isomorphisme $\varphi : \mathbb{L} \to \mathbb{L}'$ tel que $\varphi(\alpha) = \beta$.
- $\mathbb{K}[X]/(P)$ est un corps de rupture de P.

Lemme 44 (Gauss)**.** (i) Le produit de deux polynômes primitifs est primitif (ie. dont le PGCD des coefficients est égal à 1). p. 10

(ii) $\forall P, Q \in \mathbb{Z}[X] \setminus \{0\}$, $\gamma(PQ) = \gamma(P)\gamma(Q)$ (où $\gamma(P)$ est le contenu du polynôme P).

Théorème 45 (Critère d'Eisenstein)**.** Soit $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ de degré $n \geq 1$. On suppose qu'il existe p premier tel que :

(i) $p \mid a_i$, $\forall i \in [\![0, n-1]\!]$.

(ii) $p \nmid a_n$.

(iii) $p^2 \nmid a_0$.

Alors P est irréductible dans $\mathbb{Q}[X]$.

Application 46. Soit $n \in \mathbb{N}^*$. Il existe des polynômes irréductibles de degré n sur $\mathbb{Z}$. **[PER]** p. 67

Théorème 47 (Critère d'irréductibilité modulo p)**.** Soit $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ de degré $n \geq 1$. Soit p un premier. On suppose $p \nmid a_n$. **[GOZ]** p. 12

Si $\overline{P}$ est irréductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$, alors P est irréductible dans $\mathbb{Q}[X]$.

Exemple 48. Le polynôme $X^3 - 127X^2 + 3608X + 19$ est irréductible dans $\mathbb{Z}[X]$.

2. Entiers sommes de deux carrés

Notation 49. On note **[I-P]** p. 137

$$N : \begin{array}{ccc} \mathbb{Z}[i] & \to & \mathbb{N} \\ a+ib & \mapsto & a^2+b^2 \end{array}$$

et Σ l'ensemble des entiers qui sont somme de deux carrés.

Remarque 50. $n \in \Sigma \iff \exists z \in \mathbb{Z}[i]$ tel que $N(z) = n$.

Théorème 51 (Deux carrés de Fermat)**.** Soit $n \in \mathbb{N}^*$. Alors $n \in \Sigma$ si et seulement si $v_p(n)$ est pair pour tout p premier tel que $p \equiv 3 \mod 4$ (où $v_p(n)$ désigne la valuation p-adique de n).

3. En algèbre linéaire

Lemme 52. Soient $p \geq 3$ un nombre premier et V un espace vectoriel sur $\mathbb{F}_p$ de dimension finie. Les dilatations engendrent $\mathrm{GL}(V)$. **[I-P]** p. 203

[DEV]

Théorème 53 (Frobenius-Zolotarev)**.** Soient $p \geq 3$ un nombre premier et V un espace vectoriel sur $\mathbb{F}_p$ de dimension finie.

$$\forall u \in \mathrm{GL}(V), \epsilon(u) = \left(\frac{\det(u)}{p}\right)$$

où u est vu comme une permutation des éléments de V.

On se place pour la suite de cette sous-section dans le cadre d'un espace vectoriel E de dimension m sur le corps $\mathbb{F}_q$. [ULM21] p. 124

Proposition 54. Les groupes précédents sont finis, et :

(i) $|\mathrm{GL}(E)| = q^{\frac{m(m-1)}{2}}((q^m-1)\dots(q-1))$.

(ii) $|\mathrm{PGL}(E)| = |\mathrm{SL}(E)| = \frac{|\mathrm{GL}(E)|}{q-1}$.

(iii) $|\mathrm{PSL}(E)| = |\mathrm{SL}(E)| = \frac{|\mathrm{GL}(E)|}{(q-1)\mathrm{pgcd}(m,q-1)}$.

Application 55. Pour tout entier $p \in [\![1, m]\!]$, il y a [ROM21] p. 157

$$\frac{\prod_{k=m-(p-1)}^{n}(q^k-1)}{\prod_{k=1}^{p}(q^k-1)}$$

sous-espaces vectoriels de dimension p dans E.

4. Codes correcteurs

Définition 56. On appelle : [BMP] p. 190

— **Mot** un vecteur à coefficients dans $\mathbb{F}_q$.

— **Code correcteur** de taille m un sous-ensemble de $\mathbb{F}_q^m$.

— **Code linéaire** de taille m et de dimension r un sous-espace vectoriel de dimension r de $\mathbb{F}_q^m$.

— **Code cyclique** de taille m, un code linéaire stable par décalage circulaire.

Exemple 57. Soit un code linéaire $\mathscr{C}$ de taille m et de dimension r. On peut décrire $\mathscr{C}$ avec une matrice $G \in \mathscr{M}_{m\times r}(\mathbb{F}_q)$, dont les colonnes forment une base de $\mathscr{C}$, de la manière suivante :

$$\mathscr{C} = \{Gx \mid x \in \mathbb{F}_q^m\}$$

G est la **matrice génératrice** de $\mathscr{C}$. Le codage consiste alors à transformer un mot m du message d'origine en un mot $c \in \mathscr{C}$.

Définition 58.
— Le **poids** d'un mot $x \in \mathbb{F}_q^m$, noté $\omega(x)$ est le nombre de coefficients non nuls de x.
— La **distance de Hamming** entre deux mots $x, y \in \mathbb{F}_q^m$, est définie par $d_H(x,y) = \omega(x-y)$.

Cette distance permet de mesurer la qualité d'un code comme l'atteste la remarque ci-dessous.

Remarque 59. d_H est une distance, elle quantifie la notion de "mot le plus proche".

Définition 60. Un code $\mathscr{C}$ est dit t-correcteur si les boules de centre un mot du code et de rayon t (pour d_H) sont disjointes : les mots de $\mathscr{C}$ sont à une distance d'au moins $2t+1$ les uns des autres.

Proposition 61. Soit $\mathscr{C}$ un code correcteur. On note d la **distance minimale** de $\mathscr{C}$:

$$d = \min_{\substack{x,y\in\mathscr{C}\\ x\neq y}} \{d_H(x,y)\}$$

Alors $\mathscr{C}$ est t-correcteur si et seulement si $d \geq 2t+1$.

Exemple 62. On considère le code $\mathscr{C}$ de taille 7 et de dimension 4 sur $\mathbb{F}_2$ dont la matrice génératrice est

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$\mathscr{C}$ est un code linéaire, dont chacun des mots non nuls est de poids supérieur à 3 : il est 1-correcteur.

Proposition 63 (Borne de Singleton)**.** Soit $\mathscr{C}$ un code linéaire de longueur m, de dimension r et de distance minimale d. Alors,

$$d = \min_{x\in\mathscr{C}\setminus\{0\}} \{\omega(x)\} \leq m+1-r$$

Annexes

[ULM18]
p. 122

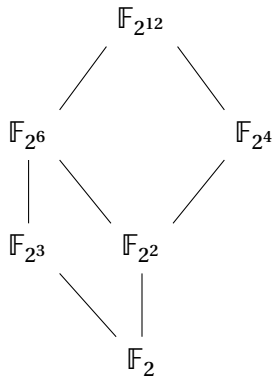


FIGURE I.3 – Sous-corps de $\mathbb{F}_{2^{12}}$.

125 Extensions de corps. Exemples et applications.

Sauf mention contraire, les corps sont supposés commutatifs. Soit $\mathbb{K}$ un corps.

I - Extensions de corps

1. Généralités

a. Définition

Définition 1. On appelle **extension** de $\mathbb{K}$ tout corps $\mathbb{L}$ tel que

$$\exists j : \mathbb{K} \to \mathbb{L} \text{ morphisme de corps}$$

On note cela $\mathbb{L}/\mathbb{K}$.

[GOZ] p. 21

Remarque 2.
- Si $\mathbb{K}$ est un sous-corps de $\mathbb{L}$, alors $\mathbb{L}$ est une extension de $\mathbb{K}$.
- Réciproquement, un morphisme de corps $j : \mathbb{K} \to \mathbb{L}$ est forcément injectif. Par conséquent, le sous-corps $\mathbb{K}' = j(\mathbb{K})$ de $\mathbb{L}$ est isomorphe à $\mathbb{K}$.
- Aux notations abusives près, on a donc

$$\mathbb{K} \text{ est un sous-corps de } \mathbb{L} \iff \mathbb{L} \text{ est une extension de } \mathbb{K}$$

Exemple 3.
- $\mathbb{C}$ est une extension de $\mathbb{R}$.
- $\mathbb{R}$ est une extension de $\mathbb{Q}$.
- $\mathbb{K}(X)$ est une extension de $\mathbb{K}$.

Proposition 4. Soit $\mathbb{L}$ une extension de $\mathbb{K}$ dont on note j le morphisme d'inclusion. Alors, muni du "produit par un scalaire" défini par

$$\forall \lambda \in \mathbb{K}, \forall x \in \mathbb{L}, \lambda x = j(\lambda) \cdot x$$

$\mathbb{L}$ est une algèbre sur $\mathbb{K}$.

b. Degré

Définition 5. Soit $\mathbb{L}$ une extension de $\mathbb{K}$. On appelle **degré** de $\mathbb{L}/\mathbb{K}$ et on note $[\mathbb{L}:\mathbb{K}]$ la dimension de $\mathbb{L}$ considéré comme un espace vectoriel sur $\mathbb{K}$.

Remarque 6.
— $[\mathbb{L}:\mathbb{K}] = 1 \iff \mathbb{L} = \mathbb{K}$.
— Le degré d'une extension peut être fini ($[\mathbb{C}:\mathbb{R}] = 2$) ou infini ($[\mathbb{R}:\mathbb{Q}] = +\infty$).

Théorème 7 (Base télescopique)**.** Soient $\mathbb{L}$ un sur-corps de $\mathbb{K}$ et E un espace vectoriel sur $\mathbb{L}$.Soient $(e_i)_{i\in I}$ une base de E en tant que $\mathbb{L}$-espace vectoriel et $(\alpha_j)_{j\in J}$ une base de $\mathbb{L}$ en tant que $\mathbb{K}$-espace vectoriel.

Alors $(\alpha_j e_i)_{(i,j)\in I\times J}$ est une base de E en tant que $\mathbb{K}$-espace vectoriel.

Corollaire 8 (Multiplicativité des degrés)**.** Soient $\mathbb{L}$ une extension de $\mathbb{K}$ et $\mathbb{M}$ une extension de $\mathbb{L}$. Alors, sont équivalentes :

(i) $\mathbb{M}$ est un $\mathbb{K}$-espace vectoriel de dimension finie.

(ii) $\mathbb{M}$ est un $\mathbb{L}$-espace vectoriel de dimension finie et $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel de dimension finie.

On a alors :

$$\dim_{\mathbb{K}}(M) = \dim_{\mathbb{L}}(M)\dim_{\mathbb{K}}(L) \iff [\mathbb{M}:\mathbb{K}] = [\mathbb{M}:\mathbb{L}][\mathbb{L}:\mathbb{K}]$$

c. Générateurs

Définition 9. Soit $\mathbb{L}$ une extension de $\mathbb{K}$.
— Soit $A \subseteq \mathbb{L}$. On dit que A **engendre** $\mathbb{L}$ sur $\mathbb{K}$ si $\mathbb{L}$ est le plus petit sous corps de $\mathbb{L}$ contenant $\mathbb{K}$ et A. On note cela $\mathbb{L} = \mathbb{K}(A)$ ou, si $A = \{\alpha_1, \dots, \alpha_n\}$ est fini, $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_n)$ et $\mathbb{L}$ est alors **de type fini**.
— L'extension $\mathbb{L}/\mathbb{K}$ est dite **monogène** s'il existe $\alpha \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}(\alpha)$.

[PER] p. 66

Exemple 10.
— Une extension $\mathbb{L}$ de $\mathbb{K}$ de degré fini est de type fini sur $\mathbb{K}$.
— Si $[\mathbb{L}:\mathbb{K}]$ est un nombre premier, alors $\mathbb{L}$ est une extension monogène de $\mathbb{K}$.

[GOZ] p. 23

Remarque 11. Si $\mathbb{L} = \mathbb{K}(\alpha)$ est une extension monogène de $\mathbb{K}$, il n'y a pas unicité de α. Tout élément $u \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}(u)$ est appelé **élément primitif** de $\mathbb{L}/\mathbb{K}$.

[PER] p. 66

Définition 12. Soient $\mathbb{L}$ une extension de $\mathbb{K}$ et $\alpha \in \mathbb{L}$. On note $\mathbb{K}[\alpha]$ le sous-anneau de $\mathbb{L}$ engendré par $\mathbb{K}$ et α.

Proposition 13. En reprenant les notations précédentes :

(i) Si $x \in \mathbb{K}[\alpha], x = P(\alpha)$ avec $P \in \mathbb{K}[X]$.

(ii) Si $x \in \mathbb{K}(\alpha), x = \frac{P(\alpha)}{Q(\alpha)}$ avec $P, Q \in \mathbb{K}[X]$ et $Q(\alpha) \neq 0$.

(iii) $\mathbb{K}[\alpha] \subseteq \mathbb{K}(\alpha)$.

2. Algébricité

Définition 14. Soient $\mathbb{L}$ une extension de $\mathbb{K}$ et $\alpha \in \mathbb{L}$. Soit $\mathrm{ev}_\alpha : \mathbb{K}[X] \to \mathbb{L}$ le morphisme d'évaluation en α.

— On note $\mathrm{Ann}(\alpha)$ l'idéal des polynômes annulateurs de α. Notons qu'on a $\mathrm{Ann}(\alpha) = \mathrm{Ker}(\mathrm{ev}_\alpha)$.

— Si ev_α est injectif, on dit que α est **transcendant** sur $\mathbb{K}$.

— Sinon, α est dit **algébrique** sur $\mathbb{K}$.

Exemple 15. — e et π sont transcendants sur $\mathbb{Q}$ (théorèmes d'Hermite et de Lindemann).

— $\sqrt{2}$, i, ... sont algébriques sur $\mathbb{Q}$.

Proposition 16. Soient $\mathbb{L}$ une extension de $\mathbb{K}$ et $\alpha \in \mathbb{L}$. Les assertions suivantes sont équivalentes.

(i) α est algébrique sur $\mathbb{K}$.

(ii) $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$.

(iii) $[\mathbb{K}[\alpha] : \mathbb{K}] < +\infty$.

Proposition 17. En reprenant les notations précédentes, si α est transcendant, on a

$$\mathbb{K}[\alpha] \cong \mathbb{K}[X] \text{ et } \mathbb{K}(\alpha) \cong \mathbb{K}(X)$$

Définition 18. Soient $\mathbb{L}$ une extension de $\mathbb{K}$ et $\alpha \in \mathbb{L}$. Si α est algébrique sur $\mathbb{K}$, alors $\mathrm{Ann}(\alpha)$ est un idéal principal non nul. Donc, il existe $P \in \mathbb{K}[X]$ unitaire tel que $\mathrm{Ann}(\alpha) = (P)$. On note π_α ce polynôme P : c'est le **polynôme minimal** de α sur $\mathbb{K}$.

Exemple 19. Sur $\mathbb{Q}$, on a $\pi_{\sqrt{2}} = X^2 - 2$ et $\pi_i = X^2 + 1$.

Proposition 20. Soient $\mathbb{L}$ une extension de $\mathbb{K}$ et $\alpha \in \mathbb{L}$. Soient $P \in \mathbb{K}[X]$. Les assertions suivantes sont équivalentes : [GOZ] p. 31

(i) $P = \pi_\alpha$.

(ii) $P \in \mathrm{Ann}(\alpha)$ et est unitaire et $\forall R \in \mathrm{Ann}(\alpha) \setminus \{0\}$, $\deg(P) \leq \deg(R)$.

(iii) $P \in \mathrm{Ann}(\alpha)$ et est unitaire et irréductible dans $\mathbb{K}[X]$.

Définition 21. Soit $\mathbb{L}$ une extension de $\mathbb{K}$. [PER] p. 67

— $\mathbb{L}/\mathbb{K}$ est dite **finie** si $[\mathbb{L} : \mathbb{K}] < +\infty$.

— $\mathbb{L}/\mathbb{K}$ est dite **algébrique** si tout élément de $\mathbb{L}$ est algébrique sur $\mathbb{K}$.

Proposition 22. Toute extension finie est algébrique.

Contre-exemple 23. On considère

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ est algébrique sur } \mathbb{Q}\}$$

alors, $\overline{\mathbb{Q}}$ est une extension algébrique de $\mathbb{Q}$ mais n'est pas finie (cf. Théorème 26).

Lemme 24 (Gauss)**.** Soit A un anneau factoriel. Alors : [GOZ] p. 10

(i) Le produit de deux polynômes primitifs est primitif (ie. dont le PGCD des coefficients est associé à 1).

(ii) $\forall P, Q \in A[X] \setminus \{0\}$, $\gamma(PQ) = \gamma(P)\gamma(Q)$ (où $\gamma(P)$ est le contenu du polynôme P).

[DEV]

Théorème 25 (Critère d'Eisenstein)**.** On suppose que $\mathbb{K}$ le corps des fractions d'un anneau factoriel A. Soit $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ de degré $n \geq 1$. On suppose qu'il existe $p \in A$ irréductible tel que :

(i) $p \mid a_i$, $\forall i \in [\![0, n-1]\!]$.

(ii) $p \nmid a_n$.

(iii) $p^2 \nmid a_0$.

Alors P est irréductible dans $\mathbb{K}[X]$.

Application 26. Soit $n \in \mathbb{N}^*$. Il existe des polynômes irréductibles de degré n sur $\mathbb{Z}$. **[PER]** p. 67

II - Adjonction de racines

1. Corps de rupture

Définition 27. Soient $\mathbb{L}$ une extension de $\mathbb{K}$ et $P \in \mathbb{K}[X]$ irréductible. On dit que $\mathbb{L}$ est un **corps de rupture** de P si $\mathbb{L} = \mathbb{K}[\alpha]$ où $\alpha \in \mathbb{L}$ est une racine de P. **[GOZ]** p. 57

Exemple 28. En reprenant les notations précédentes, si $\deg(P) = 1$, alors $\mathbb{K}$ est un corps de rupture de P.

Théorème 29. Soit $P \in \mathbb{K}[X]$ un polynôme irréductible sur $\mathbb{K}$.

— Il existe un corps de rupture de P.

— Si $\mathbb{L} = \mathbb{K}[\alpha]$ et $\mathbb{L}' = \mathbb{K}[\beta]$ sont deux corps de rupture de P, alors il existe un unique $\mathbb{K}$-isomorphisme $\varphi : \mathbb{L} \to \mathbb{L}'$ tel que $\varphi(\alpha) = \beta$.

Application 30. $X^2 + 1$ est un polynôme irréductible sur $\mathbb{R}$ dont $\mathbb{R}[X]/(X^2+1)$ est un corps de rupture. On pose alors $\mathbb{C} = \mathbb{R}[X]/(X^2+1)$, le corps des nombres complexes, et on note i la classe de X dans l'anneau quotient.

Remarque 31. Si $\mathbb{L}$ est un corps de rupture d'un polynôme $P \in \mathbb{K}[X]$, on a $[\mathbb{L} : \mathbb{K}] = \deg(P)$. Plus précisément, une base de $\mathbb{L}$ en tant que $\mathbb{K}$-espace vectoriel est $(1, \alpha, \dots, \alpha^{\deg(P)-1})$.

2. Corps de décomposition

Définition 32. Soit $P \in \mathbb{K}[X]$ de degré $n \geq 1$. On dit que $\mathbb{L}$ est un **corps de décomposition** de P si :

— Il existe $a \in \mathbb{L}$ et $\alpha_1, \dots, \alpha_n \in \mathbb{L}$ tels que $P = a(X - \alpha_1) \dots (X - \alpha_n)$.

— $\mathbb{L} = \mathbb{K}[\alpha_1, \dots, \alpha_n]$.

Exemple 33.
— $\mathbb{K}$ est un corps de décomposition de tout polynôme de degré 1 sur $\mathbb{K}$.

— $\mathbb{C}$ est un corps de décomposition de $X^2 + 1$ sur $\mathbb{R}$.

Théorème 34. Soit $P \in \mathbb{K}[X]$ un polynôme de degré supérieur ou égal à 1.
— Il existe un corps de décomposition de P.
— Deux corps de décomposition de P sont $\mathbb{K}$-isomorphes.

[DEV]

Application 35. Soit $A \in \mathcal{M}_n(\mathbb{K})$. On note $\mathcal{C}(A)$ le commutant de A. Alors,

$$\mathbb{K}[A] = \mathcal{C}(A) \iff \pi_A = \chi_A = \det(XI_n - A)$$

[FGN2] p. 160

3. Clôture algébrique

Proposition 36. Les assertions suivantes sont équivalentes :
(i) Tout polynôme de $\mathbb{K}[X]$ de degré supérieur ou égal à 1 est scindé sur $\mathbb{K}$.
(ii) Tout polynôme de $\mathbb{K}[X]$ de degré supérieur ou égal à 1 admet au moins une racine dans $\mathbb{K}$.
(iii) Les seuls polynômes irréductibles de $\mathbb{K}[X]$ sont ceux de degré 1.
(iv) Toute extension algébrique de $\mathbb{K}$ est égale à $\mathbb{K}$.

[GOZ] p. 62

Définition 37. Si $\mathbb{K}$ vérifie un des points de la Théorème 36, $\mathbb{K}$ est dit **algébriquement clos**.

Proposition 38. Tout corps algébriquement clos est infini.

Contre-exemple 39. $\mathbb{Q}$ et même $\mathbb{R}$ ne sont pas algébriquement clos.

Théorème 40 (D'Alembert-Gauss)**.** $\mathbb{C}$ est algébriquement clos.

Définition 41. On dit que $\mathbb{L}$ est une **clôture algébrique** de $\mathbb{K}$ si $\mathbb{L}$ est une extension de $\mathbb{K}$ algébriquement close et si

$$\forall x \in \mathbb{L}, \exists P \in \mathbb{K}[X] \text{ tel que } P(x) = 0$$

Exemple 42. — $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.
— $\overline{\mathbb{Q}}$ du Théorème 23 est une clôture algébrique de $\mathbb{Q}$.

Théorème 43 (Steinitz)**.** (i) Il existe une clôture algébrique de $\mathbb{K}$.
(ii) Deux clôtures algébriques de $\mathbb{K}$ sont $\mathbb{K}$-isomorphes.

III - Corps particuliers

1. Corps finis

Soit $q = p^n$ où p est un nombre et n un entier supérieur ou égal à 1.

Proposition 44. Les conditions suivantes sont équivalentes : p. 3

(i) n est un nombre premier.

(ii) $\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre.

(iii) $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Notation 45. On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Théorème 46. p. 85

(i) Il existe un corps fini à q éléments : c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.

(ii) Si F et F' sont deux corps finis à q éléments, ils sont $\mathbb{F}_p$-isomorphes.

On peut donc noter $\mathbb{F}_q$ l'unique (à isomorphisme près) corps fini à q éléments.

Théorème 47. Soit F un corps fini. Alors : p. 81

(i) Sa caractéristique est un nombre premier p.

(ii) Il existe $n \geq 1$ tel que $|F\| = p^n$.

On a donc $F = \mathbb{F}_{p^n}$.

Exemple 48. Il n'existe pas de corps fini à 6 éléments.

Théorème 49. Tout sous-groupe du groupe multiplicatif d'un corps fini est cyclique.

Corollaire 50.

$$\mathbb{F}_q^* \cong \mathbb{Z}/(q-1)\mathbb{Z}$$

Proposition 51. Soit F un corps fini de caractéristique p et soit ξ un générateur de F^*. Alors, en posant $n = [F : \mathbb{F}_p]$, on a

$$F = \bigoplus_{i=0}^{n} \mathbb{F}_p \xi^i$$

Théorème 52 (Élément primitif pour les corps finis)**.** Soit $\mathbb{L}$ une extension de degré fini de $\mathbb{K}$. Si $\mathbb{K}$ est un corps fini, alors $\mathbb{L}$ est monogène.

Théorème 53. (i) Si $\mathbb{K}$ est un sous-corps de $\mathbb{F}_q$, alors il existe $d \mid n$ tel que $|K| = p^d$. p. 91

(ii) Pour chaque diviseur d de n, $\mathbb{F}_q$ a un et un seul sous-corps de cardinal p^d. Il est isomorphe à $\mathbb{F}_{p^d}$.

2. Corps cyclotomiques

Soit m un entier supérieur ou égal à 1.

Définition 54. On définit p. 67

$$\mu_m = \{z \in \mathbb{C}^* \mid z^m = 1\}$$

l'ensemble des **racines m-ièmes de l'unité**. C'est un groupe (cyclique) pour la multiplication dont l'ensemble des générateurs, noté μ_m^*, est formé des **racines primitives m-ièmes de l'unité**.

Proposition 55. (i) $\mu_m^* = \{e^{\frac{2ik\pi}{m}} \mid k \in [\![0, m-1]\!], \operatorname{pgcd}(k, m) = 1\}$.

(ii) $|\mu_m^*| = \varphi(m)$, où φ désigne l'indicatrice d'Euler.

Proposition 56. Le sous-corps $\mathbb{Q}(\xi)$ de $\mathbb{C}$ ne dépend pas de la racine m-ième primitive ξ de l'unité considérée.

Définition 57. On appelle **corps cyclotomique**, un corps de la forme de la Théorème 56 (ie. engendré par une racine primitive de l'unité).

Définition 58. On appelle **m-ième polynôme cyclotomique** le polynôme

$$\Phi_m = \prod_{\xi \in \mu_m^*} (X - \xi)$$

Théorème 59. (i) $X^m - 1 = \prod_{d|m} \Phi_d$.

(ii) $\Phi_m \in \mathbb{Z}[X]$.

(iii) Φ_m est irréductible sur $\mathbb{Q}$.

Corollaire 60. Le polynôme minimal sur $\mathbb{Q}$ de tout élément ξ de μ_m^* est Φ_m. En particulier,

$$[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(m)$$

Application 61 (Théorème de Wedderburn)**.** Tout corps fini est commutatif.

Application 62 (Dirichlet faible)**.** Pour tout entier n, il existe une infinité de nombres premiers congrus à 1 modulo n.

[GOU21] p. 99

127 Exemples de nombres remarquables. Exemples d'anneaux de nombres remarquables. Applications.

I - Nombres remarquables

1. Deux exemples fondamentaux : e et π

Définition 1. On définit la fonction **exponentielle complexe** pour tout $z \in \mathbb{C}$ par

$$\sum_{n=0}^{+\infty} \frac{z^n}{n!}$$

on note cette somme e^z ou parfois $\exp(z)$.

[QUE] p. 4

Remarque 2. Cette somme est bien définie pour tout $z \in \mathbb{C}$ d'après le critère de d'Alembert.

Proposition 3. (i) $\forall z, z' \in \mathbb{C}$, $e^{z+z'} = e^z e^{z'}$.

(ii) exp est holomorphe sur $\mathbb{C}$, de dérivée elle-même.

(iii) exp ne s'annule jamais.

Définition 4. On définit e le **nombre d'Euler** par $e = e^1 > 0$.

p. 383

Proposition 5. La fonction $\varphi : t \mapsto e^{it}$ est un morphisme surjectif de $\mathbb{R}$ sur $\mathbb{U}$, le groupe des nombres complexes de module 1.

p. 7

Proposition 6. En reprenant les notations précédentes, $\mathrm{Ker}(\varphi)$ est un sous-groupe fermé de $\mathbb{R}$, de la forme $\mathrm{Ker}(\varphi) = a\mathbb{Z}$. On note $a = 2\pi$.

2. Nombres algébriques, transcendants

Définition 7. Un nombre complexe (resp. réel) z est dit **nombre algébrique complexe** (resp. **nombre algébrique réel**) s'il existe $P \in \mathbb{Z}[X] \setminus \{0\}$ tel que $P(z) = 0$.

[GOZ] p. 40

Exemple 8. $\pm\sqrt{2}$ et $\pm i$ sont des nombres algébriques.

p. 40

Théorème 9 (Liouville)**.** Soit α un nombre algébrique réel, racine d'un polynôme $P \in \mathbb{Z}[X]$ de degré supérieur ou égal à 2. Alors,

$$\exists C_\alpha > 0 \text{ tel que } \forall \frac{p}{q} \in \mathbb{Q}, \left\| x - \frac{p}{q} \right\| \geq \frac{C}{q^d}$$

[QUE] p. 391

Application 10. Le nombre de Liouville,

$$\sum_{n=1}^{+\infty} \frac{1}{10^{n!}}$$

est transcendant.

Théorème 11 (Hermite)**.** e est transcendant.

[GOZ] p. 41

Théorème 12 (Lindemann)**.** π est transcendant.

Application 13. Les nombres $\zeta(2k)$ sont transcendants pour $k \in \mathbb{N}^*$.

[QUE] p. 385

II - Anneaux de nombres algébriques

Notation 14. On note $\mathbb{A}$ l'ensemble des nombres algébriques complexes. $\mathbb{A} \cap \mathbb{R}$ est alors l'ensemble des nombres algébriques réels.

[GOZ] p. 40

Théorème 15. (i) $\mathbb{A}$ est un sous-corps de $\mathbb{C}$ qui contient $\mathbb{Q}$.

(ii) $\mathbb{A} \cap \mathbb{R}$ est un sous-corps de $\mathbb{R}$ qui contient $\mathbb{Q}$.

Corollaire 16. $\mathbb{A}$ est la clôture algébrique de $\mathbb{Q}$.

p. 63

Remarque 17. Toute extension de $\mathbb{Q}$ de degré fini est alors un sous-corps de $\mathbb{A}$.

1. Corps de nombres quadratiques

Proposition 18. Soit $d \in \mathbb{N}$ tel que $d \geq 2$. Les assertions suivantes sont équivalentes. p. 33

(i) $\sqrt{d} \notin \mathbb{Q}$.

(ii) $\sqrt{d} \notin \mathbb{N}$.

(iii) Il existe p premier tel que $v_p(d)$ (la valuation p-adique de d) est impair.

(iv) $\mathbb{Q}[\sqrt{d}]$ est une extension de $\mathbb{Q}$ de degré 2.

Définition 19. On appelle **corps quadratique** toute extension de degré 2 de $\mathbb{Q}$ dans $\mathbb{C}$.

Théorème 20. Soit $\mathbb{L}$ un corps quadratique. Alors, il existe un entier relatif $d \notin \{0,1\}$, sans facteur carré tel que

$$\mathbb{L} = \mathbb{Q}[\sqrt{d}]$$

où $\sqrt{d}$ désigne un complexe dont le carré est égal à d.

Définition 21. Soit d un entier non nul qui n'est pas un carré dans $\mathbb{Z}$ et $z = x + y\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$ avec $x, y \in \mathbb{Q}$. La **norme** de z est [ULM18] p. 67

$$N(z) = x^2 - y^2 d$$

Proposition 22. Soit d un entier non nul qui n'est pas un carré dans $\mathbb{Z}$. Pour $z = x + y\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$ avec $x, y \in \mathbb{Q}$. Posons $\tilde{z} = x - y\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$.

(i) L'application $z \mapsto \tilde{z}$ est un automorphisme des anneaux $\mathbb{Q}[\sqrt{d}]$ et $\mathbb{Z}[\sqrt{d}]$. Pour tout $z \in \mathbb{Q}[\sqrt{d}]$, nous avons $\tilde{\tilde{z}} = z$ et $N(z) = z\tilde{z}$. Si $z \in \mathbb{Z}[\sqrt{d}]$, alors $N(z) \in \mathbb{Z}$.

(ii) $\mathbb{Q}[\sqrt{d}] = \mathbb{Q}[X]/(X^2 - d)$ est un corps.

(iii) Dans $\mathbb{Q}[\sqrt{d}]$ et $\mathbb{Z}[\sqrt{d}]$, nous avons $N(z_1 z_2) = N(z_1)N(z_2)$ et $N(z) = 0 \iff z = 0$.

Proposition 23. Soit d un entier non nul qui n'est pas un carré dans $\mathbb{Z}$.

(i) Les inversibles de $\mathbb{Z}[\sqrt{d}]$ avec $N(z) = \pm 1$.

(ii) Tout élément non nul, non inversible possède une décomposition en irréductibles dans $\mathbb{Z}(\sqrt{d})$.

2. Anneau des entiers de Gauss

Définition 24. L'anneau $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$ est **l'anneau des entiers de Gauss**.

Exemple 25. Pour $z = x + iy \in \mathbb{Z}[i]$, nous avons $N(z) = x^2 + y^2$ et donc les inversibles de $\mathbb{Z}[i]$ sont ± 1 et $\pm i$.

Notation 26. On note Σ l'ensemble des entiers qui sont somme de deux carrés. **[I-P]** p. 137

Remarque 27. $n \in \Sigma \iff \exists z \in \mathbb{Z}[i]$ tel que $N(z) = n$.

Lemme 28. $\mathbb{Z}[i]$ est euclidien de stathme N.

Lemme 29. Soit p un nombre premier. Si p n'est pas irréductible dans $\mathbb{Z}[i]$, alors $p \in \Sigma$.

[DEV]

Théorème 30 (Deux carrés de Fermat)**.** Soit $n \in \mathbb{N}^*$. Alors $n \in \Sigma$ si et seulement si $v_p(n)$ est pair pour tout p premier tel que $p \equiv 3 \mod 4$ (où $v_p(n)$ désigne la valuation p-adique de n).

3. Corps cyclotomiques

Soit m un entier supérieur ou égal à 1.

Définition 31. On définit

$$\mu_m = \{z \in \mathbb{C}^* \mid z^m = 1\}$$

l'ensemble des **racines m-ièmes de l'unité**. C'est un groupe (cyclique) pour la multiplication dont l'ensemble des générateurs, noté μ_m^*, est formé des **racines primitives m-ièmes de l'unité**. **[GOZ]** p. 67

Proposition 32. (i) $\mu_m^* = \{e^{\frac{2ik\pi}{m}} \mid k \in [\![0, m-1]\!], \operatorname{pgcd}(k, m) = 1\}$.

(ii) $|\mu_m^*| = \varphi(m)$, où φ désigne l'indicatrice d'Euler.

Proposition 33. Le sous-corps $\mathbb{Q}(\xi)$ de $\mathbb{C}$ ne dépend pas de la racine m-ième primitive ξ de l'unité considérée.

Définition 34. On appelle **corps cyclotomique**, un corps de la forme de la Théorème 33 (ie. engendré par une racine primitive de l'unité).

Définition 35. On appelle m**-ième polynôme cyclotomique** le polynôme

$$\Phi_m = \prod_{\xi \in \mu_m^*} (X - \xi)$$

Théorème 36. (i) $X^m - 1 = \prod_{d|m} \Phi_d$.

(ii) $\Phi_m \in \mathbb{Z}[X]$.

(iii) Φ_m est irréductible sur $\mathbb{Q}$.

Corollaire 37. Le polynôme minimal sur $\mathbb{Q}$ de tout élément ξ de μ_m^* est Φ_m. En particulier, le degré de $\mathbb{Q}(\xi)$ sur $\mathbb{Q}$ est $\varphi(m)$.

Application 38 (Théorème de Wedderburn)**.** Tout corps fini est commutatif.

Application 39 (Dirichlet faible)**.** Pour tout entier n, il existe une infinité de nombres premiers congrus à 1 modulo n. **[GOU21]** p. 99

III - Application à la constructibilité à la règle et au compas

On note $\mathscr{P}$ un plan affine euclidien muni d'un repère orthonormé direct $\mathscr{R} = (O, \vec{i}, \vec{j})$. On s'autorise à identifier chaque point $M \in \mathscr{P}$ avec ses coordonnées $(x, y) \in \mathbb{R}^2$ dans $\mathscr{R}$. **[GOZ]** p. 47

Définition 40. On dit qu'un point $M \in \mathscr{P}$ est **constructible** (sous-entendu *à la règle et au compas*) si on peut le construire en utilisant uniquement la règle et le compas, en supposant O et $I = (1, 0)$ déjà construits.

Proposition 41. Soient A, B deux points constructibles distincts.

(i) Si A est constructible, son symétrique par rapport à O l'est aussi.

(ii) $J = (0, 1)$ est constructible.

(iii) Si C est un point constructible, on peut construire à la règle et au compas la perpendiculaire à (AB) passant par C.

(iv) Si C est un point constructible, on peut construire à la règle et au compas la parallèle à (AB) passant par C.

Proposition 42. Soit $x \in \mathbb{R}$.

$$(x,0) \text{ est constructible} \iff (0,x) \text{ est constructible}$$

Définition 43. Un nombre vérifiant la proposition précédente est dit **nombre constructible**.

Proposition 44. (i) Tout élément de $\mathbb{Q}$ est constructible.

(ii) (x,y) est constructible si et seulement si x et y le sont.

Théorème 45. L'ensemble $\mathbb{E}$ des nombres constructibles est un sous-corps de $\mathbb{R}$ stable par racine carrée.

[DEV]

Théorème 46 (Wantzel)**.** Soit $t \in \mathbb{R}$. t est constructible si et seulement s'il existe une suite fini $(L_0, \dots, L_p)$ de sous-corps de $\mathbb{R}$ vérifiant :

(i) $L_0 = \mathbb{Q}$.

(ii) $\forall i \in [\![1, p-1]\!]$, L_i est une extension quadratique de L_{i-1}.

(iii) $t \in L_p$.

Corollaire 47. (i) Si x est constructible, le degré de l'extension $\mathbb{Q}[x]$ sur $\mathbb{Q}$ est de la forme 2^s pour $s \in \mathbb{N}$.

(ii) Tout nombre constructible est algébrique.

Contre-exemple 48.
— $\sqrt[3]{2}$ est algébrique, non constructible.
— $\sqrt{\pi}$ est transcendant et n'est donc pas constructible.

Application 49 (Quadrature du cercle)**.** Il est impossible de construire, à la règle et au compas, un carré ayant même aire qu'un disque donné.

Application 50 (Duplication du cube)**.** Il est impossible de construire, à la règle et au compas, l'arête d'un cube ayant un volume double de celui d'un cube donné.

141 Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

Sauf mention contraire, les corps sont supposés commutatifs.

I - Irréductibilité de polynômes

1. Racines et polynômes irréductibles

Définition 1. Soit A un anneau. Un polynôme P de $A[X]$ est dit **irréductible** si $\deg(A) \geq 1$ et ses seuls diviseurs dans $A[X]$ sont les polynômes uP où $u \in A^\times$. [GOZ] p. 8

Remarque 2. Soit $\mathbb{K}$ un corps. Alors, $\mathbb{K}[X]$ est euclidien, donc principal, donc factoriel.

Définition 3. Soient $\mathbb{L}$ un corps et $\mathbb{K}$ un sous-corps de $\mathbb{L}$. Soit $P \in \mathbb{K}[X]$.

- Une **racine** est un élément $\alpha \in \mathbb{K}$ tel que $P(\alpha) = 0$.
- La **multiplicité** de α comme racine de P est le plus grand $n \in \mathbb{N}$ tel que $(X-a)^n$ divise P dans $\mathbb{K}[X]$.
- La somme des multiplicités des racines de P dans $\mathbb{K}$ est inférieure ou égale à $\deg(P)$. En cas d'égalité, on dit que P est **scindé** *sur* $\mathbb{K}$ (ou *dans* $\mathbb{K}[X]$).

Proposition 4. (i) Tout polynôme de degré 1 est irréductible.

(ii) Tout polynôme irréductible de degré strictement supérieur à 1 n'a pas de racine dans $\mathbb{K}$.

Contre-exemple 5. $(X^2+1)^2$ n'a pas de racine dans $\mathbb{Q}$, mais est réductible dans $\mathbb{Q}[X]$.

Proposition 6. La réciproque de la Théorème 4 Point (ii) est vraie pour les polynômes de degré 2 ou 3.

Proposition 7. Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ un polynôme de degré n tel que $a_0 \neq 0$. Si $\alpha = \frac{p}{q} \in \mathbb{Q}$ est une racine de P, en supposant $\frac{p}{q}$ irréductible, alors $p \mid a_0$ et $q \mid a_n$.

Exemple 8. $X^3 + X + 1$ n'a pas de racine dans $\mathbb{Q}$. p. 19

2. Quelques critères d'irréductibilité

Soit A un anneau factoriel.

Définition 9. Pour tout polynôme non nul $P \in A[X]$, on appelle **contenu** de P, noté $\gamma(P)$, le PGCD des coefficients de P. P est dit **primitif** si $\gamma(P) = 1$. p. 10

Lemme 10 (Gauss)**.** (i) Le produit de deux polynômes primitifs est primitif.

(ii) $\forall P, Q \in A[X] \setminus \{0\}, \gamma(PQ) = \gamma(P)\gamma(Q)$.

Théorème 11. Soient $\mathbb{K}$ le corps des fractions de A et $P \in A[X]$ de degré supérieur ou égal à 1. Alors, P est irréductible dans $A[X]$ si et seulement si P est irréductible dans $\mathbb{K}[X]$ et $\gamma(P) = 1$.

[DEV]

Théorème 12 (Critère d'Eisenstein)**.** Soient $\mathbb{K}$ le corps des fractions de A et $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ de degré $n \geq 1$. On suppose qu'il existe $p \in A$ irréductible tel que :

(i) $p \mid a_i, \forall i \in [\![0, n-1]\!]$.

(ii) $p \nmid a_n$.

(iii) $p^2 \nmid a_0$.

Alors P est irréductible dans $\mathbb{K}[X]$.

Exemple 13. Soit p un nombre premier. Le polynôme $\Phi_p = \sum_{k=0}^{p-1} X^k$ est irréductible dans $\mathbb{Z}[X]$.

Application 14. Soit $n \in \mathbb{N}^*$. Il existe des polynômes irréductibles de degré n sur $\mathbb{Z}$. [PER] p. 67

Théorème 15 (Critère d'irréductibilité modulo p)**.** Soient $\mathbb{K}$ le corps des fractions de A et $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ de degré $n \geq 1$. Soit I un idéal premier de A. On pose $B = A/I$ et $\mathbb{L}$ le corps des fractions de B. On suppose $a_n \notin I$. [GOZ] p. 12

Si $\overline{P}$ est irréductible dans $\mathbb{L}[X]$, alors P est irréductible dans $\mathbb{K}[X]$.

Exemple 16. Le polynôme $X^3 - 127X^2 + 3608X + 19$ est irréductible dans $\mathbb{Z}[X]$.

II - Adjonction de racines

Soit $\mathbb{K}$ un corps commutatif.

1. Éléments algébriques, transcendants

Définition 17. Soient $\mathbb{L}$ une extension de $\mathbb{K}$ et $\alpha \in \mathbb{L}$. Soit $\mathrm{ev}_\alpha : \mathbb{K}[X] \to \mathbb{L}$ le morphisme d'évaluation en α. [PER] p. 66

- On note $\mathrm{Ann}(\alpha)$ l'idéal des polynômes annulateurs de α. Notons qu'on a $\mathrm{Ann}(\alpha) = \mathrm{Ker}(\mathrm{ev}_\alpha)$.
- Si ev_α est injectif, on dit que α est **transcendant** sur $\mathbb{K}$.
- Sinon, α est dit **algébrique** sur $\mathbb{K}$.

Exemple 18.
- e et π sont transcendants sur $\mathbb{Q}$ (théorèmes d'Hermite et de Lindemann).
- $\sqrt{2}$, i, ... sont algébriques sur $\mathbb{Q}$.

Proposition 19. Soient $\mathbb{L}$ une extension de $\mathbb{K}$ et $\alpha \in \mathbb{L}$. Les assertions suivantes sont équivalentes.

(i) α est algébrique sur $\mathbb{K}$.
(ii) $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$.
(iii) $[\mathbb{K}[\alpha] : \mathbb{K}] < +\infty$.

Proposition 20. En reprenant les notations précédentes, si α est transcendant, on a

$$\mathbb{K}[\alpha] \cong \mathbb{K}[X] \text{ et } \mathbb{K}(\alpha) \cong \mathbb{K}(X)$$

Définition 21. Soient $\mathbb{L}$ une extension de $\mathbb{K}$ et $\alpha \in \mathbb{L}$. Si α est algébrique sur $\mathbb{K}$, alors $\mathrm{Ann}(\alpha)$ est un idéal principal non nul. Donc, il existe $P \in \mathbb{K}[X]$ unitaire tel que $\mathrm{Ann}(\alpha) = (P)$. On note π_α ce polynôme P : c'est le **polynôme minimal** de α sur $\mathbb{K}$.

Exemple 22. Sur $\mathbb{Q}$, on a $\pi_{\sqrt{2}} = X^2 - 2$ et $\pi_i = X^2 + 1$.

Proposition 23. Soient $\mathbb{L}$ une extension de $\mathbb{K}$ et $\alpha \in \mathbb{L}$. Soient $P \in \mathbb{K}[X]$. Les assertions suivantes sont équivalentes : [GOZ] p. 31

(i) $P = \mu_\alpha$.
(ii) $P \in \mathrm{Ann}(\alpha)$ et est unitaire et $\forall R \in \mathrm{Ann}(\alpha) \setminus \{0\}$, $\deg(P) \leq \deg(R)$.
(iii) $P \in \mathrm{Ann}(\alpha)$ et est unitaire et irréductible dans $\mathbb{K}[X]$.

2. Corps de rupture

p. 57

Définition 24. Soient $\mathbb{L}$ une extension de $\mathbb{K}$ et $P \in \mathbb{K}[X]$ irréductible. On dit que $\mathbb{L}$ est un **corps de rupture** de P si $\mathbb{L} = \mathbb{K}[\alpha]$ où $\alpha \in \mathbb{L}$ est une racine de P.

Exemple 25. En reprenant les notations précédentes, si $\deg(P) = 1$, alors $\mathbb{K}$ est un corps de rupture de P.

Théorème 26. Soit $P \in \mathbb{K}[X]$ un polynôme irréductible sur $\mathbb{K}$.

— Il existe un corps de rupture de P.

— Si $\mathbb{L} = \mathbb{K}[\alpha]$ et $\mathbb{L}' = \mathbb{K}[\beta]$ sont deux corps de rupture de P, alors il existe un unique $\mathbb{K}$-isomorphisme $\varphi : \mathbb{L} \to \mathbb{L}'$ tel que $\varphi(\alpha) = \beta$.

Application 27. $X^2 + 1$ est un polynôme irréductible sur $\mathbb{R}$ dont $\mathbb{R}[X]/(X^2+1)$ est un corps de rupture. On pose alors $\mathbb{C} = \mathbb{R}[X]/(X^2+1)$, le corps des nombres complexes, et on note i la classe de X dans l'anneau quotient.

Remarque 28. Si $\mathbb{L}$ est un corps de rupture d'un polynôme $P \in \mathbb{K}[X]$, on a $[\mathbb{L} : \mathbb{K}] = \deg(P)$. Plus précisément, une base de $\mathbb{L}$ en tant que $\mathbb{K}$-espace vectoriel est $(1, \alpha, \dots, \alpha^{\deg(P)-1})$.

3. Corps de décomposition

Définition 29. Soit $P \in \mathbb{K}[X]$ de degré $n \geq 1$. On dit que $\mathbb{L}$ est un **corps de décomposition** de P si :

— Il existe $a \in \mathbb{L}$ et $\alpha_1, \dots, \alpha_n \in \mathbb{L}$ tels que $P = a(X - \alpha_1)\dots(X - \alpha_n)$.

— $\mathbb{L} = \mathbb{K}[\alpha_1, \dots, \alpha_n]$.

Exemple 30.
— $\mathbb{K}$ est un corps de décomposition de tout polynôme de degré 1 sur $\mathbb{K}$.

— $\mathbb{C}$ est un corps de décomposition de $X^2 + 1$ sur $\mathbb{R}$.

Théorème 31. Soit $P \in \mathbb{K}[X]$ un polynôme de degré supérieur ou égal à 1.

— Il existe un corps de décomposition de P.

— Deux corps de décomposition de P sont $\mathbb{K}$-isomorphes.

[FGN2]
p. 160

Application 32. Soit $A \in \mathcal{M}_n(\mathbb{K})$. On note $\mathcal{C}(A)$ le commutant de A. Alors,

$$\mathbb{K}[A] = \mathcal{C}(A) \iff \pi_A = \chi_A = \det(XI_n - A)$$

4. Clôture algébrique

[GOZ] p. 62

Proposition 33. Les assertions suivantes sont équivalentes :

(i) Tout polynôme de $\mathbb{K}[X]$ de degré supérieur ou égal à 1 est scindé sur $\mathbb{K}$.

(ii) Tout polynôme de $\mathbb{K}[X]$ de degré supérieur ou égal à 1 admet au moins une racine dans $\mathbb{K}$.

(iii) Les seuls polynômes irréductibles de $\mathbb{K}[X]$ sont ceux de degré 1.

(iv) Toute extension algébrique de $\mathbb{K}$ est égale à $\mathbb{K}$.

Définition 34. Si $\mathbb{K}$ vérifie un des points de la Théorème 33, $\mathbb{K}$ est dit **algébriquement clos**.

Proposition 35. Tout corps algébriquement clos est infini.

Contre-exemple 36. $\mathbb{Q}$ et même $\mathbb{R}$ ne sont pas algébriquement clos.

Théorème 37 (D'Alembert-Gauss)**.** $\mathbb{C}$ est algébriquement clos.

Définition 38. On dit que $\mathbb{L}$ est une **clôture algébrique** de $\mathbb{K}$ si $\mathbb{L}$ est une extension de $\mathbb{K}$ algébriquement close et si

$$\forall x \in \mathbb{L}, \exists P \in \mathbb{K}[X] \text{ tel que } P(x) = 0$$

Exemple 39.
— $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.
— $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ est algébrique sur } \mathbb{Q}\}$ est une clôture algébrique de $\mathbb{Q}$.

Théorème 40 (Steinitz)**.** (i) Il existe une clôture algébrique de $\mathbb{K}$.

(ii) Deux clôtures algébriques de $\mathbb{K}$ sont $\mathbb{K}$-isomorphes.

III - Polynômes cyclotomiques

Définition 41. On appelle m**-ième polynôme cyclotomique** le polynôme

$$\Phi_m = \prod_{\xi \in \mu_m^*} (X - \xi)$$

Théorème 42. (i) $X^m - 1 = \prod_{d|m} \Phi_d$.

(ii) $\Phi_m \in \mathbb{Z}[X]$.

(iii) Φ_m est irréductible sur $\mathbb{Q}$.

Corollaire 43. Le polynôme minimal sur $\mathbb{Q}$ de tout élément ξ de μ_m^* est Φ_m. En particulier,

$$[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(m)$$

Application 44 (Théorème de Wedderburn)**.** Tout corps fini est commutatif.

Lemme 45. Soient $a \in \mathbb{N}$ et p premier tels que $p \mid \Phi_n(a)$ mais $p \nmid \Phi_d(a)$ pour tout diviseur strict d de n. Alors $p \equiv 1 \mod n$. [GOU21] p. 99

[DEV] **Application 46** (Dirichlet faible)**.** Pour tout entier n, il existe une infinité de nombres premiers congrus à 1 modulo n.

IV - Polynômes irréductibles sur $\mathbb{F}_q$

Soient p un nombre premier et $n \in \mathbb{N}^*$. On pose $q = p^n$. [GOZ] p. 87

Théorème 47.

$$\mathbb{F}_q = \mathbb{F}_p[X]/(P)$$

où $P \in \mathbb{F}_p[X]$ est un polynôme irréductible de degré n sur $\mathbb{F}_p$.

Corollaire 48. (i) Il existe des polynômes irréductibles de tout degré dans $\mathbb{F}_p[X]$.

(ii) Si $P \in \mathbb{F}_p[X]$ est un polynôme irréductible sur $\mathbb{F}_p$ de degré n, alors P divise $X^q - X$. En particulier, il est scindé sur $\mathbb{F}_q$. Donc son corps de rupture $\mathbb{F}_q = \mathbb{F}_p[X]/(P)$ est aussi son corps de décomposition.

Théorème 49. Pour tout $j \in \mathbb{N}^*$, on note $I(p,q)$ l'ensemble des polynômes irréductibles unitaires de degré j sur $\mathbb{F}_p$. Alors,

$$X^q - X = \prod_{d|n} \prod_{Q \in I(p,q)} Q$$

Corollaire 50.

$$q = \sum_{d|n} d|I(p,d)|$$

Définition 51. On définit la **fonction de Möbius**, notée μ, par

$$\mu : \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z} \\ n & \mapsto & \begin{cases} 1 & \text{si } n = 1 \\ (-1)^k & \text{si } n = p_1 \dots p_k \text{ avec } p_1, \dots, p_k \text{ premiers distincts} \\ 0 & \text{sinon} \end{cases} \end{array}$$

Théorème 52 (Formule d'inversion de Möbius)**.** Soient f et g des fonctions de $\mathbb{N}^*$ dans $\mathbb{C}$ telles que $\forall n \in \mathbb{N}^*, f(n) = \sum_{d|n} g(d)$. Alors,

$$\forall n \in \mathbb{N}^*, g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$$

Corollaire 53.

$$\forall n \in \mathbb{N}^*, |I(p,q)| = \frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}} = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d$$

142 PGCD et PPCM, algorithmes de calcul. Applications.

I - Notion de PGCM/PPCM dans un anneau

Soit A un anneau commutatif unitaire.

Définition 1. Soient $a, b \in A$. [ULM18] p. 39

— On dit que a **divise** b (ou que b est un multiple de a), noté $a \mid b$ s'il existe $c \in A$ tel que $b = ac$.

— On dit que a et b sont **associés**, noté $a \sim b$ si $a \mid b$ et si $b \mid a$.

Remarque 2. Soient $a, b \in A$.

— $a \mid b \iff (b) \subseteq (a)$.

— $a \sim b \iff (b) = (a)$. Ainsi, $\sim$ est une relation d'équivalence sur A.

Proposition 3. Soient $a, b \in A$. Alors,

$$a \sim b \iff \exists u \in A^\times \text{ tel que } b = ua$$

Définition 4. Soient $a_1, \dots, a_n \in A^*$.

— $d \in A$ est un **plus grand commun diviseur** "PGCD" de $a_1, \dots, a_m$ si d satisfait les deux propriétés suivantes :

(i) $d \mid a_i, \forall i \in [\![1, n]\!]$.

(ii) Si $\exists d' \in A$ tel que $d' \mid a_i, \forall i \in [\![1, n]\!]$, alors $d' \mid d$.

— $m \in A$ est un **plus petit commun multiple** "PPCM" de $a_1, \dots, a_n$ si m satisfait les deux propriétés suivantes :

(i) $a_i \mid m, \forall i \in [\![1, n]\!]$.

(ii) Si $\exists m' \in A$ tel que $a_i \mid m', \forall i \in [\![1, n]\!]$, alors $m \mid m'$.

Remarque 5. Un PGCD (resp. un PPCM), lorsqu'il existe, n'est pas toujours unique. Dans un anneau intègre, deux PGCD (resp. PPCM) sont toujours associés puisqu'ils se divisent l'un l'autre. Dans un anneau intègre, on peut donc noter $d \sim \text{pgcd}(a, b)$ (resp. $m \sim \text{pgcd}(a, b)$) lorsque d est un pgcd (resp. m est un ppcm) de a et de b.

Exemple 6. Soient $\mathbb{K}$ un corps commutatif. On pose $P_n = X^n - 1 \in \mathbb{K}[X]$ pour $n \in \mathbb{N}^*$. Alors, pour $a, b \in \mathbb{N}^*$, le PGCD unitaire de P_a et P_b est égal à $P_{\text{pgcd}(a,b)}$. [GOU21] p. 60

Proposition 7. Soient $a, b \in A^*$. Un élément $c \in A$ est un PPCM de a et b si et seulement si $(a) \cap (b) = (c)$. En particulier, a et b admettent un PPCM si et seulement si $(a) \cap (b)$ est un idéal principal. [ULM18] p. 40

Proposition 8. Soient $a, b \in A^*$. Soit $d \in A$. Les assertions suivantes sont équivalentes.

(i) $d \mid a$, $d \mid b$ et il existe $u, v \in A$ tels que $d = au + bv$.

(ii) $d \sim \text{pgcd}(a, b)$ et il existe $u, v \in A$ tels que $d = au + bv$.

(iii) $(d) = (a, b)$.

Définition 9. Deux éléments a et b de A sont dits **premiers entre eux** s'ils admettent un PGCD et $\text{pgcd}(a, b) \sim 1$.

Exemple 10. 2 et X sont premiers entre eux dans $\mathbb{Z}[X]$.

II - Dans un anneau principal

Dans cette section, A désigne toujours un anneau commutatif unitaire. On le suppose de plus principal.

1. Existence

Théorème 11 (Décomposition de Bézout)**.** Soient $a_1, \dots, a_n \in A^*$. Alors :

(i) Il existe d un pgcd de $a_1, \dots, a_n$. d est tel que $(d) = (a_1, \dots, a_n)$. En particulier, d est de la forme $d = b_1 a_1 + \cdots + b_n a_n$ avec $\forall i \in [\![1, n]\!]$, $b_i \in A$.

(ii) Il existe m un ppcm de $a_1, \dots, a_n$. m est tel que $(m) = (a_1) \cap \cdots \cap (a_n)$.

Exemple 12. Dans $\mathbb{F}_2[X]$: p. 52

$$-X(X^3 + X^2 + 1) + (1 + X^2)(X^2 + X + 1) = 1$$

Application 13. $\overline{X}^2 + 1$ est inversible dans $\mathbb{F}_2[X]/(X^3 + X^2 + 1)$ d'inverse $\overline{X}^2 + X + 1$.

Lemme 14 (Gauss)**.** Soient $a, b, c \in A$ avec a et b premiers entre eux. Alors, p. 42

$$a \mid bc \implies a \mid c$$

et

$$a \mid c \text{ et } b \mid c \implies ab \mid c$$

2. Dans les anneaux euclidiens

a. Principalité des anneaux euclidiens

Proposition 15. Un anneau euclidien est principal.

On a donc existence de PGCD et de PPCM dans un tel anneau, mais la structure euclidienne permet de plus de fournir des algorithmes de calculs.

Théorème 16. Si $\mathbb{K}$ est un corps commutatif, alors $\mathbb{K}[X]$ est un anneau euclidien de stathme le degré. De plus, le quotient et le reste sont uniques.

p. 47

Corollaire 17. Les assertions suivantes sont équivalentes :

(i) A est un corps commutatif.

(ii) $A[X]$ est un anneau euclidien.

(iii) $A[X]$ est un anneau principal.

b. Algorithmes de calcul

Lemme 18. On suppose A euclidien de stathme ν. Soient $a, b \in A^*$ et r un reste dans la division euclidienne de a par b. À inversible près, on a alors :

— Si $r = 0$: $\text{pgcd}(a, b) = b$.

— Sinon : $\text{pgcd}(a, b) = \text{pgcd}(b, r)$.

[ROM21] p. 264

Théorème 19 (Algorithme d'Euclide)**.** On suppose A euclidien de stathme ν. Soient $a, b \in A^*$ tels que $\nu(a) \geq \nu(b)$. On définit une suite (r_k) décroissante (au sens du stathme) par :

— $r_k = b$;

— r_1 est un reste dans la division euclidienne de a par b, on a donc $r_1 = 0$ ou $0 \leq \nu(r_1) < \nu(r_0)$;

— pour $k \geq 2$, si $r_{k-1} = 0$, alors $r_k = 0$, sinon r_k est un reste dans la division euclidienne de r_{k-2} par r_{k-1} et on a $r_k = 0$ ou $0 \leq \nu(r_k) < \nu(r_{k-1})$.

$\text{pgcd}(a, b)$ est alors le dernier reste non nul dans cette suite de divisions euclidiennes, que l'on note r_{n-1}.

Remarque 20. On peut “remonter” l’algorithme d’Euclide pour obtenir les coefficients de Bézout. On parle alors d’algorithme d’Euclide “étendu”.

Au lieu de faire les calculs en deux temps (descente, puis remontée), on peut tout faire en même temps via l’algorithme suivant. **[ULM18]** p. 44

Proposition 21 (Algorithme d’Euclide généralisé)**.** En reprenant les notations du Théorème 19 :

- Étape 0 : On écrit $r_0 = a = u_0 \times a + v_0 \times b$ avec $(u_0, v_0) = (1,0)$.
- Étape 1 : On écrit $r_1 = b = u_1 \times a + v_1 \times b$ avec $(u_1, v_1) = (0,1)$.
- Étape 2 : On écrit $r_0 - q_1 r_1 = r_2 = u_2 \times a + v_2 \times b$ avec $(u_2, v_2) = (1, -q_1)$.
- …
- Étape k : On écrit $r_{k-1} - q_k r_k = r_{k+1} = u_{k+1} \times a + v_{k+1} \times b$.
- …
- Étape $n-1$: On écrit $r_{n-2} - q_{n-1} r_{n-1} = r_n = u_n \times a + v_n \times b$.
- Étape n : On écrit $r_{n-1} - q_n r_n = 0 = u_{n+1} \times a + v_{n+1} \times b$.

À la fin, on obtient $\text{pgcd}(a,b) = r_n = u_n a + v_n b$.

Exemple 22. Calculons le PGCD et les coefficients de Bézout de 1763 et 731 dans $\mathbb{Z}$.

				1763	=	1	×	1763	+	0	×	731
				731	=	0	×	1763	+	1	×	731
Il y va	2	fois	reste	301	=	1	×	1763	+	(-2)	×	731
	2	fois	reste	129	=	(-2)	×	1763	+	5	×	731
	2	fois	reste	43	=	5	×	1763	+	(-12)	×	731
	3	fois	reste	0	=	(-17)	×	1763	+	41	×	731

On a $\text{pgcd}(1763, 731) = 43 = 5 \times 1763 - 12 \times 731$.

[FFN] p. 23

Proposition 23. En reprenant les notations précédentes, on a

$$\forall k \in [\![0, n-1]\!],\ r_k \geq \left(\frac{1+\sqrt{5}}{2}\right)^{n-k}$$

Corollaire 24. En reprenant les notations précédentes, cet algorithme a une complexité en $O(\ln(a) \times \ln(b))$.

3. Dans un anneau factoriel

Proposition 25. Si A vérifie la relation $(*)$ de la Théorème 26, alors les assertions suivantes sont équivalentes : [PER] p. 48

(i) A vérifie le lemme d'Euclide : si $p \in A$ est irréductible, alors $p \mid ab \implies p \mid a$ ou $p \mid b$.

(ii) Pour tout $p \in A$, p est irréductible si et seulement si (p) premier.

(iii) A vérifie le lemme de Gauss : si $p \in A$ est irréductible, alors $a \mid bc \implies a \mid c$ pour tout $a, b, c \in A$ avec a et b premiers entre eux.

Proposition 26. On suppose A factoriel. Tout élément $a \neq 0$ peut s'écrire de manière unique [ULM18] p. 65

$$a = u_a \prod_{p \in \mathcal{S}} p^{v_p(a)} \qquad (*)$$

où $\mathcal{S}$ est un **système de représentants d'éléments premiers** de A (pour la relation $\sim$), u_a est inversible et $v_p(a) \in \mathbb{N}$ tous nuls sauf un nombre fini.

Exemple 27. Dans l'anneau principal (donc factoriel, voir Théorème 29) $\mathbb{Z}$, un choix standard pour $\mathcal{S}$ est l'ensemble des nombres premiers positifs.

Proposition 28. On suppose A factoriel. Soient $a, b \in A^*$. Alors, en reprenant les notations précédentes :

(i) $a \mid b \iff v_p(a) \leq v_p(b)$ pour tout $p \in \mathcal{S}$.

(ii) $\prod_{p \in \mathcal{S}} p^{\min(v_p(a), v_p(b))}$ est un PGCD de a et de b.

(iii) $\prod_{p \in \mathcal{S}} p^{\max(v_p(a), v_p(b))}$ est un PPCM de a et de b.

Théorème 29. Tout anneau principal est factoriel.

Contre-exemple 30. $\mathbb{Z}[i\sqrt{5}]$ est principal mais n'est pas factoriel.

Lemme 31 (Gauss)**.** On suppose A factoriel. Alors :

(i) Le produit de deux polynômes primitifs est primitif (ie. dont le PGCD des coefficients est associé à 1).

(ii) $\forall P, Q \in A[X] \setminus \{0\}$, $\gamma(PQ) = \gamma(P)\gamma(Q)$ (où $\gamma(P)$ est le contenu du polynôme P).

[GOZ] p. 10

[DEV]

Théorème 32 (Critère d'Eisenstein)**.** Soient $\mathbb{K}$ le corps des fractions de A et $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ de degré $n \geq 1$. On suppose que A est factoriel et qu'il existe $p \in A$ irréductible tel que :

(i) $p \mid a_i$, $\forall i \in [\![0, n-1]\!]$.

(ii) $p \nmid a_n$.

(iii) $p^2 \nmid a_0$.

Alors P est irréductible dans $\mathbb{K}[X]$.

Application 33. Soit $n \in \mathbb{N}^*$. Il existe des polynômes irréductibles de degré n sur $\mathbb{Z}$.

[PER] p. 67

III - Applications

1. En algèbre linéaire

Soit E un espace vectoriel de dimension finie n sur un corps $\mathbb{K}$. Soit $f : E \to E$ un endomorphisme de E.

Proposition 34. Il existe un unique polynôme de $\mathbb{K}[X]$ unitaire qui engendre l'idéal $\{P \in \mathbb{K}[X] \mid P(f) = 0\}$: c'est le **polynôme minimal** de f, noté π_f. Il s'agit du polynôme unitaire de plus bas degré annulant f. Il divise tous les autres polynômes annulateurs de f.

[GOU21] p. 186

Théorème 35 (Lemme des noyaux)**.** Soit $P = P_1 \dots P_k \in \mathbb{K}[X]$ où les polynômes $P_1, \dots, P_k$ sont premiers entre eux deux à deux. Alors,

$$\mathrm{Ker}(P(f)) = \bigoplus_{i=1}^{k} \mathrm{Ker}(P_i(f))$$

Application 36. f est diagonalisable si et seulement si π_f est scindé à racines simples.

2. Systèmes de congruences

Proposition 37. Soit a un entier non nul. L'équation

$$ax \equiv 1 \mod n$$

admet des solutions si et seulement si $\text{pgcd}(a,n) = 1$.

[ROM21] p. 289

Corollaire 38. Soient a un entier non nul et b un entier relatif. L'équation

$$ax \equiv b \mod n$$

a des solutions si et seulement si $d = \text{pgcd}(a,n) \mid b$. Dans ce cas, l'ensemble des solutions est

$$\left\{ \frac{b}{d}x_0 + k\frac{n}{d} \mid k \in \mathbb{Z} \right\}$$

où x_0 est une solution de l'équation $\frac{a}{n}x \equiv 1 \mod n$.

[DEV]

Théorème 39 (Chinois)**.** Soient $n_1, \dots, n_r \geq 2$ des entiers. On note $n = \prod_{i=1}^r n_i$ et $\pi_k = \pi_{n_k\mathbb{Z}}$ la surjection canonique de $\mathbb{Z}$ sur $\mathbb{Z}/k\mathbb{Z}$ pour tout $k \in [\![1,r]\!]$.

Les entiers $n_1, \dots, n_r$ sont premiers entre eux si et seulement si les anneaux $\mathbb{Z}/n\mathbb{Z}$ et $\prod_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}$ sont isomorphes. Dans ce cas, l'isomorphisme est explicité par l'application

$$\psi : \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \to & \prod_{i=1}^r \mathbb{Z}/n_i\mathbb{Z} \\ \pi_n k & \mapsto & (\pi_i(k))_{i\in[\![1,r]\!]} \end{array}$$

p. 285

Exemple 40.

$$\begin{cases} k \equiv 2 \mod 4 \\ k \equiv 3 \mod 5 \\ k \equiv 1 \mod 9 \end{cases}$$

admet pour ensemble de solutions $\{838 + 180q \mid q \in \mathbb{Z}\}$.

p. 291

144 Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.

Soient $\mathbb{K}$ un corps commutatif et $\mathscr{A}$ une algèbre sur $\mathbb{K}$. À tout polynôme $P = \sum_{i=0}^{n} a_i X^i$ de $\mathscr{K}[X]$, on associe l'application

$$\widetilde{P} : \begin{array}{ccc} \mathscr{A} & \to & \mathscr{A} \\ x & \mapsto & \sum_{i=0}^{n} a_i x^i \end{array}$$

L'application $P \mapsto \widetilde{P}$ est un morphisme d'algèbres. On notera abusivement $P = \widetilde{P}$ par la suite s'il n'y a pas d'ambiguïté.

I - Polynômes

1. Racines

Soit $P \in \mathbb{K}[X]$.

[GOU21] p. 63

Définition 1. Soit $\mathbb{L}$ une extension de $\mathbb{K}$ (cf. Section II). On dit que $a \in \mathbb{L}$ est une **racine** de P si $P(a) = 0$.

Proposition 2. $a \in \mathbb{K}$ est racine de P si et seulement si $X - a \mid P$.

Application 3 (Polynômes d'interpolation de Lagrange)**.** Soient $a_1, \dots, a_n \in \mathbb{K}$ deux à deux distincts et $b_1, \dots b_n \in \mathbb{K}$. Alors

$$\exists! L \in \mathbb{K}[X] \text{ tel que } \forall i \in [\![1, n]\!],\ L(a_i) = b_i$$

Définition 4. Soient $a \in \mathbb{K}$ et $h \in \mathbb{N}^*$. On dit que a est **racine de P d'ordre** h si $(X-a)^h \mid P$ mais $(X-a)^{h+1} \nmid P$.

Proposition 5. Soient $a_1, \dots, a_r \in \mathbb{K}$ des racines de P distinctes deux à deux et d'ordre $h_1, \dots, h_r$. Alors, $\exists Q \in \mathbb{K}[X]$ tel que

$$P = (X-a_1)^{h_1} \dots (X-a_r)^{h_r} Q(X) \quad \text{et} \quad Q(a_i) \neq 0 \ \forall i \in [\![1, n]\!]$$

Corollaire 6. Si $P \in \mathbb{K}[X]$ est de degré $n \geq 1$, alors P a au plus n racines (comptées avec leur ordre de multiplicité).

Contre-exemple 7. C'est faux en général dans un anneau. Par exemple, si $P = \overline{4}X \in \mathbb{Z}/8\mathbb{Z}[X]$, alors P a trois racines : $\overline{0}$, $\overline{1}$ et $\overline{4}$, mais $\deg(P) = 1$.

Proposition 8. Si $\mathbb{K}$ est infini et $P(x) = 0$ pour tout $x \in \mathbb{K}$, alors $P = 0$.

Contre-exemple 9. Si $\mathbb{K} = \{a_1, \dots, a_n\}$, le polynôme $(X - a_1) \dots (X - a_n)$ est non nul, mais son évaluation en tout élément de $\mathbb{K}$ vaut 0.

Définition 10. P est dit **scindé sur** $\mathbb{K}$ si on peut écrire

$$P = \lambda(X - a_1)^{h_1} \dots (X - a_r)^{h_r}$$

avec $\lambda \in \mathbb{K}$ et pour tout $i \in [\![1, n]\!]$, $a_i \in \mathbb{K}$ et $h_i \in \mathbb{N}^*$.

Définition 11. On appelle **polynôme dérivé** de P le polynôme

$$P' = a_1 + 2a_2X + \cdots + na_nX^{n-1}$$

Remarque 12. L'application $P \to P'$ est linéaire, et les règles de dérivation coïncident avec les règles usuelles.

Théorème 13 (Formule de Taylor)**.** On suppose $\mathbb{K}$ de caractéristique nulle. Alors tout polynôme F de degré inférieur ou égal à n vérifie

$$\forall a \in \mathbb{K}, F(X) = \sum_{i=0}^{n} \frac{(X-a)^i}{i!} F^{(i)}(a)$$

Corollaire 14. On suppose $\mathbb{K}$ de caractéristique nulle et $P \neq 0$. Alors $a \in \mathbb{K}$ est racine d'ordre h de P si et seulement si

$$\forall i \in [\![1, h-1]\!], P^{(i)}(a) = 0 \quad \text{et} \quad P^{(h)}(a) \neq 0$$

Exemple 15. Le polynôme $P_n = \sum_{i=0}^{n} \frac{1}{i!} X^i$ n'a que des racines simples dans $\mathbb{C}$.

Remarque 16. C'est encore vrai en caractéristique non nulle pour $h = 1$.

2. Polynômes symétriques

Soit A un anneau commutatif unitaire.

Définition 17. Soit $P \in A[X_1,\dots,X_n]$. On dit que P est **symétrique** si

$$\forall \sigma \in S_n,\ P(X_{\sigma(1)},\dots,X_{\sigma(n)}) = P(X_1,\dots,X_n)$$

p. 83

Exemple 18. Dans $\mathbb{R}[X]$, le polynôme $XY+YZ+ZX$ est symétrique.

Définition 19. On appelle **polynômes symétriques élémentaires** de $A[X_1,\dots,X_n]$ les polynômes noté Σ_p où $p \in [\![1,n]\!]$ définis par

$$\Sigma_p = \sum_{1\le i_1<\cdots<i_p\le n} X_{i_1}\dots X_{i_p}$$

Exemple 20.
- $\Sigma_1 = X_1+\cdots+X_n$.
- $\Sigma_2 = \sum_{1\le i<j\le n} X_iX_j$.
- $\Sigma_n = X_1\dots X_n$.

Remarque 21. Si $P \in A[X_1,\dots,X_n]$, alors $P(\Sigma_1(X_1,\dots,X_n),\dots,\Sigma_n(X_1,\dots,X_n))$ est symétrique. Et la réciproque est vraie.

Théorème 22 (Théorème fondamental des polynômes symétriques)**.** Soit $P \in A[X_1,\dots,X_n]$ un polynôme symétrique. Alors,

$$\exists ! \Phi \in A[X_1,\dots,X_n] \text{ tel que } \Phi(\Sigma_1,\dots,\Sigma_n)$$

Exemple 23. $P = X^3+Y^3+Z^3$ s'écrit $P = \Sigma_1^3 - 3\Sigma_1\Sigma_2 + 3\Sigma_3$.

Application 24 (Relations coefficients - racines)**.** Soit $P = a_0X^n+\cdots+a_n \in \mathbb{K}[X]$ avec $a_0 \neq 0$ scindé sur $\mathbb{K}$, dont les racines (comptées avec leur ordre de multiplicité) sont $x_1,\dots,x_n$. Alors

$$\forall p \in [\![1,n]\!],\ \Sigma_p(x_1,\dots,x_n) = (-1)^p\frac{a_p}{a_0}$$

p. 64

En particulier,
- $\Sigma_1(x_1,\dots,x_n) = \sum_{i=1}^n x_i = -\frac{a_1}{a_0}$.
- $\Sigma_n(x_1,\dots,x_n) = \prod_{i=1}^n x_i = (-1)^n\frac{a_n}{a_0}$.

[DEV]

Application 25 (Théorème de Kronecker)**.** Soit $P \in \mathbb{Z}[X]$ unitaire tel que toutes ses racines complexes appartiennent au disque unité épointé en l'origine (que l'on note D). Alors toutes ses racines sont des racines de l'unité.

[I-P] p. 279

Corollaire 26. Soit $P \in \mathbb{Z}[X]$ unitaire et irréductible sur $\mathbb{Q}$ tel que toutes ses racines complexes soient de module inférieur ou égal à 1. Alors $P = X$ ou P est un polynôme cyclotomique.

Définition 27. On appelle **identités de Newton** les polynômes

$$S_p = \sum_{i=1}^{n} X_i^p \in \mathbb{R}[X]$$

[GOU21] p. 86

Proposition 28.
— $\forall k \in [\![1, n-1]\!], S_k = (-1)^{k+1} k\Sigma_k + \sum_{i=1}^{k-1} (-1)^{i+1} \Sigma_i S_{n-k+i}$.
— $\forall p \in \mathbb{N}, S_{p+n} = \sum_{i=1}^{n} \Sigma_i S_{p+n-i}$.

[DEV]

Application 29 (Formes de Hankel)**.** On suppose $\mathbb{K} = \mathbb{R}$ et on note $x_1, \dots, x_t$ les racines complexes de P de multiplicités respectives $m_1, \dots, m_t$. On pose

$$s_0 = n \text{ et } \forall k \geq 1,\ s_k = \sum_{i=1}^{t} m_i x_i^k$$

Alors :

(i) $\sigma = \sum_{i,j \in [\![0,n-1]\!]} s_{i+j} X_i X_j$ définit une forme quadratique sur $\mathbb{C}^n$ ainsi qu'une forme quadratique $\sigma_{\mathbb{R}}$ sur $\mathbb{R}^n$.

(ii) Si on note (p, q) la signature de $\sigma_{\mathbb{R}}$, on a :
— $t = p + q$.
— Le nombre de racines réelles distinctes de P est $p - q$.

[C-G] p. 356

II - Adjonction de racines

Définition 30. On appelle **extension** de $\mathbb{K}$ tout corps $\mathbb{L}$ tel qu'il existe un morphisme de corps de $\mathbb{K}$ dans $\mathbb{L}$. On notera $\mathbb{L}/\mathbb{K}$ pour signifier que $\mathbb{L}$ est une extension de $\mathbb{K}$ par la suite.

[GOZ] p. 21

Remarque 31.
— Si $\mathbb{K}$ est un sous-corps de $\mathbb{L}$, alors $\mathbb{L}$ est une extension de $\mathbb{K}$.
— Un morphisme de corps est forcément injectif, donc on peut identifier $\mathbb{K}$ à son image

et dire que $\mathbb{K} \subseteq \mathbb{L}$ de manière abusive.

Exemple 32. $\mathbb{C}$ est une extension de $\mathbb{R}$.

L'idée dans la suite va être de chercher comment "rajouter" des racines à des polynômes pourtant irréductibles sur un corps.

1. Corps de rupture

Définition 33. Soient $\mathbb{L}$ une extension de $\mathbb{K}$ et $P \in \mathbb{K}[X]$ irréductible. On dit que $\mathbb{L}$ est un **corps de rupture** de P si $\mathbb{L} = \mathbb{K}[\alpha]$ où $\alpha \in \mathbb{L}$ est une racine de P. p. 57

Exemple 34.
- Avec les notations précédentes, si $\deg(P) = 1$, $\mathbb{K}$ est un corps de rupture de P.
- $\mathbb{C}$ est un corps de rupture de $X^2 + 1$ sur $\mathbb{R}$.
- $\mathbb{F}_4$ est un corps de rupture de $X^2 + X + 1$ sur $\mathbb{F}_2$.

Théorème 35. Soit $P \in \mathbb{K}[X]$ un polynôme irréductible sur $\mathbb{K}$.
- Il existe un corps de rupture de P.
- Si $\mathbb{L} = \mathbb{K}[\alpha]$ et $\mathbb{L}' = \mathbb{K}[\beta]$ sont deux corps de rupture de P, alors il existe un unique $\mathbb{K}$-isomorphisme $\varphi : \mathbb{L} \to \mathbb{L}'$ tel que $\varphi(\alpha) = \beta$.

2. Corps de décomposition

Définition 36. Soit $P \in \mathbb{K}[X]$ de degré $n \geq 1$. On dit que $\mathbb{L}$ est un **corps de décomposition** de P si :
- Il existe $a \in \mathbb{L}$ et $\alpha_1, \dots, \alpha_n \in \mathbb{L}$ tels que $P = a(X - \alpha_1) \dots (X - \alpha_n)$.
- $\mathbb{L} = \mathbb{K}[\alpha_1, \dots, \alpha_n]$.

Exemple 37.
- $\mathbb{K}$ est un corps de décomposition de tout polynôme de degré 1 sur $\mathbb{K}$.
- $\mathbb{C}$ est un corps de décomposition de $X^2 + 1$ sur $\mathbb{R}$.
- Soit $\xi \in \mu_n^*$, alors $\mathbb{Q}[\xi]$ est un corps de décomposition de Φ_n (le n-ième polynôme cyclotomique) sur $\mathbb{Q}$.

Théorème 38. Soit $P \in \mathbb{K}[X]$ un polynôme de degré supérieur ou égal à 1.
- Il existe un corps de décomposition de P.

— Deux corps de décomposition de P sont $\mathbb{K}$-isomorphes.

3. Clôture algébrique

Définition 39. $\mathbb{K}$ est **algébriquement clos** si tout polynôme de $\mathbb{K}[X]$ de degré supérieur ou égal à 1 admet au moins une racine dans $\mathbb{K}$.

Exemple 40. — $\mathbb{Q}$ n'est pas algébriquement clos.
— $\mathbb{R}$ non plus.

Proposition 41. Tout corps algébriquement clos est infini.

Théorème 42 (D'Alembert-Gauss)**.** $\mathbb{C}$ est algébriquement clos.

Définition 43. On dit que $\mathbb{L}$ est une **clôture algébrique** de $\mathbb{K}$ si $\mathbb{L}$ est une extension de $\mathbb{K}$ algébriquement close et si

$$\forall x \in \mathbb{L}, \exists P \in \mathbb{K}[X] \text{ tel que } P(x) = 0$$

Exemple 44. — $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.
— $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \exists P \in \mathbb{Q}[X] \setminus \{0\} \text{ tel que } P(\alpha) = 0\}$ est une clôture algébrique de $\mathbb{Q}$.

Théorème 45 (Steinitz)**.** (i) Il existe une clôture algébrique de $\mathbb{K}$.
(ii) Deux clôtures algébriques de $\mathbb{K}$ sont $\mathbb{K}$-isomorphes.

III - Application en algèbre linéaire

Définition 46. Soit $A \in \mathcal{M}_n(\mathbb{K})$. On appelle : [GOU21] p. 171
— **Polynôme caractéristique** de A le polynôme $\chi_A = \det(A - XI_n)$.
— **Polynôme minimal** de A l'unique polynôme unitaire π_A qui engendre l'idéal $\mathrm{Ann}(A) = \{Q \in \mathbb{K}[X] \mid Q(A) = 0\}$. p. 186

Proposition 47. p. 172

$$\lambda \text{ est valeur propre de } A \iff \chi_A(\lambda) = 0 \iff \pi_A(\lambda) = 0$$

Proposition 48. — A est trigonalisable si et seulement si χ_A est scindé sur $\mathbb{K}$.
— A est diagonalisable si et seulement si π_A est scindé à racines simples sur $\mathbb{K}$.

p. 185

Corollaire 49. Si $\mathbb{K} = \mathbb{F}_q$, A est diagonalisable si et seulement si $A^q = A$.

148 Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.

Soit E un espace vectoriel sur un corps commutatif $\mathbb{K}$.

I - Espaces vectoriels de dimension finie

1. Familles génératrices, familles libres

Définition 1. Soit $A \subseteq E$. [GOU21] p. 117

- On dit que A est une **partie génératrice** de E si $E = \text{Vect}(A)$.
- On dit que A est une **partie libre** de E si

$$\forall (a_i)_{i\in I} \subseteq A, \forall (\lambda_i)_{i\in I} \subseteq \mathbb{K}, \sum_{i\in I} \lambda_i a_i = 0 \implies \forall i \in I, \lambda_i = 0$$

  (ou de manière équivalente, si aucun vecteur de A n'est combinaison linéaire des autres).
- On dit que A est une **partie liée** de E si A n'est pas libre.

Exemple 2. Dans le $\mathbb{R}$-espace vectoriel des fonctions réelles continues, les familles suivantes sont libres :

- (f_λ) où $\forall \lambda \in \mathbb{R}, f_\lambda : x \mapsto e^{\lambda x}$.
- (g_λ) où $\forall \lambda \in \mathbb{R}, g_\lambda : x \mapsto \cos(\lambda x)$.
- (h_λ) où $\forall \lambda \in \mathbb{R}, h_\lambda : x \mapsto |x - \lambda|$.

Proposition 3 (Polynômes à degrés échelonnés)**.** Une famille de polynômes non nuls de $\mathbb{K}_n[X] = \{P \in \mathbb{K}[X] \mid \deg(P) \leq n\}$ échelonnée en degré est libre dans $\mathbb{K}_n[X]$. [ROM21] p. 357

Application 4 (Théorème des extrema liés)**.** Soit U un ouvert de $\mathbb{R}^n$ et soient $f, g_1, \dots, g_r : U \to \mathbb{R}$ des fonctions de classe $\mathscr{C}^1$. On note $\Gamma = \{x \in U \mid g_1(x) = \cdots = g_r(x) = 0\}$. Si $f_{|\Gamma}$ admet un extremum relatif en $a \in \Gamma$ et si les formes linéaires $\mathrm{d}(g_1)_a, \dots, \mathrm{d}(g_r)_a$ sont linéairement indépendantes, alors il existe des uniques $\lambda_1, \dots, \lambda_r$ appelés **multiplicateurs de Lagrange** tels que [GOU20] p. 337

$$\mathrm{d}f_a = \lambda_1 \mathrm{d}(g_1)_a + \cdots + \lambda_r \mathrm{d}(g_r)_a$$

[GOU21] p. 117

Définition 5. On dit que E est de **dimension finie** s'il existe une partie génératrice finie de E. Dans le cas contraire, E est dit de **dimension infinie**.

2. Bases

Définition 6. Une partie libre et génératrice de E est une **base** de E.

Exemple 7.
— La famille $(e_i)_{i\in[\![1,n]\!]}$ (où $e_i = (0,\dots,0,1,0,\dots 0)$, le 1 se trouvant à la i-ième position) est une base de $\mathbb{K}^n$ appelée **base canonique** de $\mathbb{K}^n$.
— La famille $(X^i)_{i\in\mathbb{N}}$ est une base de $\mathbb{K}[X]$ appelée **base canonique** de $\mathbb{K}[X]$.

Proposition 8. Plus généralement, toute famille de polynômes non nuls de $\mathbb{K}_n[X]$ échelonnée en degré est une base de $\mathbb{K}_n[X]$. **[ROM21]** p. 257

Proposition 9. Soit $B = (e_i)_{i\in I}$ une base de E. Alors, tout vecteur x de E s'écrit de manière unique $x = \sum_{i\in I} x_i e_i$ avec $\forall i \in I$, $x_i \in E$. Les x_i sont les **coordonnées** de x dans la base B. **[GOU21]** p. 117

Théorème 10. On suppose E de dimension finie. Alors pour toute partie génératrice $\mathscr{G} \subseteq E$ et toute famille libre $\mathscr{L} \subseteq \mathscr{G}$, il existe une base B de E telle que $\mathscr{L} \subseteq B \subseteq \mathscr{G}$.

Corollaire 11. On suppose E de dimension finie.
— Il existe une base de E.
— (Théorème de la base extraite) De toute partie génératrice de E, on peut extraire une base de E.
— (Théorème de la base incomplète) Toute partie libre de E peut-être complétée en une base de E.

3. Théorie de la dimension

Théorème 12. On suppose E de dimension finie. Toutes les bases de E ont le même cardinal n. L'entier n s'appelle **dimension** de E, noté $\dim_{\mathbb{K}}(E)$ (ou simplement $\dim(E)$ en l'absence d'ambiguïté sur le corps de base).

Dans toute la suite, on se limitera au cas où E est de dimension finie, et on notera $n = \dim(E)$.

Proposition 13.
— Tout système libre de n vecteurs de E est une base de E.
— Tout système générateur de n vecteurs de E est une base de E.

Proposition 14. Soient $E_1, \dots, E_k$ des sous-espaces vectoriels de E. Alors,

$$E = E_1 \oplus \cdots \oplus E_k \iff E = E_1 + \cdots + E_k \text{ et } n = \sum_{i=1}^{k} \dim(E_i)$$

Proposition 15 (Formule de Grassmann)**.** Soient E_1 et E_2 deux sous-espaces vectoriels de E. Alors,

$$\dim(E_1 + E_2) = \dim(E_1) + \dim(E_2) - \dim(E_1 \cap E_2)$$

Corollaire 16. Soient E_1 et E_2 deux sous-espaces vectoriels de E. Les assertions suivantes sont équivalentes :

(i) $E = E_1 \oplus E_2$.

(ii) $\dim(E) = \dim(E_1) + \dim(E_2)$ et $E_1 \cap E_2 = \{0\}$.

(iii) $\dim(E) = \dim(E_1) + \dim(E_2)$ et $E = E_1 + E_2$.

Exemple 17.

$$\mathcal{M}_n(\mathbb{K}) = \mathcal{S}_n(\mathbb{K}) \oplus \mathcal{A}_n(\mathbb{K})$$

p. 240

II - Rang

1. Rang d'une application linéaire

Définition 18. Soient E et F deux espaces vectoriels sur $\mathbb{K}$. Soit $f \in \mathcal{L}(E,F)$. Si $\mathrm{Im}(f)$ est de dimension finie, on appelle **rang** de f l'entier $\dim(\mathrm{Im}(f))$, noté $\mathrm{rang}(f)$.

p. 120

Théorème 19 (Théorème du rang)**.** Soient E et F deux espaces vectoriels sur $\mathbb{K}$ avec E de dimension finie. Alors,

$$\dim(E) = \dim(\mathrm{Ker}(f)) + \mathrm{rang}(f)$$

Corollaire 20. Soit $f \in \mathcal{L}(E,F)$ où E et F sont de même dimension finie. Alors :

$$f \text{ bijective} \iff f \text{ injective} \iff f \text{ surjective}$$

Contre-exemple 21. L'application

$$\begin{array}{ccc} \mathbb{R}[X] & \to & \mathbb{R}[X] \\ P & \mapsto & P' \end{array}$$

est linéaire surjective, mais pas injective.

Application 22. L'application

$$\begin{array}{ccc} \mathcal{M}_n(\mathbb{K}) & \to & \mathcal{L}(\mathcal{M}_n(\mathbb{K}),\mathbb{K}) \\ A & \mapsto & (X \mapsto \text{trace}(AX)) \end{array}$$

est un isomorphisme.

p. 138

2. Rang d'une matrice

Définition 23. Soit $A \in \mathcal{M}_{p,q}(\mathbb{K})$. On appelle **rang** de A la dimension du sous-espace vectoriel de $\mathbb{K}^q$ engendré par les colonnes de A. Si A est la matrice d'une application linéaire f, on a $\text{rang}(A) = \text{rang}(f)$.

p. 128

Remarque 24. Soit $A \in \mathcal{M}_{p,q}(\mathbb{K})$.

— $\text{rang}(A) \leq \min(p,q)$.

— Si $p = q$, A est inversible si et seulement si $\text{rang}(A) = p$.

Théorème 25. Soit $A \in \mathcal{M}_{p,q}(\mathbb{K})$. Si A est de rang $r \geq 1$, alors A est équivalente à

$$J_r = \begin{pmatrix} I_r & 0 \\ 0 & O \end{pmatrix}$$

Corollaire 26. Deux matrices A et $B \in \mathcal{M}_{p,q}(\mathbb{K})$ sont équivalentes si et seulement si elles ont le même rang.

Théorème 27. Le rang d'une matrice est le plus grand des ordres des matrices carrées inversibles extraites de cette matrice.

Corollaire 28. Le rang de toute matrice est égal au rang de sa transposée.

Remarque 29. Autrement dit, la dimension du sous-espace engendré par les vecteurs colonnes d'une matrice est égal à la dimension du sous-espace engendré par ses vecteurs lignes.

Proposition 30. On ne change pas le rang d'une matrice par opérations élémentaires.

Exemple 31. On peut utiliser l'algorithme du pivot de Gauss pour trouver le rang d'une matrice. Ainsi,

$$\operatorname{rang}\begin{pmatrix} 2 & 1 & 3 & -3 \\ -1 & 2 & 1 & 4 \\ 1 & 1 & 2 & -1 \end{pmatrix} = \operatorname{rang}\begin{pmatrix} 2 & 1 & 3 & -3 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} = 2$$

III - Applications

1. Dualité

Soit E un espace vectoriel sur $\mathbb{K}$ de dimension finie n.

Définition 32. L'ensemble $E^* = \mathscr{L}(E, \mathbb{K})$ est appelé **dual** de E. Ses éléments sont les **formes linéaires** sur E.

Définition 33. Soit $B = (e_1, \dots, e_n)$ une base de E. Pour tout $i \in [\![1, n]\!]$, on définit

$$e_i^* : e_j \mapsto \begin{cases} 1 & \text{si } i = j \\ 0 & \text{sinon} \end{cases}$$

la **forme linéaire coordonnée** d'indice i.

Théorème 34. $B^* = (e_1^*, \dots, e_n^*)$ est une base de E^* appelée **base duale** de B. B est alors la **base antéduale** de B^*.

Corollaire 35.
— E^* est de dimension finie et $\dim(E^*) = n$.
— $\forall \varphi \in E^*, \varphi = \sum_{i=1}^{n} \varphi(e_i) e_i^*$.

Application 36 (Formule de Taylor)**.** On suppose $\mathbb{K}$ de caractéristique nulle. Pour tout $j \in [\![0, n]\!]$, on définit :

$$e_j : \begin{array}{ccc} \mathbb{K}_n[X] & \to & \mathbb{K} \\ P & \mapsto & \frac{P^{(j)}(0)}{j!} \end{array}$$

Alors, $(e_i)_{i \in [\![0,n]\!]}$ est une base de $K_n[X]^*$, dont la base antéduale est $(X^i)_{i \in [\![0,n]\!]}$.

[ROM21] p. 442

2. Classification des formes quadratiques

On se place sur le corps $\mathbb{K} = \mathbb{R}$.

[GOU21] p. 239

Définition 37. Soit $\varphi : E \times E \to \mathbb{K}$ une application.

— φ est une **forme bilinéaire** sur E si $\forall x \in E, \varphi(x,\cdot)$ est linéaire et de même pour $\varphi(\cdot,y), \forall y \in E$. Si $B = (e_i)_{i\in[\![1,n]\!]}$ est une base de E, on définit la matrice M de φ dans B par $M = (\varphi(e_i,e_j))_{i,j\in[\![1,n]\!]}$.

— Si de plus $\forall x,y \in E, \varphi(x,y) = \varphi(y,x)$, on dit que φ est **symétrique**.

Définition 38. On appelle **forme quadratique** sur E toute application q de la forme

$$q : \begin{array}{ccc} E & \to & \mathbb{K} \\ x & \mapsto & \varphi(x,x) \end{array}$$

où φ est une forme bilinéaire symétrique sur E.

Proposition 39. Soit q une forme quadratique sur E. Il existe une unique forme bilinéaire symétrique φ telle que pour tout $x \in E$, $q(x) = \varphi(x,x)$.

φ est alors la **forme polaire** de q, et on a

$$\forall x,y \in E, \varphi(x,y) = \frac{1}{2}(q(x+y) - q(x) - q(y))$$

Définition 40. Soit q une forme quadratique sur E. On appelle **rang** de q (noté $\mathrm{rang}(q)$) le rang de la matrice de sa forme polaire.

Lemme 41. Soit Φ une forme quadratique sur E. Il existe une base Φ-orthogonale (ie. si φ est la forme polaire de Φ, une base B où $\forall e,e' \in B, \varphi(e,e') = 0$ si $e \neq e'$).

[DEV]

Théorème 42 (Loi d'inertie de Sylvester)**.** Soit Φ une forme quadratique sur E.

$$\exists p,q \in \mathbb{N} \text{ et } \exists f_1,\dots,f_{p+q} \in E^* \text{ tels que } \Phi = \sum_{i=1}^{p} |f_i|^2 - \sum_{i=p+1}^{p+q} |f_i|^2$$

où les formes linéaires f_i sont linéairement indépendantes et où $p+q \leq n$. De plus, ces entiers ne dépendent que de Φ et pas de la décomposition choisie.

Le couple (p,q) est la **signature** de Φ et le rang Φ est égal à $p+q$.

Exemple 43. La signature de la forme quadratique $\Phi : (x,y,z) \mapsto x^2 - 2y^2 + xz + yz$ est $(2,1)$, donc son rang est 3.

3. Extensions de corps

Définition 44. On appelle **extension** de $\mathbb{K}$ tout corps $\mathbb{L}$ tel qu'il existe un morphisme de corps de $\mathbb{K}$ dans $\mathbb{L}$. On notera $\mathbb{L}/\mathbb{K}$ pour signifier que $\mathbb{L}$ est une extension de $\mathbb{K}$ par la suite.

[GOZ] p. 21

Définition 45. Soit $\mathbb{L}/\mathbb{K}$ une extension de $\mathbb{K}$. On appelle **degré** de $\mathbb{L}/\mathbb{K}$ et on note $[\mathbb{L} : \mathbb{K}]$, la dimension de $\mathbb{L}$ comme $\mathbb{K}$-espace vectoriel.

Théorème 46 (Base télescopique)**.** Soient $\mathbb{L}/\mathbb{K}$ une extension de $\mathbb{K}$ et E un espace vectoriel sur $\mathbb{L}$.Soient $(e_i)_{i\in I}$ une base de E en tant que $\mathbb{L}$-espace vectoriel et $(\alpha_j)_{j\in J}$ une base de $\mathbb{L}$ en tant que $\mathbb{K}$-espace vectoriel.

Alors $(\alpha_j e_i)_{(i,j)\in I\times J}$ est une base de E en tant que $\mathbb{K}$-espace vectoriel.

Corollaire 47 (Multiplicativité des degrés)**.** Soient $\mathbb{L}/\mathbb{K}$ une extension de $\mathbb{K}$ et $\mathbb{M}/\mathbb{L}$ une extension de $\mathbb{L}$. Alors, sont équivalentes :

(i) $\mathbb{M}$ est un $\mathbb{K}$-espace vectoriel de dimension finie.

(ii) $\mathbb{M}$ est un $\mathbb{L}$-espace vectoriel de dimension finie et $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel de dimension finie.

On a alors :

$$\dim_{\mathbb{K}}(M) = \dim_{\mathbb{L}}(M)\dim_{\mathbb{K}}(L) \iff [\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$$

Exemple 48.

$$[\mathbb{Q}[i+\sqrt{2}] : \mathbb{Q}] = 4$$

p. 46

4. Commutant

Soit $A \in \mathcal{M}_n(\mathbb{K})$.

Lemme 49. Si $\pi_A = \chi_A$, alors A est cyclique :

$$\exists x \in \mathbb{K}^n \setminus \{0\} \text{ tel que } (x, Ax, \dots, A^{n-1}x) \text{ est une base de } \mathbb{K}^n$$

[GOU21] p. 289

[FGN2] p. 160

Notation 50. — On note $\mathcal{T}_n(\mathbb{K})$ l'ensemble des matrices carrées triangulaires supérieures d'ordre n à coefficients dans le corps $\mathbb{K}$.

— On note $\mathscr{C}(A)$ le commutant de A.

Lemme 51.

$$\dim_{\mathbb{K}}(\mathscr{C}(A)) \geq n$$

Lemme 52. Le rang de A est invariant par extension de corps.

[DEV]

Théorème 53.

$$\mathbb{K}[A] = \mathscr{C}(A) \iff \pi_A = \chi_A$$

149 Déterminant. Exemples et applications.

Soient $\mathbb{K}$ un corps commutatif et E un espace vectoriel de dimension finie n sur $\mathbb{K}$.

I - Construction

1. Formes n-linéaires alternées et déterminant

[GOU21] p. 140

Définition 1. Soient $E_1, \dots, E_p$ et F des espaces vectoriels sur $\mathbb{K}$ et $f : E_1, \dots, E_p \to F$.

- f est dite p-**linéaire** si en tout point les p applications partielles sont linéaires.
- Si f est p-linéaire et si $E_1 = \cdots = E_p$ ainsi que $F = \mathbb{K}$, f est une **forme p-linéaire**. On note $\mathscr{L}_p(E, \mathbb{K})$ l'ensemble des formes p-linéaires sur E.
- Si de plus $f(x_1, \dots, x_p) = 0$ dès que deux vecteurs parmi les x_i sont égaux, alors f est dite **alternée**.

Exemple 2. En reprenant les notations précédentes, pour $p = 2$, f est bilinéaire.

Proposition 3. $\mathscr{L}_p(E, \mathbb{K})$ est un espace vectoriel et, $\dim(\mathscr{L}_p(E, \mathbb{K})) = \dim(E)^p$.

Théorème 4. L'ensemble des formes n-linéaires alternées sur E est un $\mathbb{K}$-espace vectoriel de dimension 1. De plus, il existe une unique forme n-linéaire alternée f prenant la valeur 1 sur une base $\mathscr{B}$ de E. On note $f = \det_{\mathscr{B}}$.

Définition 5. $\det_{\mathscr{B}}$ est l'application **déterminant** dans la base $\mathscr{B}$. En l'absence d'ambiguïté, on s'autorise à noter $\det = \det_{\mathscr{B}}$.

Proposition 6. Soit $\mathscr{B} = (e_1, \dots, e_n)$ une base de E. Si $x_1, \dots, x_n \in E$ ($\forall i \in [\![1, n]\!]$, on peut écrire $x_i = \sum_{j=1}^{n} x_{i,j} e_j$), on a la formule $\det_{\mathscr{B}}(x_1, \dots, x_n) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^{n} x_{i,\sigma(i)}$.

Proposition 7. Soit $\mathscr{B}$ une base de E. Si $\mathscr{B}'$ est une autre base de E, alors $\det_{\mathscr{B}'} = \det_{\mathscr{B}'}(\mathscr{B}) \det_{\mathscr{B}}$.

Théorème 8. Une famille de vecteurs est liée si et seulement si son déterminant est nul dans une base quelconque de E.

2. Déterminant d'un endomorphisme

Lemme 9. Soient $f \in \mathscr{L}(E)$ et $\mathscr{B} = (e_1, \dots, e_n)$ une base de E. Le scalaire $\det_{\mathscr{B}}(f(e_1), \dots, f(e_n))$ ne dépend pas de la base $\mathscr{B}$ considérée.

Définition 10. Soient $f \in \mathscr{L}(E)$ et $\mathscr{B} = (e_1, \dots, e_n)$ une base de E. On appelle **déterminant** de f le scalaire $\det_{\mathscr{B}}(f(e_1), \dots, f(e_n))$. On le note $\det(f)$.

Proposition 11. Soient $f, g \in \mathscr{L}(E)$.

(i) $\det(f \circ g) = \det(f) \times \det(g)$.

(ii) $\det(\mathrm{id}_e) = 1$.

(iii) $f \in \mathrm{GL}(E) \iff \det(f) \neq 0$. Dans ce cas, on a $\det(f^{-1}) = \det(f)^{-1}$.

3. Déterminant d'une matrice carrée

Définition 12. Soit $A \in \mathscr{M}_n(\mathbb{K})$. On appelle **déterminant** de A, le déterminant de ses vecteurs colonnes dans la base canonique de $\mathbb{K}^n$. On le note $\det(A)$.

Notation 13. Si $A = (a_{i,j})_{i,j \in [\![1,n]\!]} \in \mathscr{M}_n(\mathbb{K})$, on note son déterminant sous la forme

$$\det(A) = \begin{vmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \dots & a_{n,n} \end{vmatrix}$$

Exemple 14. — $\begin{vmatrix} a & c \\ b & d \end{vmatrix} = ad - bc$. [GRI] p. 104

— $\begin{vmatrix} 1 & -2 & 3 \\ 2 & 1 & -1 \\ 1 & 5 & 1 \end{vmatrix} = 39$.

Proposition 15. Soit $A \in \mathscr{M}_n(\mathbb{K})$. [GOU21] p. 142

(i) $\det(A) = \det({}^tA)$.

(ii) $\det(A)$ dépend linéairement des colonnes (resp. des lignes) de A.

(iii) $\forall \lambda \in \mathbb{K}, \det(\lambda A) = \lambda^n \det(A)$.

(iv) $\det(A) \neq 0 \iff A \in \mathrm{GL}_n(\mathbb{K})$.

(v) Si A est la matrice de $f \in \mathscr{L}(E)$ dans une base, alors $\det(f) = \det(A)$.

(vi) Si $B \in \mathcal{M}_n(\mathbb{K})$, $\det(AB) = \det(A)\det(B)$.

(vii) Deux matrices semblables ont le même déterminant.

II - Méthodes de calcul

1. Propriétés

Proposition 16. Soit $A \in \mathcal{M}_n(\mathbb{K})$.

(i) Si on effectue une permutation $\sigma \in S_n$ sur les colonnes ou les lignes de A, le déterminant est multiplié par $\epsilon(\sigma)$ (la signature de σ).

(ii) Si A est triangulaire, $\det(A)$ est le produit des éléments diagonaux de A.

(iii) On ne change pas la valeur d'un déterminant en ajoutant à une colonne une combinaison linéaire des autres colonnes. Même chose sur les lignes.

Exemple 17.

$$\begin{vmatrix} 1 & 2 & 1 \\ 1 & 0 & 1 \\ -1 & 1 & m \end{vmatrix} = \begin{vmatrix} 1 & 2 & 0 \\ 1 & 0 & 0 \\ -1 & 1 & m+1 \end{vmatrix} = -2(m+1)$$

Proposition 18 (Déterminant par blocs)**.** Soit $M \in \mathcal{M}_n(\mathbb{K})$ une matrice triangulaire par blocs, de la forme

$$M = \begin{pmatrix} A & C \\ 0 & B \end{pmatrix}$$

alors $\det(M) = \det(A)\det(B)$.

2. Mineurs et cofacteurs

Définition 19. Soit $A = (a_{i,j})_{i,j\in[\![1,n]\!]} \in \mathcal{M}_n(\mathbb{K})$.

— Pour tout $i, j \in [\![1, n]\!]$, on appelle **mineur** de l'élément $a_{i,j}$ le déterminant $\Delta_{i,j}$ de la matrice obtenue en supprimant la i-ième ligne et la j-ième colonne de A.

— Le scalaire $A_{i,j} = (-1)^{i+j}\Delta_{i,j}$ s'appelle le **cofacteur** de $a_{i,j}$.

— On appelle **mineurs principaux** de A les déterminants $\Delta_k = \det((a_{i,j})_{i,j\in[\![1,k]\!]})$ pour $k \in [\![1, n]\!]$.

Proposition 20. En reprenant les notations précédentes :

(i) Soit $j \in [\![1, n]\!]$. On a $\det(A) = \sum_{i=1}^{n} a_{i,j}A_{i,j}$ (développement par rapport à la j-ième

colonne).

(ii) Soit $i \in [\![1,n]\!]$. On a $\det(A) = \sum_{j=1}^{n} a_{i,j}A_{i,j}$ (développement par rapport à la i-ième ligne).

Exemple 21. [GRI] p. 118

$$\begin{vmatrix} 6 & 0 & -6 \\ 0 & 2 & 7 \\ 0 & 2 & 3 \end{vmatrix} = 6\begin{vmatrix} 2 & 7 \\ 2 & 3 \end{vmatrix} = 6(6-14) = -48$$

Définition 22. Soit $A \in \mathcal{M}_n(\mathbb{K})$. La matrice $(A_{i,j})_{i,j\in[\![1,n]\!]}$ des cofacteurs des éléments de A est appelée **comatrice** de A, et on la note $\mathrm{com}(A)$. [GOU21] p. 143

Proposition 23. Soit $A \in \mathcal{M}_n(\mathbb{K})$. On a :

$$A\,{}^t\mathrm{com}(A) = {}^t\mathrm{com}(A)A = \det(A)I_n$$

Corollaire 24. Soit $A \in \mathrm{GL}_n(\mathbb{K})$. Alors,

$$A^{-1} = \frac{1}{\det(A)}\,{}^t\mathrm{com}(A)$$

Exemple 25. Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{K})$. Alors,

$$A^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

3. Exemples classiques

Exemple 26 (Déterminant de Vandermonde)**.** Soient $a_1, \dots, a_n \in \mathbb{K}$. Alors

$$\begin{vmatrix} 1 & a_1 & \dots & a_1^{n-1} \\ 1 & a_2 & \dots & a_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \dots & a_n^{n-1} \end{vmatrix} = \prod_{1\le i<j\le n} (a_j - a_i)$$

Exemple 27 (Déterminant de Cauchy)**.** Soient $a_1, \dots, a_n, b_1, \dots, b_n \in \mathbb{K}$ tels que pour tout p. 150

$i,j \in [\![1,n]\!]$, $a_i + b_j \neq 0$. Alors

$$\det\left(\frac{1}{a_i+b_j}\right) = \frac{\prod_{1\leq i<j\leq n}(a_j-a_i)\prod_{1\leq i<j\leq n}(b_j-b_i)}{\prod_{i,j=1}^{n}(a_i+b_j)}$$

Exemple 28 (Déterminant circulant)**.** Soient $a_1,\dots,a_n \in \mathbb{C}$. On pose $\omega = e^{\frac{2i\pi}{n}}$. Alors

$$\begin{vmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \dots & a_0 \end{vmatrix} = \prod_{j=0}^{n-1} P(\omega^j)$$

où $P = \sum_{k=0}^{n-1} a_k X^k$.

p. 153

III - Applications

1. En géométrie

a. Volume d'un parallélépipède

Théorème 29. L'aire $\mathcal{A}(v,w)$ du parallélogramme engendré par deux vecteurs $v,w \in \mathbb{R}^n$ est égale à

$$\mathcal{A}(v,w) = |\det(v,w)|$$

[GRI] p. 130

Corollaire 30. Soient $v_1,\dots,v_n \in \mathbb{R}^n$. On note $\mathcal{V}(v_1,\dots,v_n)$ le volume du parallélépipède rectangle engendré par $v_1,\dots,v_n$ (ie. l'ensemble $\{z \in \mathbb{R}^n \mid z = \sum_{i=1}^n \lambda_i v_i, \lambda_i \in [0,1]\}$). On a alors :

$$\mathcal{V}(v_1,\dots,v_n) = |\det(v_1,\dots,v_n)|$$

b. Suite de polygones

[DEV]

Théorème 31 (Suite de polygones)**.** Soit P_0 un polygone dont les sommets sont $\{z_{0,1},\dots,z_{0,n}\}$. On définit la suite de polygones (P_k) par récurrence en disant que, pour tout $k \in \mathbb{N}^*$, les sommets de P_{k+1} sont les milieux des arêtes de P_k.

Alors la suite (P_k) converge vers l'isobarycentre de P_0.

[I-P] p. 389

2. En algèbre linéaire

a. Aux systèmes d'équations linéaires

On cherche à résoudre un système d'équations linéaires de la forme p. 143

$$AX = B \tag{S}$$

avec $A = (a_{i,j})_{\substack{i\in[\![1,p]\!]\\ j\in[\![1,q]\!]}}$ et $B = (b_i)_{i\in[\![1,p]\!]} \in \mathbb{K}^p$.

Théorème 32 (Formules de Cramer)**.** On se place dans le cas $p = q = n$. Alors, (S) admet une unique solution si et seulement si $\det(A) \neq 0$. Dans ce cas, elle est donnée par $X = (x_i)_{i\in[\![1,n]\!]}$ où

$$\forall i \in [\![1,n]\!],\ x_i = \frac{\det(A_i)}{\det(A)}$$

avec A_i obtenue en remplaçant la i-ième colonne de A par B.

Lemme 33. Soit $r = \operatorname{rang}(A)$. Il existe un déterminant Δ d'ordre r extrait de A.

Définition 34.
- Le déterminant Δ précédent est le **déterminant principal** de A.
- Les équations (resp. inconnues) dont les indices sont deux des lignes (resp. colonnes) de Δ s'appellent les **équations principales** (resp. **inconnues principales**).
- Si $\Delta = \det(a_{i,j})_{\substack{i\in I\\ j\in J}}$, on appelle **déterminants caractéristiques** les déterminants d'ordre $r+1$ de la forme

$$\left|\begin{array}{c|c} (a_{i,j})_{\substack{i\in I\\ j\in J}} & (b_i)_{i\in I} \\ \hline (a_{k,j})_{j\in J} & b_k \end{array}\right| \text{ avec } k \notin J.$$

Théorème 35 (Rouché-Fontené)**.** Le système (S) admet des solutions si et seulement si $p = r$ ou les $p - r$ déterminants caractéristiques sont nuls. Le système est alors équivalent au système des équations principales. Les inconnues principales étant déterminées par un système de Cramer à l'aide des inconnues non principales.

Exemple 36. Si,

$$(S) \iff \begin{cases} x + 2y + z + t = 1 \\ x - z - t = 1 \\ -x + y + z + 2t = m \end{cases} \qquad m \in \mathbb{R}$$

on a $\text{rang}(A) = 2$, (S) admet des solutions si et seulement si $m = -1$, et

$$(S) \iff \begin{cases} x + 2y = 1 + z - t \\ x = 1 + z + t \end{cases} \iff \begin{cases} x = 1 + z + t \\ y = -t \end{cases}$$

b. À la réduction des endomorphismes

Définition 37. Soit $A \in \mathcal{M}_n(\mathbb{K})$. On appelle : [GOU21] p. 171

— **Polynôme caractéristique** de A le polynôme $\chi_A = \det(A - XI_n)$.

— **Polynôme minimal** de A l'unique polynôme unitaire π_A qui engendre l'idéal $\text{Ann}(A) = \{Q \in \mathbb{K}[X] \mid Q(A) = 0\}$. p. 186

Proposition 38. p. 172

$$\lambda \text{ est valeur propre de } A \iff \chi_A(\lambda) = 0 \iff \pi_A(\lambda) = 0$$

Proposition 39. p. 185

— A est trigonalisable si et seulement si χ_A est scindé sur $\mathbb{K}$.

— A est diagonalisable si et seulement si π_A est scindé à racines simples sur $\mathbb{K}$.

Corollaire 40. Si $\mathbb{K} = \mathbb{F}_q$, A est diagonalisable si et seulement si $A^q = A$.

Théorème 41 (Cayley-Hamilton)**.**

$$\pi_u \mid \chi_u$$

c. À l'étude du groupe linéaire

Théorème 42. Soit $u \in \mathcal{L}(E)$. Les assertions suivantes sont équivalentes : [ROM21] p. 140

(i) $u \in \text{GL}(E)$.

(ii) $\text{Ker}(u) = \{0\}$.

(iii) $\text{Im}(u) = E$.

(iv) $\text{rang}(u) = n$.

(v) $\det(u) = 0$.

(vi) u transforme toute base de E en une base de E.

(vii) Il existe $v \in \mathcal{L}(E)$ tel que $u \circ v = \text{id}_E$.

(viii) Il existe $w \in \mathcal{L}(E)$ tel que $w \circ u = \text{id}_E$.

Proposition 43. $\det : \mathrm{GL}(E) \to \mathbb{K}^*$ est un morphisme surjectif. [PER] p. 95

Soit p un nombre premier ≥ 3. On se place sur le corps $\mathbb{K} = \mathbb{F}_p$.

Définition 44. Soit H un hyperplan de E et G un supplémentaire de H. On définit f la **dilatation** de base H, de direction G et de rapport $\lambda \in \mathbb{K}^*$ par [I-P] p. 203

$$\forall x \in H, \forall y \in G, f(x+y) = x + \lambda y$$

Théorème 45. Si $|\mathbb{K}| \geq 3$, les dilatations engendre $\mathrm{GL}(E)$.

Notation 46. Soit $a \in \mathbb{F}_p$. On note $\left(\frac{a}{p}\right)$ le symbole de Legendre de a modulo p.

Lemme 47. $a \mapsto \left(\frac{a}{p}\right)$ est un morphisme de groupes.

Lemme 48. Il y a $\frac{p-1}{2}$ résidus quadratiques dans $\mathbb{F}_p^*$.

Théorème 49. Le groupe multiplicatif d'un corps fini est cyclique.

[DEV]

Théorème 50 (Frobenius-Zolotarev)**.**

$$\forall u \in \mathrm{GL}(E), \epsilon(u) = \left(\frac{\det(u)}{p}\right)$$

où u est vu comme une permutation des éléments de E.

Annexes

[I-P]
p. 389

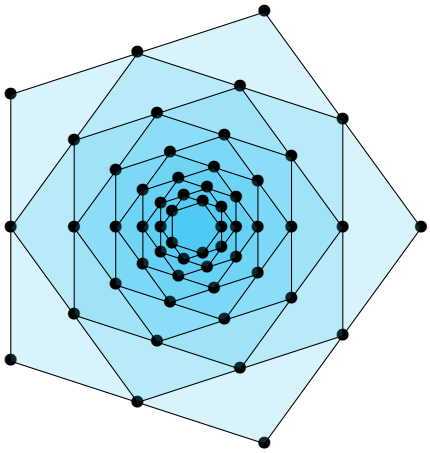


FIGURE I.4 – La suite de polygones.

150 Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.

Soit E un espace vectoriel de dimension finie n sur un corps commutatif $\mathbb{K}$. Soit $u \in \mathscr{L}(E)$.

I - Polynômes d'endomorphismes

1. L'algèbre $\mathbb{K}[u]$

Notation 1. On note $u^0 = \mathrm{id}_E$ et

$$u^k = \underbrace{u \circ \ldots \circ u}_{k \text{ fois}}$$

[ROM21] p. 603

Définition 2. À tout polynôme $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ on fait correspondre l'endomorphisme $P(u) = \sum_{k=1}^{n} a_k u^k$.

Proposition 3. L'ensemble,

$$\mathbb{K}[u] = \{P(u) \mid P \in \mathbb{K}[X]\}$$

est une sous-algèbre commutative de $\mathscr{L}(E)$, de dimension inférieure ou égale à n^2.

Remarque 4. Au vu de l'isomorphisme entre $\mathscr{L}(E)$ et $\mathscr{M}_n(\mathbb{K})$, on définit de même $\mathbb{K}[A]$ pour une matrice $A \in \mathscr{M}_n(\mathbb{K})$. Si A est la matrice de u dans une base de E, alors pour tout $P \in \mathbb{K}[X]$, $P(A)$ est la matrice de $P(u)$ dans cette même base. Toute les propriétés énoncées pour les endomorphismes sont vraies pour les matrices, et réciproquement.

Proposition 5. Soient $M \in \mathscr{M}_n(\mathbb{K})$ triangulaire de la forme

$$M = \begin{pmatrix} \alpha_1 & * & \ldots & * \\ 0 & \alpha_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \ldots & 0 & \alpha_n \end{pmatrix}$$

[GOU21] p. 184

et $P \in \mathbb{K}[X]$. Alors, $P(M)$ est de la forme

$$P(M) = \begin{pmatrix} P(\alpha_1) & * & \dots & * \\ 0 & P(\alpha_2) & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \dots & 0 & P(\alpha_n) \end{pmatrix}$$

2. Polynôme caractéristique de u

Définition 6. Soit $\lambda \in \mathbb{K}$. [ROM21] p. 643

- On dit que λ est **valeur propre** de u si $E_\lambda = \mathrm{Ker}(u - \lambda \mathrm{id}_E)$ n'est pas réduit à $\{0\}$.
- Un vecteur $x \neq 0$ tel que $u(x) = \lambda x$ est un **vecteur propre** de u associé à la valeur propre λ.
- E_λ est le **sous-espace propre** associé à la valeur propre λ.
- L'ensemble des valeurs propres de u est appelé **spectre** de u. On le note $\mathrm{Sp}(u)$.

Proposition 7. En notant $\chi_u = \det(X\mathrm{id}_E - u)$,

$$\mathrm{Sp}(u) = \{\lambda \in \mathbb{K} \mid \chi_u(\lambda) = 0\}$$

Théorème 8. Soit $P \in \mathbb{K}[X]$. Pour tout valeur propre λ de u (voir Théorème 6), $P(\lambda)$ est une valeur propre de $P(u)$. Si le corps $\mathbb{K}$ est algébriquement clos, on a alors p. 604

$$\mathrm{Sp}(P(u)) = \{P(\lambda) \mid \lambda \in \mathrm{Sp}(u)\}$$

Contre-exemple 9. Pour $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathcal{M}_2(\mathbb{R})$ et $P = X^2$, on a $A^2 = -I_2$ et $\mathrm{Sp}(A) = \emptyset$.

Définition 10. Le polynôme χ_u précédent est appelé **polynôme caractéristique** de u. p. 644

Remarque 11. On peut définir de la même manière les mêmes notions pour une matrice de $\mathcal{M}_n(\mathbb{K})$ (une valeur est propre pour une matrice si et seulement si elle l'est pour l'endomorphisme associé). On reprendra les mêmes notations.

Exemple 12. Pour $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{K})$, on a $\chi_A = X^2 - \mathrm{trace}(A)X + \det(A)$.

Proposition 13. Soit λ une valeur propre de u de multiplicité α en tant que racine de χ_u. Alors,

$$\dim(E_\lambda) \in [\![1, \alpha]\!]$$

Proposition 14. (i) Le polynôme caractéristique est un invariant de similitude.

(ii) Soit $A \in \mathcal{M}_n(\mathbb{K})$. On note $\chi_A = \sum_{k=0}^{n} a_k X^k$. Alors, $a_0 = \det(A)$ et $a_{n-1} = \text{trace}(A)$ (à un signe près).

[GOU21] p. 172

3. Polynôme minimal de u

Lemme 15. (i) $\text{Ann}(u) = \{P \in \mathbb{K}[X] \mid P(u) = 0\}$ est un sous-ensemble de $\mathbb{K}[u]$ non réduit au polynôme nul.

(ii) $\text{Ann}(u)$ est le noyau de $P \mapsto P(u)$: c'est un idéal de $\mathbb{K}[u]$.

(iii) Il existe un unique polynôme unitaire engendrant cet idéal.

[ROM21] p. 604

Définition 16. On appelle **idéal annulateur** de u l'idéal $\text{Ann}(u)$. Le polynôme unitaire générateur est noté π_u et est appelé **polynôme minimal** de u.

Remarque 17. — π_u est le polynôme unitaire de plus petit degré annulant u.

— Si $A \in \mathcal{M}_n(\mathbb{K})$ est la matrice de u dans une base de E, on a $\text{Ann}(u) = \text{Ann}(A)$ et $\pi_u = \pi_A$.

Exemple 18. Un endomorphisme est nilpotent d'indice q si et seulement si son polynôme minimal est X^q.

Proposition 19. Soit F un sous-espace vectoriel de E stable par u. Alors, le polynôme minimal de l'endomorphisme $u_{|F} : F \to F$ divise π_u.

Proposition 20. (i) Les valeurs propres de u sont racines de tout polynôme annulateur.

(ii) Les valeurs propres de u sont exactement les racines de π_u.

Remarque 21. π_u et χ_u partagent dont les mêmes racines.

[GOU21] p. 186

Théorème 22. $P \mapsto P(u)$ induit un isomorphisme :

$$\mathbb{K}[X]/(\pi_u) \cong \mathbb{K}[u]$$

[ROM21] p. 606

Corollaire 23. L'espace vectoriel $\mathbb{K}[u]$ est de dimension égale à $p_u = \deg(\pi_u)$, une base étant donnée par $(u^k)_{k\in[\![1,p_u]\!]}$.

Corollaire 24.

$$\mathbb{K}[u] \text{ est un corps} \iff \mathbb{K}[u] \text{ est intègre} \iff u \text{ est irréductible}$$

Théorème 25 (Cayley-Hamilton)**.**

$$\pi_u \mid \chi_u$$

Corollaire 26.

$$\dim(\mathbb{K}[u]) \leq n$$

Corollaire 27. Si u est inversible,

$$u^{-1} = -\frac{1}{\det(u)} \sum_{k=1}^{n} a_k u^{k-1}$$

En particulier, $u^{-1} \in \mathbb{K}[u]$.

Corollaire 28. u est nilpotent si et seulement si $\chi_u = X^n$.

II - Réduction d'endomorphismes

1. Diagonalisation

Définition 29. — On dit que u est **diagonalisable** s'il existe une base de E dans laquelle la matrice de u est diagonale.

— On dit qu'une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est **diagonalisable** si elle est semblable à une matrice diagonale.

p. 683

Remarque 30. u est diagonalisable si et seulement si sa matrice dans n'importe quelle base de E l'est.

Exemple 31. — Les projecteurs (ie. les endomorphismes $p \in \mathcal{L}(E)$ tels que $p^2 = p$) sont toujours diagonalisables, à valeurs propres dans $\{0, 1\}$.

— Les symétries (ie. les endomorphismes $s \in \mathcal{L}(E)$ tels que $s^2 = \mathrm{id}_E$) sont toujours diagonalisables, à valeurs propres dans $\{\pm 1\}$. Par exemple, l'endomorphisme de trans-

[BMP] p. 166

position $A \mapsto {}^tA$ est diagonalisable.

Proposition 32. Si u a n valeurs propres distinctes dans $\mathbb{K}$, alors il est diagonalisable. [ROM21] p. 683

Théorème 33 (Lemme des noyaux)**.** Soit $P = P_1 \dots P_k \in \mathbb{K}[X]$ où les polynômes $P_1, \dots, P_k$ sont premiers entre eux deux à deux. Alors, p. 609

$$\operatorname{Ker}(P(u)) = \bigoplus_{i=1}^{k} \operatorname{Ker}(P_i(u))$$

Théorème 34. Soit $\operatorname{Sp}(u) = \{\lambda_1, \dots, \lambda_p\}$. Les assertions suivantes sont équivalentes : p. 683

(i) u est diagonalisable sur $\mathbb{K}$.

(ii) $E = \bigoplus_{k=1}^{p} E_{\lambda_k}$.

(iii) $\sum_{k=1}^{p} \dim(E_{\lambda_k}) = n$.

(iv) χ_n est scindé sur $\mathbb{K}$ et pour tout $k \in [\![1, p]\!]$, la dimension de E_{λ_k} est égale à la multiplicité de λ_k dans χ_u.

(v) $\exists P \in \operatorname{Ann}(u)$ scindé à racines simples.

(vi) π_u est scindé à racines simples.

Exemple 35. $\begin{pmatrix} 0 & 2 & -1 \\ 3 & -2 & 0 \\ -2 & 2 & 1 \end{pmatrix}$ est diagonalisable, semblable à $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -4 \end{pmatrix}$. [GOU21] p. 177

Théorème 36 (Diagonalisation simultanée)**.** Soit $(u_i)_{i \in I}$ une famille d'endomorphismes de E diagonalisables. Il existe une base commune de diagonalisation dans E pour $(u_i)_{i \in I}$ si et seulement si ces endomorphismes commutent deux-à-deux. [ROM21] p. 684

Théorème 37 (Spectral)**.** Tout endomorphisme symétrique se diagonalise dans une base orthonormée. p. 734

2. Trigonalisation

Définition 38. — On dit que u est **trigonalisable** s'il existe une base de E dans laquelle la matrice de u est triangulaire supérieure.
— On dit qu'une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est **trigonalisable** si elle est semblable à une matrice diagonale.

p. 675

Remarque 39. u est trigonalisable si et seulement si sa matrice dans n'importe quelle base de E l'est.

Exemple 40. Une matrice à coefficients réels ayant des valeurs propres imaginaires pures n'est pas trigonalisable dans $\mathcal{M}_n(\mathbb{R})$.

Théorème 41. u est trigonalisable sur $\mathbb{K}$ si et seulement si χ_u est scindé sur $\mathbb{K}$.

Corollaire 42. Si $\mathbb{K}$ est algébriquement clos, tout endomorphisme de u est trigonalisable sur $\mathbb{K}$.

Proposition 43. Si u est trigonalisable, sa trace est la somme de ses valeurs propres et son déterminant est le produit de ses valeurs propres.

Théorème 44 (Trigonalisation simultanée)**.** Soit $(u_i)_{i\in I}$ une famille d'endomorphismes de E diagonalisables qui commutent deux-à-deux. Alors, il existe une base commune de trigonalisation.

3. Décomposition de Dunford

[DEV]

Théorème 45 (Décomposition de Dunford)**.** On suppose que π_u est scindé sur $\mathbb{K}$. Alors il existe un unique couple d'endomorphismes (d, n) tels que :
— d est diagonalisable et n est nilpotent.
— $u = d + n$.
— $dn = nd$.

[GOU21] p. 203

Corollaire 46. Si u vérifie les hypothèse précédentes, pour tout $k \in \mathbb{N}$, $u^k = (d+n)^k = \sum_{i=0}^{m} \binom{k}{i} d^i n^{k-i}$, avec $m = \min(k, l)$ où l désigne l'indice de nilpotence de n.

Remarque 47. On peut montrer de plus que d et n sont des polynômes en u.

III - Applications

1. Commutant

Soit $A \in \mathcal{M}_n(\mathbb{K})$.

[FGN2] p. 160

Notation 48. On note $\mathcal{C}(A)$ le commutant de A.

Lemme 49.

$$\dim_{\mathbb{K}}(\mathcal{C}(A)) \geq n$$

[DEV]

Application 50. Soit $A \in \mathcal{M}_n(\mathbb{K})$. On note $\mathcal{C}(A)$ le commutant de A. Alors,

$$\mathbb{K}[A] = \mathcal{C}(A) \iff \pi_A = \chi_A = \det(XI_n - A)$$

2. Exponentielles de matrices

[ROM21] p. 761

Lemme 51. (i) La série entière $\sum \frac{z^k}{k!}$ a un rayon de convergence infini.

(ii) $\sum \frac{A^k}{k!}$ est convergente pour toute matrice $A \in \mathcal{M}_n(\mathbb{K})$.

Définition 52. Soit $A \in \mathcal{M}_n(\mathbb{K})$. On définit **l'exponentielle** de A par

$$\sum_{k=0}^{+\infty} \frac{A^k}{k!}$$

on la note aussi $\exp(A)$ ou e^A.

Théorème 53. Soit $A \in \mathcal{M}_n(\mathbb{K})$.

(i) $\exp : \mathcal{M}_n(\mathbb{K}) \to \mathcal{M}_n(\mathbb{K})$ est continue.

(ii) Si A est nilpotente d'indice q, $\exp(A) = \sum_{k=0}^{q-1} \frac{A^k}{k!}$.

(iii) $\exp(A) \in \mathbb{K}[A]$. En particulier, $\exp(A)$ commute avec A.

(iv) Si $A = \mathrm{Diag}(\lambda_1, \dots, \lambda_n)$, alors $\exp(A) = \mathrm{Diag}(e^{\lambda}_1, \dots, e^{\lambda}_n)$.

(v) Si $B = PAP^{-1}$ pour $P \in \mathrm{GL}_n(\mathbb{K})$, alors $e^B = P^{-1}e^A P$.

(vi) $\det(e^A) = e^{\mathrm{trace}(A)}$.

(vii) $t \mapsto e^{tA}$ est de classe $\mathcal{C}^\infty$, de dérivée $t \mapsto e^{tA}A$.

Proposition 54. Soient $A, B \in \mathcal{M}_n(\mathbb{K})$ qui commutent. Alors,

$$e^A e^B = e^{A+B} = e^B e^A$$

Corollaire 55. Soit $A \in \mathcal{M}_n(\mathbb{K})$. Alors, e^A est inversible, d'inverse e^{-A}.

Exemple 56. Soit $A \in \mathcal{M}_n(\mathbb{K})$ qui admet une décomposition de Dunford $A = D + N$ où D est diagonalisable et N est nilpotente d'indice q. Alors,

— $e^A = e^D e^N = e^D \sum_{k=0}^{q-1} \frac{N^k}{k!}$.

— La décomposition de Dunford de e^A est $e^A = e^D + e^D(e^N - I_n)$ avec e^D diagonalisable et $e^D(e^N - I_n)$ nilpotente.

Application 57. Une équation différentielle linéaire homogène $(H) : Y' = AY$ (où A est constante en t) a ses solutions maximales définies sur $\mathbb{R}$ et le problème de Cauchy

$$\begin{cases} Y' = AY \\ Y(0) = y_0 \end{cases}$$

a pour (unique) solution $t \mapsto e^{tA} y_0$.

[GOU20] p. 380

Application 58 (Équation de Sylvester)**.** Soient A et $B \in \mathcal{M}_n(\mathbb{C})$ deux matrices dont les valeurs propres sont de partie réelle strictement négative. Alors pour tout $C \in \mathcal{M}_n(\mathbb{C})$, l'équation $AX + XB = C$ admet une unique solution X dans $\mathcal{M}_n(\mathbb{C})$.

[I-P] p. 177

3. Étude d'une suite de polygones

Lemme 59 (Déterminant circulant)**.** Soient $n \in \mathbb{N}^*$ et $a_1, \dots, a_n \in \mathbb{C}$. On pose $\omega = e^{\frac{2i\pi}{n}}$. Alors

$$\begin{vmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \dots & a_0 \end{vmatrix} = \prod_{j=0}^{n-1} P(\omega^j)$$

où $P = \sum_{k=0}^{n-1} a_k X^k$.

[GOU21] p. 153

Application 60 (Suite de polygones)**.** Soit P_0 un polygone dont les sommets sont $\{z_{0,1}, \dots, z_{0,n}\}$. On définit la suite de polygones (P_k) par récurrence en disant que, pour tout $k \in \mathbb{N}^*$, les sommets de P_{k+1} sont les milieux des arêtes de P_k.

[I-P] p. 389

Alors la suite (P_k) converge vers l'isobarycentre de P_0.

Annexes

[I-P]
p. 389

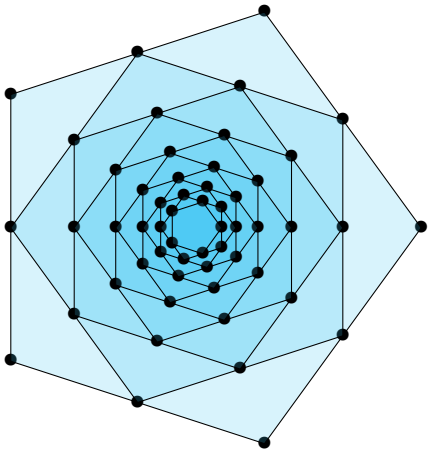


FIGURE I.5 – La suite de polygones.

151 Sous-espaces stables par un endomorphisme ou une famille d'endomorphismes d'un espace vectoriel de dimension finie. Applications.

Soit E un espace vectoriel sur un corps $\mathbb{K}$ de dimension finie n. Soit $u \in \mathscr{L}(E)$ un endomorphisme de E.

I - Stabilité

1. Définitions, endomorphismes induits

Définition 1. Soit F un sous-espace vectoriel de E. On dit que F est **stable** par u si $u(F) \subseteq F$. [BMP] p. 158

Exemple 2. Le noyau et l'image de u sont stables par u.

Proposition 3. Si $\mathbb{K} = \mathbb{R}$, alors u admet au moins une droite ou un plan stable.

Proposition 4. Soit F un sous-espace de E stable par u. Alors u induit deux endomorphismes :

- $u_{|F} : F \to F$ la restriction de u à F.
- $\overline{u} : E/F \to E/F$ obtenu par passage au quotient.

Définition 5. Soit A la matrice de l'endomorphisme u dans une base quelconque de E. On définit le **polynôme caractéristique** de u par $\chi_u = \det(XI_n - A)$. p. 163

Proposition 6. Soit F un sous-espace de E stable par u de dimension r. Soit $\mathscr{B} = (e_1, \dots, e_n)$ une base de E telle que les r premiers vecteurs forment une base $\mathscr{B}_F$ de F. Alors : p. 158

(i) La matrice de u dans la base $\mathscr{B}$ est de la forme

$$\mathrm{Mat}(u, \mathscr{B}) = \begin{pmatrix} A & C \\ 0 & B \end{pmatrix}$$

(ii) $\mathscr{B}_{E/F} = \pi_F(\mathscr{B} \setminus \mathscr{B}_F)$ est une base de E/F où $\pi_F : E \to E/F$ désigne la projection canonique sur le quotient.

(iii) $A = \mathrm{Mat}(u_{|F}, \mathscr{B}_F)$ et $B = \mathrm{Mat}(\overline{u}, \mathscr{B}_{E/F})$.

(iv) $\chi_u = \chi_{u_{|F}} \chi_{\overline{u}}$.

2. Sous-espaces stables et polynôme minimal

Proposition 7. Il existe un polynôme qui engendre l'idéal $\{P \in \mathbb{K}[X] \mid P(u) = 0\}$. Il s'agit du **polynôme minimal** de u noté π_u. p. 161

Théorème 8 (Cayley-Hamilton)**.**

$$\pi_u \mid \chi_u$$

Proposition 9. Soit F un sous-espace de E stable par u. Alors $\pi_{u_{|F}} \mid \pi_u$.

Proposition 10. Si $E = F_1 \oplus F_2$ avec F_1 et F_2 deux sous-espaces stables par u, alors $\pi_u = \text{ppcm}(\pi_{u_{|F_1}}, \pi_{u_{|F_2}})$.

Proposition 11. Soient P et Q deux polynômes unitaires tels que $\pi_u = PQ$. On note $F = \text{Ker}(P(u))$. Alors $\pi_{u_{|F}} = P$.

3. Recherche de sous-espaces stables

Définition 12. On suppose que le polynôme caractéristique de u est scindé sur $\mathbb{K}$: **[GOU21]** p. 201

$$\chi_u = \prod_{i=1}^{p} (X - \lambda_i)^{\alpha_i} \text{ où les } \lambda_i \text{ sont distincts deux-à-deux}$$

Pour tout $i \in [\![1, p]\!]$, le sous-espace vectoriel $N_i = \text{Ker}(f - \lambda_i \,\text{id}_E)^{\alpha_i}$ s'appelle le **sous-espace caractéristique** de f associé à λ_i.

Proposition 13 (Lemme des noyaux)**.** Soient $P_1, \dots, P_r \in \mathbb{K}[X]$ premiers entre eux. Alors p. 185

$$\bigoplus_{i=1}^{r} \text{Ker}(P_i(u)) = \text{Ker}\left(\left(\prod_{i=1}^{r} P_i\right)(u)\right)$$

Proposition 14. On suppose que le polynôme caractéristique de u est scindé sur $\mathbb{K}$. On note $N_1, \dots, N_p$ les sous-espaces caractéristiques de u. p. 202

- $\forall i \in [\![1, p]\!]$, N_i est stable par u.
- $E = N_1 \oplus \cdots \oplus N_p$.
- $\forall i \in [\![1, p]\!]$, $\dim N_i = \alpha_i$ où α_i est la multiplicité de λ_i dans χ_u.

[BMP] p. 159

Remarque 15. Plus généralement, $\forall \lambda \in \mathbb{K}$, $\forall i \in \mathbb{N}$, $\mathrm{Ker}(u - \lambda \mathrm{id}_E)^i$ est stable par u. C'est en fait un corollaire de la proposition suivante.

Proposition 16. Soient $u, v \in \mathscr{L}(E)$ tels que $uv = vu$ (pour la composition). Alors le noyau et l'image de v sont stables par u (et réciproquement).

Proposition 17. On suppose que le polynôme caractéristique de u est scindé sur $\mathbb{K}$. [GOU21] p. 202

$$\chi_u = \prod_{i=1}^{p} (X - \lambda_i)^{\alpha_i} \text{ où les } \lambda_i \text{ sont distincts deux-à-deux}$$

Alors :

(i) π_u est de la forme :

$$\pi_u = \prod_{i=1}^{p} (X - \lambda_i)^{r_i} \text{ où les } \lambda_i \text{ sont distincts deux-à-deux}$$

(ii) $\forall i \in [\![1, p]\!]$, $N_i = \mathrm{Ker}(f - \lambda_i \mathrm{id}_E)^{r_i}$.

(iii) $\forall i \in [\![1, p]\!]$, r_i est l'indice de nilpotence de l'endomorphisme $f_{|N_i} - \lambda_i \mathrm{id}_{N_i}$.

4. Utilisation de la dualité

Définition 18. On appelle **forme linéaire** de E toute application linéaire de E dans $\mathbb{K}$ et on note E^* appelé **dual** de E l'ensemble des formes linéaires de E. p. 132

Proposition 19. E^* est un espace vectoriel sur $\mathbb{K}$ de dimension n.

Définition 20. Si $A \subset E$, on note $A^\perp = \{\varphi \in E^* \mid \forall x \in A, \varphi(x) = 0\}$ l'**orthogonal** (au sens de la dualité) de A qui est un sous-espace vectoriel de E^*.

Proposition 21. Si F est un sous-espace vectoriel de E, on a $\dim F + \dim F^\perp = \dim E$.

Définition 22. On définit ${}^t u : E^* \to E^*$ l'**application transposée** de u par

$$\forall \varphi \in E^*, {}^t u(\varphi) = \varphi \circ u$$

Proposition 23. Un sous-espace vectoriel F de E est stable par u si et seulement si $F^\perp$ est stable par ${}^t u$.

Remarque 24. C'est un résultat qui peut s'avérer utile dans les démonstrations par récurrence s'appuyant sur la dimension d'un sous-espace stable (cf. Théorème 31).

II - Application à la réduction d'endomorphismes

1. Diagonalisation et trigonalisation

Définition 25. On dit que $\lambda \in \mathbb{K}$ est **valeur propre** de u s'il existe $x \neq 0$ tel que $u(x) = \lambda x$. x est alors un **vecteur propre** de u associé à λ. Le sous-espace

$$E_\lambda = \{x \in E \mid u(x) = \lambda x\} = \operatorname{Ker}(u - \lambda \operatorname{Id})$$

est le **sous-espace propre** associé à λ.

p. 171

Définition 26. On dit que u est **diagonalisable** (resp. **trigonalisable**) s'il existe une base $\mathscr{B}$ de E telle que $\operatorname{Mat}(u, \mathscr{B})$ soit diagonale (resp. triangulaire supérieure).

Théorème 27. Les assertions suivantes sont équivalentes :

(i) u est diagonalisable.

(ii) π_u est scindé à racines simples.

(iii) χ_u est scindé et, pour toute valeur propre λ, la dimension du sous-espace propre E_λ est égale à la multiplicité de λ dans χ_u.

(iv) E est somme directe des sous-espaces propres de u.

[BMP] p. 165

Exemple 28.
— Soit $p \in \mathscr{L}(E)$ tel que $p^2 = p$. Alors p est annulé par $X^2 - X$ donc est diagonalisable et à valeurs propres dans $\{0, 1\}$.
— Soit $s \in \mathscr{L}(E)$ tel que $s^2 = \mathrm{id}_E$. Alors si $\operatorname{car}(\mathbb{K}) \neq 2$, s est annulé par $X^2 - 1$ donc est diagonalisable et à valeurs propres dans $\{\pm 1\}$.

Théorème 29. Les assertions suivantes sont équivalentes :

(i) u est trigonalisable.

(ii) π_u est scindé.

(iii) χ_u est scindé.

Exemple 30. Si $\mathbb{K}$ est algébriquement clos, tout endomorphisme de E est trigonalisable.

[DEV]

Théorème 31. Soit $(u_i)_{i\in I}$ une famille d'endomorphismes telle que $\forall i,j \in I,\ u_i u_j = u_j u_i$. Si tous les u_i sont trigonalisables (resp. diagonalisables), on peut co-trigonaliser (resp. co-diagonaliser) la famille $(u_i)_{i\in I}$.

Remarque 32. Dans le cas de la diagonalisabilité, cette condition est à la fois nécessaire et suffisante.

Proposition 33. On suppose que u est diagonalisable. Soit F un sous-espace de E stable par u. Alors $u_{|F}$ est diagonalisable.

[GOU21] p. 174

Application 34. Les assertions suivantes sont équivalentes :

(i) u est trigonalisable avec des zéros sur la diagonale.

(ii) u est nilpotent (ie. $\exists m \in \mathbb{N}$ tel que $u^m = 0$).

(iii) $\chi_u = X^n$.

(iv) $\pi_u = X^p$ où p est l'indice de nilpotence de u.

[BMP] p. 170

2. Décomposition de Dunford

[DEV]

Théorème 35 (Décomposition de Dunford)**.** On suppose que π_u est scindé sur $\mathbb{K}$. Alors il existe un unique couple d'endomorphismes (d,n) tels que :

— d est diagonalisable et n est nilpotent.

— $u = d + n$.

— $dn = nd$.

[GOU21] p. 203

Corollaire 36. Si u vérifie les hypothèse précédentes, pour tout $k \in \mathbb{N}$, $u^k = (d+n)^k = \sum_{i=0}^{m} \binom{k}{i} d^i n^{k-i}$, avec $m = \min(k,l)$ où l désigne l'indice de nilpotence de n.

Remarque 37.

— Un autre intérêt est le calcul d'exponentielles de matrices.

— On peut montrer de plus que d et n sont des polynômes en u.

3. Réduction de Jordan

Définition 38. Un **bloc de Jordan** de taille m associé à $\lambda \in \mathbb{K}$ désigne la matrice $J_m(\lambda)$ suivante : [BMP] p. 171

$$J_m(\lambda) = \begin{pmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{pmatrix} \in \mathcal{M}_m(\mathbb{K})$$

Proposition 39. Les assertions suivantes sont équivalentes :

(i) Il existe une base de E telle que la matrice de u est $J_n(0)$.

(ii) u est nilpotent et cyclique (voir Théorème 43).

(iii) u est nilpotent d'indice de nilpotence n.

Théorème 40 (Réduction de Jordan d'un endomorphisme nilpotent)**.** On suppose que u est nilpotent. Alors il existe des entiers $n_1 \geq \cdots \geq n_p$ et une base $\mathcal{B}$ de E tels que :

$$\mathrm{Mat}(u, \mathcal{B}) = \begin{pmatrix} J_{n_1}(0) & & \\ & \ddots & \\ & & J_{n_p}(0) \end{pmatrix}$$

De plus, on a unicité dans cette décomposition.

Remarque 41. Comme l'indice de nilpotence d'un bloc de Jordan est égal à sa taille, l'indice de nilpotence de u est la plus grande des tailles des blocs de Jordan de la réduite.

Théorème 42 (Réduction de Jordan d'un endomorphisme)**.** On suppose que le polynôme caractéristique de u est scindé sur $\mathbb{K}$: [GOU21] p. 209

$$\chi_u = \prod_{i=1}^{p} (X - \lambda_i)^{\alpha_i} \text{ où les } \lambda_i \text{ sont distincts deux-à-deux}$$

Alors il existe des entiers $n_1 \geq \cdots \geq n_p$ et une base $\mathcal{B}$ de E tels que :

$$\mathrm{Mat}(u, \mathcal{B}) = \begin{pmatrix} J_{n_1}(\lambda_1) & & \\ & \ddots & \\ & & J_{n_p}(\lambda_p) \end{pmatrix}$$

De plus, on a unicité dans cette décomposition.

4. Réduction de Frobenius

p. 397

Définition 43. On dit que u est **cyclique** s'il existe $x \in E$ tel que $\{P(u)(x) \mid P \in \mathbb{K}[X]\} = E$.

Proposition 44. u est cyclique si et seulement si $\deg(\pi_u) = n$.

Définition 45. Soit $P = X^p + a_{p-1}X^{p-1} + \cdots + a_0 \in \mathbb{K}[X]$. On appelle **matrice compagnon** de P la matrice

$$\mathscr{C}(P) = \begin{pmatrix} 0 & \dots & \dots & 0 & -a_0 \\ 1 & 0 & \ddots & \vdots & -a_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{p-2} \\ 0 & \dots & 0 & 1 & -a_{p-1} \end{pmatrix}$$

Proposition 46. u est cyclique si et seulement s'il existe une base $\mathscr{B}$ de E telle que $\mathrm{Mat}(u, \mathscr{B}) = \mathscr{C}(\pi_u)$.

Théorème 47. Il existe $F_1, \dots, F_r$ des sous-espaces vectoriels de E tous stables par u tels que :

— $E = F_1 \oplus \cdots \oplus F_r$.

— $u_i = u_{|F_i}$ est cyclique pour tout i.

— Si $P_i = \pi_{u_i}$, on a $P_{i+1} \mid P_i$ pour tout i.

La famille de polynômes $P_1, \dots, P_r$ ne dépend que de u et non du choix de la décomposition. On l'appelle **suite des invariants de similitude** de u.

Théorème 48 (Réduction de Frobenius)**.** Si $P_1, \dots, P_r$ désigne la suite des invariants de u, alors il existe une base $\mathscr{B}$ de E telle que :

$$\mathrm{Mat}(u, \mathscr{B}) = \begin{pmatrix} \mathscr{C}(P_1) & & \\ & \ddots & \\ & & \mathscr{C}(P_r) \end{pmatrix}$$

On a d'ailleurs $P_1 = \pi_u$ et $P_1 \dots P_r = \chi_u$.

Corollaire 49. Deux endomorphismes de E sont semblables si et seulement s'ils ont la même suite d'invariants de similitude.

Application 50. Toute matrice est semblable à sa transposée.

III - Endomorphismes remarquables

1. Endomorphismes normaux

Soit E un espace vectoriel sur $\mathbb{C}$ de dimension finie n. On munit E d'un produit scalaire $\langle .,. \rangle$, qui en fait un espace hermitien.

Notation 51. On note u^* **l'adjoint** de u.

[GRI] p. 286

Définition 52. Un endomorphisme $u \in \mathscr{L}(E)$ est dit **normal** s'il est tel que $u \circ u^* = u^* \circ u$.

Proposition 53. On suppose u normal. Soit $\lambda \in \mathbb{C}$ une valeur propre de u. Alors :

(i) $E_\lambda^\perp = \{x \in E^\lambda \mid \forall y \in E^\lambda, \langle x, y \rangle = 0\}$ est stable par u.

(ii) $u_{|E_\lambda^\perp}$ est normal.

Corollaire 54. On suppose u normal. Alors u est diagonalisable dans une base orthonormée.

2. Sous-représentations

Soit G un groupe d'ordre fini.

[ULM21] p. 144

Définition 55.
- Une **représentation linéaire** ρ est un morphisme de G dans $\mathrm{GL}(V)$ où V désigne un espace-vectoriel de dimension finie n sur $\mathbb{C}$.
- On dit que n est le **degré** de ρ.
- On dit que ρ est **irréductible** si $V \neq \{0\}$ et si aucun sous-espace vectoriel de V n'est stable par $\rho(g)$ pour tout $g \in G$, hormis $\{0\}$ et V.

Exemple 56. Soit $\varphi : G \to S_n$ le morphisme structurel d'une action de G sur un ensemble de cardinal n. On obtient une représentation de G sur $\mathbb{C}^n = \{e_1, \dots, e_n\}$ en posant

$$\rho(g)(e_i) = e_{\varphi(g)(i)}$$

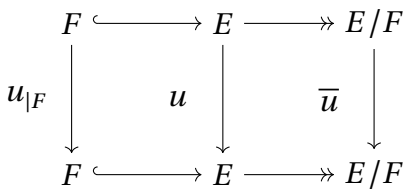
c'est la représentation par permutations de G associé à l'action. Elle est de degré n.

Définition 57. La représentation par permutations de G associée à l'action par translation à gauche de G sur lui-même est la **représentation régulière** de G, on la note ρ_G.

Définition 58. Soit $\rho : G \to \mathrm{GL}(V)$ une représentation linéaire de G. On suppose $V = W \oplus W_0$ avec W et W_0 stables par $\rho(g)$ pour tout $g \in G$. On dit alors que ρ est **somme directe** de ρ_W et de ρ_{W_0}.

Théorème 59 (Maschke)**.** Toute représentation linéaire de G est somme directe de représentations irréductibles.

Annexes



[BMP] p. 158

FIGURE I.6 – Endomorphismes induits par u sur un sous-espace stable F.

p. 157

u	Diagonalisable	Trigonalisable	Quelconque
Décomposition	de E suivant les vecteurs propres	de Dunford	de Frobenius
Sous-espace stable F	espace propre	espace caractéristique	engendré par un élément
$u_{\|F}$	homothétie	homothétie + nilpotent	cyclique

FIGURE I.7 – Réduction d'un endomorphisme en fonction de ses propriétés.

152 Endomorphismes diagonalisables en dimension finie.

Soit E un espace vectoriel sur un corps $\mathbb{K}$ de dimension finie n. Soit $u \in \mathscr{L}(E)$ un endomorphisme de E.

I - Spectre d'un endomorphisme

1. Valeurs propres, vecteurs propres

Définition 1. Soit $\lambda \in \mathbb{K}$. [GOU21] p. 171

- On dit que λ est **valeur propre** de u si $u - \lambda \mathrm{id}_E$ est non injective.
- Un vecteur $x \neq 0$ tel que $u(x) = \lambda x$ est un **vecteur propre** de u associé à la valeur propre λ.
- $E_\lambda = \mathrm{Ker}(u - \lambda \mathrm{id}_E)$ est le **sous-espace propre** associé à la valeur propre λ.
- L'ensemble des valeurs propres de u est appelé **spectre** de u. On le note $\mathrm{Sp}(u)$.

Remarque 2.
- 0 est valeur propre de u si et seulement si $\mathrm{Ker}(f) \neq \{0\}$.
- On peut définir de la même manière les mêmes notions pour une matrice de $\mathscr{M}_n(\mathbb{K})$ (une valeur est propre pour une matrice si et seulement si elle l'est pour l'endomorphisme associé). On reprendra les mêmes notations.
- Les sous-espaces E_λ sont stables par u pour toute valeur propre λ.

Exemple 3. $\begin{pmatrix}1\\1\\1\end{pmatrix}$ est vecteur propre de $\begin{pmatrix}0 & 2 & -1\\3 & -2 & 0\\-2 & 2 & 1\end{pmatrix}$ associé à la valeur propre 1.

Théorème 4. Soient $\lambda_1, \dots, \lambda_k$ des valeurs propres de u, distinctes deux à deux. Alors les sous-espaces propres $E_{\lambda_1}, \dots, E_{\lambda_k}$ sont en somme directe.

Théorème 5. Soit $P \in \mathbb{K}[X]$. Pour tout valeur propre λ de u, $P(\lambda)$ est une valeur propre de $P(u)$. Si le corps $\mathbb{K}$ est algébriquement clos, on a alors [ROM21] p. 604

$$\mathrm{Sp}(P(u)) = \{P(\lambda) \mid \lambda \in \mathrm{Sp}(u)\}$$

Contre-exemple 6. Pour $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathcal{M}_2(\mathbb{R})$ et $P = X^2$, on a $A^2 = -I_2$ et $\mathrm{Sp}(A) = \emptyset$.

2. Polynôme caractéristique

Proposition 7. En notant $\chi_u = \det(X\,\mathrm{id}_E - u)$, p. 644

$$\mathrm{Sp}(u) = \{\lambda \in \mathbb{K} \mid \chi_u(\lambda) = 0\}$$

Définition 8. Le polynôme χ_u précédent est appelé **polynôme caractéristique** de u.

Remarque 9. On peut définir la même notion pour une matrice $A \in \mathcal{M}_n(\mathbb{K})$, ces deux notions coïncidant bien si A est la matrice de u dans une base quelconque de E.

Exemple 10. Pour $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{K})$, on a $\chi_A = X^2 - \mathrm{trace}(A)X + \det(A)$.

Proposition 11. Soit λ une valeur propre de u de multiplicité α en tant que racine de χ_u. Alors,

$$\dim(E_\lambda) \in [\![1, \alpha]\!]$$

Proposition 12. [GOU21] p. 172

(i) Le polynôme caractéristique est un invariant de similitude.

(ii) Soit $A \in \mathcal{M}_n(\mathbb{K})$. On note $\chi_A = \sum_{k=0}^{n} a_k X^k$. Alors, $a_0 = \det(A)$ et $a_{n-1} = \mathrm{trace}(A)$ (à un signe près).

3. Polynôme minimal

Lemme 13. [ROM21] p. 604

(i) $\mathrm{Ann}(u) = \{P \in \mathbb{K}[X] \mid P(u) = 0\}$ est un sous-ensemble de $\mathbb{K}[u]$ non réduit au polynôme nul.

(ii) $\mathrm{Ann}(u)$ est le noyau de $P \mapsto P(u)$: c'est un idéal de $\mathbb{K}[u]$.

(iii) Il existe un unique polynôme unitaire engendrant cet idéal.

Définition 14. On appelle **idéal annulateur** de u l'idéal $\mathrm{Ann}(u)$. Le polynôme unitaire générateur est noté π_u et est appelé **polynôme minimal** de u.

Remarque 15. — π_u est le polynôme unitaire de plus petit degré annulant u.
— Si $A \in \mathcal{M}_n(\mathbb{K})$ est la matrice de u dans une base de E, on a $\mathrm{Ann}(u) = \mathrm{Ann}(A)$ et $\pi_u = \pi_A$.

Exemple 16. Un endomorphisme est nilpotent d'indice q si et seulement si son polynôme minimal est X^q.

Proposition 17. Soit F un sous-espace vectoriel de E stable par u. Alors, le polynôme minimal de l'endomorphisme $u_{|F} : F \to F$ divise π_u.

Proposition 18. (i) Les valeurs propres de u sont racines de tout polynôme annulateur.
(ii) Les valeurs propres de u sont exactement les racines de π_u.

Remarque 19. π_u et χ_u partagent dont les mêmes racines. **[GOU21]** p. 186

Théorème 20 (Cayley-Hamilton)**.** **[ROM21]** p. 607

$$\pi_u \mid \chi_u$$

Corollaire 21.

$$\dim(\mathbb{K}[u]) \leq n$$

II - Diagonalisabilité

1. Définition

Définition 22. — On dit que u est **diagonalisable** s'il existe une base de E dans laquelle la matrice de u est diagonale. p. 683
— On dit qu'une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est **diagonalisable** si elle est semblable à une matrice diagonale.

Remarque 23. u est diagonalisable si et seulement si sa matrice dans n'importe quelle base de E l'est.

Exemple 24. — Les projecteurs (ie. les endomorphismes $p \in \mathcal{L}(E)$ tels que $p^2 = p$) sont toujours diagonalisables, à valeurs propres dans $\{0, 1\}$. **[BMP]** p. 166
— Les symétries (ie. les endomorphismes $s \in \mathcal{L}(E)$ tels que $s^2 = \mathrm{id}_E$) sont toujours diagonalisables, à valeurs propres dans $\{\pm 1\}$. Par exemple, l'endomorphisme de trans-

position $A \mapsto {}^tA$ est diagonalisable.

2. Critères

Proposition 25. Si u a n valeurs propres distinctes dans $\mathbb{K}$, alors il est diagonalisable. [ROM21] p. 683

Théorème 26 (Lemme des noyaux)**.** Soit $P = P_1 \dots P_k \in \mathbb{K}[X]$ où les polynômes $P_1, \dots, P_k$ sont premiers entre eux deux à deux. Alors, p. 609

$$\mathrm{Ker}(P(u)) = \bigoplus_{i=1}^{k} \mathrm{Ker}(P_i(u))$$

Théorème 27. Soit $\mathrm{Sp}(u) = \{\lambda_1, \dots, \lambda_p\}$. Les assertions suivantes sont équivalentes : p. 683

(i) u est diagonalisable sur $\mathbb{K}$.

(ii) $E = \bigoplus_{k=1}^{p} E_{\lambda_k}$.

(iii) $\sum_{k=1}^{p} \dim(E_{\lambda_k}) = n$.

(iv) χ_n est scindé sur $\mathbb{K}$ et pour tout $k \in [\![1, p]\!]$, la dimension de E_{λ_k} est égale à la multiplicité de λ_k dans χ_u.

(v) $\exists P \in \mathrm{Ann}(u)$ scindé à racines simples.

(vi) π_u est scindé à racines simples.

Exemple 28. $\begin{pmatrix} 0 & 2 & -1 \\ 3 & -2 & 0 \\ -2 & 2 & 1 \end{pmatrix}$ est diagonalisable, semblable à $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -4 \end{pmatrix}$. [GOU21] p. 177

Corollaire 29. Sur $\mathbb{K} = \mathbb{F}_q$, u est diagonalisable si et seulement si $u^q = u$. p. 188

Théorème 30 (Diagonalisation simultanée)**.** Soit $(u_i)_{i \in I}$ une famille d'endomorphismes de E diagonalisables. Il existe une base commune de diagonalisation dans E pour $(u_i)_{i \in I}$ si et seulement si ces endomorphismes commutent deux-à-deux. p. 176

Remarque 31. La réciproque est vraie.

3. Exemples d'endomorphismes diagonalisables dans un espace euclidien ou hermitien

On se place dans le cas où $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.Si $\mathbb{K} = \mathbb{R}$, on munit E d'un produit scalaire $\langle .,. \rangle$. Si $\mathbb{K} = \mathbb{C}$, on munit E d'un produit scalaire hermitien $\langle .,. \rangle$.

a. Endomorphismes autoadjoints

Lemme 32. Il existe un unique $u^* \in \mathscr{L}(E)$ tel que

$$\forall x, y \in E, \langle u(x), y \rangle = \langle x, u^*(y) \rangle$$

[GOU21] p. 255

Définition 33. L'endomorphisme u^* précédent est **l'adjoint** de u. On dit que u est **autoadjoint** si $u = u^*$.

Proposition 34. Soit $v \in \mathscr{L}(E)$. Alors $v = u^*$ si et seulement si la matrice de v dans une base orthonormée $\mathscr{B}$ de E est la transposée (transconjuguée dans le cas hermitien) de la matrice de u dans $\mathscr{B}$.

Théorème 35. Tout endomorphisme autoadjoint se diagonalise dans une base orthonormée, ses valeurs propres étant réelles.

Lemme 36.

$$\forall A \in \mathscr{S}_n^{++}(\mathbb{R}) \, \exists! B \in \mathscr{S}_n^{++}(\mathbb{R}) \text{ telle que } B^2 = A$$

[C-G] p. 376

[DEV]

Application 37 (Décomposition polaire)**.** L'application

$$\mu : \begin{array}{ccc} \mathscr{O}_n(\mathbb{R}) \times \mathscr{S}_n^{++}(\mathbb{R}) & \to & \mathrm{GL}_n(\mathbb{R}) \\ (O, S) & \mapsto & OS \end{array}$$

est un homéomorphisme.

b. Endomorphismes normaux

On suppose dans toute cette sous-section que $\mathbb{K} = \mathbb{C}$.

Définition 38. u est dit **normal** s'il est tel que $u \circ u^* = u^* \circ u$.

[GRI] p. 286

Proposition 39. On suppose u normal. Soit $\lambda \in \mathbb{C}$ une valeur propre de u. Alors :

(i) $E_\lambda^\perp = \{x \in E^\lambda \mid \forall y \in E^\lambda, \langle x, y\rangle = 0\}$ est stable par u.

(ii) $u_{|E_\lambda^\perp}$ est normal.

Corollaire 40. On suppose u normal. Alors u est diagonalisable dans une base orthonormée.

4. Topologie

Proposition 41. L'ensemble $\mathcal{D}_n(\mathbb{C})$ des matrices diagonalisables à coefficients complexes est dense dans $\mathcal{M}_n(\mathbb{C})$.

[BMP] p. 179

Application 42. L'application qui à une matrice $M \in \mathcal{M}_n(\mathbb{C})$ associe la partie diagonalisable de sa décomposition de Dunford $M = D + N$ n'est pas continue.

Application 43.

$$\forall U \in \mathcal{M}_n(\mathbb{C}),\ \chi_U(U) = 0$$

p. 217

III - Applications

1. Réduction

[DEV]

Théorème 44 (Décomposition de Dunford)**.** On suppose que π_u est scindé sur $\mathbb{K}$. Alors il existe un unique couple d'endomorphismes (d, n) tels que :

— d est diagonalisable et n est nilpotent.

— $u = d + n$.

— $dn = nd$.

[GOU21] p. 203

Corollaire 45. Si u vérifie les hypothèse précédentes, pour tout $k \in \mathbb{N}$, $u^k = (d+n)^k = \sum_{i=0}^{m} \binom{k}{i} d^i n^{k-i}$, avec $m = \min(k, l)$ où l désigne l'indice de nilpotence de n.

Remarque 46. On peut montrer de plus que d et n sont des polynômes en u.

2. Calcul d'exponentielles

Lemme 47. (i) La série entière $\sum \frac{z^k}{k!}$ a un rayon de convergence infini.
(ii) $\sum \frac{A^k}{k!}$ est convergente pour toute matrice $A \in \mathcal{M}_n(\mathbb{K})$.

[ROM21] p. 761

Définition 48. Soit $A \in \mathcal{M}_n(\mathbb{K})$. On définit **l'exponentielle** de A par

$$\sum_{k=0}^{+\infty} \frac{A^k}{k!}$$

on la note aussi $\exp(A)$ ou e^A.

Théorème 49. Soit $A \in \mathcal{M}_n(\mathbb{K})$.
(i) Si $A = \mathrm{Diag}(\lambda_1, \dots, \lambda_n)$, alors $\exp(A) = \mathrm{Diag}(e_1^\lambda, \dots, e_n^\lambda)$.
(ii) Si $B = PAP^{-1}$ pour $P \in \mathrm{GL}_n(\mathbb{K})$, alors $e^B = P^{-1}e^A P$.
(iii) $\det(e^A) = e^{\mathrm{trace}(A)}$.
(iv) $t \mapsto e^{tA}$ est de classe $\mathcal{C}^\infty$, de dérivée $t \mapsto e^{tA}A$.

Proposition 50. Soient $A, B \in \mathcal{M}_n(\mathbb{K})$ qui commutent. Alors,

$$e^A e^B = e^{A+B} = e^B e^A$$

Exemple 51. Soit $A \in \mathcal{M}_n(\mathbb{K})$ qui admet une décomposition de Dunford $A = D + N$ où D est diagonalisable et N est nilpotente d'indice q. Alors,
— $e^A = e^D e^N = e^D \sum_{k=0}^{q-1} \frac{N^k}{k!}$.
— La décomposition de Dunford de e^A est $e^A = e^D + e^D(e^N - I_n)$ avec e^D diagonalisable et $e^D(e^N - I_n)$ nilpotente.

Application 52. Soit $A \in \mathcal{M}_n(\mathbb{K})$ dont le polynôme caractéristique est scindé sur $\mathbb{K}$. Alors A est diagonalisable si et seulement si e^A l'est.

Application 53. Une équation différentielle linéaire homogène $(H) : Y' = AY$ (où A est constante en t) a ses solutions maximales définies sur $\mathbb{R}$ et le problème de Cauchy

$$\begin{cases} Y' = AY \\ Y(0) = y_0 \end{cases}$$

a pour (unique) solution $t \mapsto e^{tA}y_0$.

[GOU20] p. 380

153 Valeurs propres, vecteurs propres. Calculs exacts ou approchés d'éléments propres. Applications.

I - Spectre d'un endomorphisme

Soit E un espace vectoriel sur un corps $\mathbb{K}$ de dimension finie n. Soit $u \in \mathscr{L}(E)$ un endomorphisme de E.

1. Valeurs propres, vecteurs propres

[GOU21] p. 171

Définition 1. Soit $\lambda \in \mathbb{K}$.

- On dit que λ est **valeur propre** de u si $u - \lambda \mathrm{id}_E$ est non injective.
- Un vecteur $x \neq 0$ tel que $u(x) = \lambda x$ est un **vecteur propre** de u associé à la valeur propre λ.
- $E_\lambda = \mathrm{Ker}(u - \lambda \mathrm{id}_E)$ est le **sous-espace propre** associé à la valeur propre λ.
- L'ensemble des valeurs propres de u est appelé **spectre** de u. On le note $\mathrm{Sp}(u)$.

Remarque 2.
- 0 est valeur propre de u si et seulement si $\mathrm{Ker}(f) \neq \{0\}$.
- On peut définir de la même manière les mêmes notions pour une matrice de $\mathscr{M}_n(\mathbb{K})$ (une valeur est propre pour une matrice si et seulement si elle l'est pour l'endomorphisme associé). On reprendra les mêmes notations.
- Les sous-espaces E_λ sont stables par u pour toute valeur propre λ.

Exemple 3. $\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ est vecteur propre de $\begin{pmatrix} 0 & 2 & -1 \\ 3 & -2 & 0 \\ -2 & 2 & 1 \end{pmatrix}$ associé à la valeur propre 1.

Théorème 4. Soient $\lambda_1, \dots, \lambda_k$ des valeurs propres de u, distinctes deux à deux. Alors les sous-espaces propres $E_{\lambda_1}, \dots, E_{\lambda_k}$ sont en somme directe.

[ROM21] p. 604

Théorème 5. Soit $P \in \mathbb{K}[X]$. Pour tout valeur propre λ de u, $P(\lambda)$ est une valeur propre de $P(u)$. Si le corps $\mathbb{K}$ est algébriquement clos, on a alors

$$\mathrm{Sp}(P(u)) = \{P(\lambda) \mid \lambda \in \mathrm{Sp}(u)\}$$

Contre-exemple 6. Pour $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathcal{M}_2(\mathbb{R})$ et $P = X^2$, on a $A^2 = -I_2$ et $\mathrm{Sp}(A) = \emptyset$.

2. Polynôme caractéristique

Proposition 7. En notant $\chi_u = \det(X\,\mathrm{id}_E - u)$, p. 644

$$\mathrm{Sp}(u) = \{\lambda \in \mathbb{K} \mid \chi_u(\lambda) = 0\}$$

Définition 8. Le polynôme χ_u précédent est appelé **polynôme caractéristique** de u.

Remarque 9. On peut définir la même notion pour une matrice $A \in \mathcal{M}_n(\mathbb{K})$, ces deux notions coïncidant bien si A est la matrice de u dans une base quelconque de E.

Exemple 10. Pour $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{K})$, on a $\chi_A = X^2 - \mathrm{trace}(A)X + \det(A)$.

Proposition 11. Soit λ une valeur propre de u de multiplicité α en tant que racine de χ_u. Alors,

$$\dim(E_\lambda) \in [\![1, \alpha]\!]$$

Proposition 12. [GOU21] p. 172
(i) Le polynôme caractéristique est un invariant de similitude.
(ii) Soit $A \in \mathcal{M}_n(\mathbb{K})$. On note $\chi_A = \sum_{k=0}^{n} a_k X^k$. Alors, $a_0 = \det(A)$ et $a_{n-1} = \mathrm{trace}(A)$ (à un signe près).

Lemme 13 (Déterminant circulant)**.** Soient $n \in \mathbb{N}^*$ et $a_1, \dots, a_n \in \mathbb{C}$. On pose $\omega = e^{\frac{2i\pi}{n}}$. Alors p. 153

$$\begin{vmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \dots & a_0 \end{vmatrix} = \prod_{j=0}^{n-1} P(\omega^j)$$

où $P = \sum_{k=0}^{n-1} a_k X^k$.

[DEV]

Application 14 (Suite de polygones)**.** Soit P_0 un polygone dont les sommets sont $\{z_{0,1}, \dots, z_{0,n}\}$. On définit la suite de polygones (P_k) par récurrence en disant que, pour tout $k \in \mathbb{N}^*$, les sommets de P_{k+1} sont les milieux des arêtes de P_k. [I-P] p. 389

Alors la suite (P_k) converge vers l'isobarycentre de P_0.

3. Polynôme minimal

Lemme 15. (i) $\mathrm{Ann}(u) = \{P \in \mathbb{K}[X] \mid P(u) = 0\}$ est un sous-ensemble de $\mathbb{K}[u]$ non réduit au polynôme nul.
(ii) $\mathrm{Ann}(u)$ est le noyau de $P \mapsto P(u)$: c'est un idéal de $\mathbb{K}[u]$.
(iii) Il existe un unique polynôme unitaire engendrant cet idéal.

[ROM21] p. 604

Définition 16. On appelle **idéal annulateur** de u l'idéal $\mathrm{Ann}(u)$. Le polynôme unitaire générateur est noté π_u et est appelé **polynôme minimal** de u.

Remarque 17. — π_u est le polynôme unitaire de plus petit degré annulant u.
— Si $A \in \mathcal{M}_n(\mathbb{K})$ est la matrice de u dans une base de E, on a $\mathrm{Ann}(u) = \mathrm{Ann}(A)$ et $\pi_u = \pi_A$.

Exemple 18. Un endomorphisme est nilpotent d'indice q si et seulement si son polynôme minimal est X^q.

Proposition 19. Soit F un sous-espace vectoriel de E stable par u. Alors, le polynôme minimal de l'endomorphisme $u_{|F} : F \to F$ divise π_u.

Proposition 20. (i) Les valeurs propres de u sont racines de tout polynôme annulateur.
(ii) Les valeurs propres de u sont exactement les racines de π_u.

Remarque 21. π_u et χ_u partagent dont les mêmes racines.

[GOU21] p. 186

Théorème 22 (Cayley-Hamilton)**.**

$$\pi_u \mid \chi_u$$

[ROM21] p. 607

Corollaire 23.

$$\dim(\mathbb{K}[u]) \leq n$$

II - Localisation

Soit $A = (a_{i,j})_{i,j\in[\![1,n]\!]} \in \mathcal{M}_n(\mathbb{C})$.

1. Disques de Gerschgörin

Notation 24. On note :

— Pour tout $i \in [\![1,n]\!]$, $L_i = \sum_{\substack{j=1\\ j\neq i}}^{n} |a_{i,j}|$ et $L = \max_{i\in[\![1,n]\!]}\{L_i + |a_{i,i}|\}$.

— Pour tout $j \in [\![1,n]\!]$, $C_j = \sum_{\substack{i=1\\ i\neq j}}^{n} |a_{i,j}|$ et $C = \max_{j\in[\![1,n]\!]}\{C_j + |a_{j,j}|\}$.

p. 650

Théorème 25 (Gerschgörin-Hadamard)**.** Soit $\lambda \in \mathbb{C}$ une valeur propre de A. Alors, il existe $i \in [\![1,n]\!]$ tel que $|\lambda - a_{i,i}| \leq L_i$.

Remarque 26. Ainsi,

$$\mathrm{Sp}(A) \subseteq \bigcup_{i=1}^{n} \{z \in \mathbb{C} \mid |z - a_{i,i}| \leq L_i\}$$

Les disques de cette réunion sont appelés disques de Gerschgörin.

[FGN2] p. 189

Exemple 27. Soient $a, b \in \mathbb{R}^2$. On pose

$$A(a,b) = \begin{pmatrix} a & b & 0 & \dots & 0 \\ b & a & b & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & b & a & b \\ 0 & \dots & 0 & b & a \end{pmatrix}$$

Alors,

$$\mathrm{Sp}(A(a,b)) = \left\{ a + 2b\cos\left(\frac{k\pi}{n+1}\right) \mid k \in [\![1,n]\!] \right\}$$

[ROM21] p. 672

Exemple 28. Soit

$$A = \begin{pmatrix} 1 & 0 & \dots & 0 & -1 \\ -1 & 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & -1 & 1 & 0 \\ 0 & \dots & 0 & -1 & 1 \end{pmatrix}$$

Alors,

$$\mathrm{Sp}({}^tAA) = \left\{ 4\sin\left(\frac{k\pi}{n}\right)^2 \mid k \in [\![0,n-1]\!] \right\}$$

p. 651

Corollaire 29. Pour toute valeur propre $\lambda \in \mathbb{C}$ de A, on a

$$\lambda \leq \min(L, C)$$

Corollaire 30. On suppose A à diagonale strictement dominante (ie. $\forall i \in [\![1,n]\!]$, $|a_{i,i}| > \sum_{\substack{j=1 \\ j\neq i}}^{n} |a_{i,j}|$). Alors, A est inversible.

Théorème 31 (Ostrowski)**.** Pour tout $\alpha \in [0,1]$ et toute valeur propre $\lambda \in \mathbb{C}$ de A, il existe $i \in [\![1,n]\!]$ tel que

$$|\lambda - a_{i,i}| \leq L_i^{\alpha} C_i^{1-\alpha}$$

Remarque 32. C'est une généralisation du Théorème 25 : pour $\alpha = 1$, on retrouve l'énoncé correspondant.

Corollaire 33. Pour toute valeur propre $\lambda \in \mathbb{C}$ de A, il existe $i \in [\![1,n]\!]$ tel que

$$|\lambda|^2 \leq (L_i + |a_{i,i}|)(C_i + |a_{i,i}|)$$

2. Utilisation du rayon spectral

Notation 34. À toute norme $\|.\|$ sur $\mathbb{C}^n$, on associe la norme matricielle

$$|||.||| : M \mapsto \sup_{x \in \mathbb{C}^n \setminus \{0\}} \frac{\|Mx\|}{\|x\|}$$

Définition 35. Le **rayon spectral** de A, noté $\rho(A)$ est défini par

$$\rho(A) = \max_{\lambda \in \mathrm{Sp}(A)} |\lambda|$$

Théorème 36. On a

$$|||A|||_2 = \sqrt{|||A^* A|||_2} = \sqrt{\rho(A^* A)}$$

où $|||.|||_2$ est la norme matricielle associée à la norme euclidienne sur $\mathbb{C}^n$ et A^* est la trans-conjuguée de A.

Théorème 37. (i) On a $\rho(A) \leq |||A|||$ pour toute norme matricielle $|||.|||$ induite par une norme vectorielle.

(ii) $\rho(A) = \inf_{|||.||| \in \mathcal{N}} |||A|||$ où $\mathcal{N}$ désigne l'ensemble de toutes les normes matricielles induites par une norme vectorielle.

[DEV]

Théorème 38 (Décomposition de Dunford)**.** Soit $f \in \mathcal{E}$ un endomorphisme tel que son polynôme minimal π_f soit scindé sur $\mathbb{K}$. Alors il existe un unique couple d'endomorphismes (d, n) tel que :

— $f = d + n$.

— d est diagonalisable et n est nilpotent.

— $d \circ n = n \circ d$.

[GOU21] p. 203

Corollaire 39 (Théorème de Gelfand)**.** Soit $\|.\|$ une norme sur $\mathcal{M}_n(\mathbb{C})$. Alors,

$$\rho(A) = \lim_{k \to +\infty} \|A^k\|^{\frac{1}{k}}$$

[ROM21] p. 660

Proposition 40. Les conditions suivantes sont équivalentes.

(i) $\lim_{k \to +\infty} A^k = 0$.

(ii) Pour toute valeur initiale $x_0 \in \mathbb{C}^n$, la suite définie par récurrence pour tout $k \in \mathbb{N}$ par $x_{k+1} = Ax_k$, converge vers le vecteur nul.

(iii) $\rho(A) < 1$.

(iv) Il existe au moins une norme matricielle $|||.|||$ induite par une norme vectorielle telle que $|||A||| < 1$.

III - Approximation

Soit $A = (a_{i,j})_{i,j \in [\![1,n]\!]} \in \mathcal{M}_n(\mathbb{R})$.

Théorème 41. On suppose que la valeur propre de A de module maximum est unique. On la note λ_1. Elle est alors réelle est simple, l'espace propre associé est une droite vectorielle et on a

$$\mathbb{R}^n = \mathrm{Ker}(A - \lambda_1 I_n) \oplus \mathrm{Im}(A - \lambda_1 I_n)$$

[ROM19-2] p. 210

On suppose pour la suite que la valeur propre de A de module maximum est unique. On la note λ_1.

Notation 42. On note et on définit :

— $E_1 = \mathrm{Ker}(A - \lambda_1 I_n)$ et $F_1 = \mathrm{Im}(A - \lambda_1 I_n)$.

— $x_0 = e_1 + f_1$ avec $e_1 \in E_1 \setminus \{0\}$ et $f_1 \in F_1$.

— $\forall k \in \mathbb{N}$, $x_{k+1} = \frac{1}{\|Ax_k\|} a_k$ avec $\|.\|$ norme quelconque sur $\mathbb{R}^n$.

— Pour tout $j \in [\![1, n]\!]$, on note $e_{1,j}$ la j-ième composante du vecteur e_1, $x_{k,j}$ celle de x_k et $(Ax_k)_j$ celle de Ax_k.

Théorème 43 (Méthode la puissance itérée)**.** On a :

(i) $\lim_{k\to+\infty} \|Ax_k\| = |\lambda_1| = \rho(A)$.

(ii) $\lim_{k\to+\infty} x_{2k} = v_1$ où v_1 est un vecteur propre non nul associé à la valeur propre λ_1.

(iii) $\lim_{k\to+\infty} x_{2k+1} = \text{signe}(\lambda_1) v_1$.

(iv) Pour tout $j \in [\![1, n]\!]$, tel que $e_{1,j} \neq 0$,

$$\lim_{k\to+\infty} \frac{(Ax_k)_j}{x_{k,j}} = \lambda_1$$

Remarque 44. — Si A est inversible, la méthode précédente appliquée à A^{-1} permet de calculer la valeur propre de plus petit module de A (quand cette dernière est unique).

— En notant e_1 un vecteur propre de A associé à la valeur propre λ_1 de norme euclidienne égale à 1, les valeurs propres de la matrice $B = A - \lambda_1 e_1 {}^t e_1$ sont $0, \lambda_2, \ldots, \lambda_n$. On pourra alors appliquer la méthode à B.

Annexes

[I-P]
p. 389

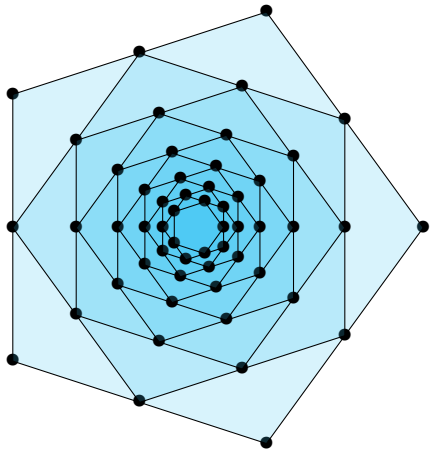


FIGURE I.8 – La suite de polygones.

154 Exemples de décompositions de matrices. Applications.

Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Soit $n \geq 1$.

I - Décomposition et réduction

1. Décomposition de Dunford

a. Décomposition "classique"

[DEV]

Théorème 1 (Décomposition de Dunford)**.** Soit $A \in \mathcal{M}_n(\mathbb{K})$. On suppose que π_A est scindé sur $\mathbb{K}$. Alors il existe un unique couple de matrices (D, N) tels que :

— D est diagonalisable et N est nilpotente.

— $A = D + N$.

— $DN = ND$.

[GOU21] p. 203

Corollaire 2. Si A vérifie les hypothèse précédentes, pour tout $k \in \mathbb{N}$, $A^k = (D+N)^k = \sum_{i=0}^{m} \binom{k}{i} D^i N^{k-i}$, avec $m = \min(k, l)$ où l désigne l'indice de nilpotence de N.

Remarque 3. On peut montrer de plus que D et N sont des polynômes en A.

Exemple 4. On a la décomposition de Dunford suivante :

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

[C-G] p. 165

Contre-exemple 5. L'égalité suivante n'est pas une décomposition de Dunford :

$$\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

car les deux matrices du membre de droite ne commutent pas.

Lemme 6. (i) La série entière $\sum \frac{z^k}{k!}$ a un rayon de convergence infini.

(ii) $\sum \frac{A^k}{k!}$ est convergente pour toute matrice $A \in \mathcal{M}_n(\mathbb{K})$.

[ROM21] p. 761

Définition 7. Soit $A \in \mathcal{M}_n(\mathbb{K})$. On définit **l'exponentielle** de A par

$$\sum_{k=0}^{+\infty} \frac{A^k}{k!}$$

on la note aussi $\exp(A)$ ou e^A.

Théorème 8. Soit $A \in \mathcal{M}_n(\mathbb{K})$.

(i) Si $A = \mathrm{Diag}(\lambda_1, \dots, \lambda_n)$, alors $\exp(A) = \mathrm{Diag}(e_1^\lambda, \dots, e_n^\lambda)$.

(ii) Si $B = PAP^{-1}$ pour $P \in \mathrm{GL}_n(\mathbb{K})$, alors $e^B = P^{-1}e^A P$.

(iii) $\det(e^A) = e^{\mathrm{trace}(A)}$.

(iv) $t \mapsto e^{tA}$ est de classe $\mathscr{C}^\infty$, de dérivée $t \mapsto e^{tA}A$.

Proposition 9. Soient $A, B \in \mathcal{M}_n(\mathbb{K})$ qui commutent. Alors,

$$e^A e^B = e^{A+B} = e^B e^A$$

Exemple 10. Soit $A \in \mathcal{M}_n(\mathbb{K})$ qui admet une décomposition de Dunford $A = D + N$ où D est diagonalisable et N est nilpotente d'indice q. Alors,

— $e^A = e^D e^N = e^D \sum_{k=0}^{q-1} \frac{N^k}{k!}$.

— La décomposition de Dunford de e^A est $e^A = e^D + e^D(e^N - I_n)$ avec e^D diagonalisable et $e^D(e^N - I_n)$ nilpotente.

Application 11. Une équation différentielle linéaire homogène $(H) : Y' = AY$ (où A est constante en t) a ses solutions maximales définies sur $\mathbb{R}$ et le problème de Cauchy

$$\begin{cases} Y' = AY \\ Y(0) = y_0 \end{cases}$$

a pour (unique) solution $t \mapsto e^{tA}y_0$.

[GOU20] p. 380

b. Décomposition multiplicative

Définition 12. On dit qu'une matrice $U \in \mathcal{M}_n(\mathbb{K})$ est **unipotente** si $U - I_n$ est nilpotente.

[ROM21] p. 687

Théorème 13 (Décomposition de Dunford multiplicative)**.** Soit $A \in \mathcal{M}_n(\mathbb{K})$. On suppose que π_A est scindé sur $\mathbb{K}$. Alors il existe un unique couple de matrices (D, U) tels que :

— D est diagonalisable et U est unipotente.

— $A = DU$.

— $DU = UD$.

2. Décomposition de Jordan

Définition 14. Un **bloc de Jordan** de taille m associé à $\lambda \in \mathbb{K}$ désigne la matrice $J_m(\lambda)$ suivante : [BMP] p. 171

$$J_m(\lambda) = \begin{pmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{pmatrix} \in \mathcal{M}_m(\mathbb{K})$$

Proposition 15. Soit $A \in \mathcal{M}_n(\mathbb{K})$. Les assertions suivantes sont équivalentes :

(i) A est semblable à $J_n(0)$.

(ii) A est nilpotente et cyclique (voir Théorème 21).

(iii) A est nilpotente d'indice de nilpotence n.

Théorème 16 (Réduction de Jordan d'un endomorphisme nilpotent)**.** On suppose que A est nilpotente. Alors il existe des entiers $n_1 \geq \cdots \geq n_p$ tels que A est semblable à la matrice

$$\begin{pmatrix} J_{n_1}(0) & & \\ & \ddots & \\ & & J_{n_p}(0) \end{pmatrix}$$

De plus, on a unicité dans cette décomposition.

Remarque 17. Comme l'indice de nilpotence d'un bloc de Jordan est égal à sa taille, l'indice de nilpotence de A est la plus grande des tailles des blocs de Jordan de la réduite.

Théorème 18 (Réduction de Jordan d'un endomorphisme)**.** Soit $A \in \mathcal{M}_n(\mathbb{K})$. On suppose que le polynôme caractéristique de A est scindé sur $\mathbb{K}$: [GOU21] p. 209

$$\chi_A = \prod_{i=1}^{p} (X - \lambda_i)^{\alpha_i} \text{ où les } \lambda_i \text{ sont distincts deux-à-deux}$$

Alors il existe des entiers $n_1 \geq \cdots \geq n_p$ tels que A est semblable à la matrice

$$\begin{pmatrix} J_{n_1}(\lambda_1) & & \\ & \ddots & \\ & & J_{n_p}(\lambda_p) \end{pmatrix}$$

De plus, on a unicité dans cette décomposition.

Application 19. Soit $A \in \mathcal{M}_n(\mathbb{K})$. Alors, A et $2A$ sont semblables si et seulement si A est nilpotente.

Application 20. Soit $A \in \mathcal{M}_n(\mathbb{K})$. Alors, A et ${}^tA$ sont semblables.

3. Décomposition de Frobenius

Soient E un espace vectoriel de dimension finie n et $u \in \mathcal{L}(E)$.

p. 397

Définition 21. On dit que u est **cyclique** s'il existe $x \in E$ tel que $\{P(u)(x) \mid P \in \mathbb{K}[X]\} = E$.

Proposition 22. u est cyclique si et seulement si $\deg(\pi_u) = n$.

Définition 23. Soit $P = X^p + a_{p-1}X^{p-1} + \cdots + a_0 \in \mathbb{K}[X]$. On appelle **matrice compagnon** de P la matrice

$$\mathscr{C}(P) = \begin{pmatrix} 0 & \cdots & \cdots & 0 & -a_0 \\ 1 & 0 & \ddots & \vdots & -a_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{p-2} \\ 0 & \cdots & 0 & 1 & -a_{p-1} \end{pmatrix}$$

Proposition 24. u est cyclique si et seulement s'il existe une base $\mathscr{B}$ de E telle que $\mathrm{Mat}(u, \mathscr{B}) = \mathscr{C}(\pi_u)$.

Théorème 25. Il existe $F_1, \ldots, F_r$ des sous-espaces vectoriels de E tous stables par u tels que :

- $E = F_1 \oplus \cdots \oplus F_r$.
- $u_i = u_{|F_i}$ est cyclique pour tout i.
- Si $P_i = \pi_{u_i}$, on a $P_{i+1} \mid P_i$ pour tout i.

La famille de polynômes $P_1, \ldots, P_r$ ne dépend que de u et non du choix de la décomposition. On l'appelle **suite des invariants de similitude** de u.

Théorème 26 (Réduction de Frobenius)**.** Si $P_1, \dots, P_r$ désigne la suite des invariants de u, alors il existe une base $\mathscr{B}$ de E telle que :

$$\mathrm{Mat}(u, \mathscr{B}) = \begin{pmatrix} \mathscr{C}(P_1) & & \\ & \ddots & \\ & & \mathscr{C}(P_r) \end{pmatrix}$$

On a d'ailleurs $P_1 = \pi_u$ et $P_1 \dots P_r = \chi_u$.

Corollaire 27. Deux endomorphismes de E sont semblables si et seulement s'ils ont la même suite d'invariants de similitude.

Application 28. Pour $n = 2$ ou 3, deux matrices sont semblables si et seulement si elles ont mêmes polynômes minimal et caractéristique.

Application 29. Soit $\mathbb{L}$ une extension de $\mathbb{K}$. Alors, si $A, B \in \mathscr{M}_n(\mathbb{K})$ sont semblables dans $\mathscr{M}_n(\mathbb{L})$, elles le sont aussi dans $\mathscr{M}_n(\mathbb{K})$.

II - Décomposition et résolution de systèmes

1. Décomposition LU

Définition 30. Les **sous-matrices principales** d'une matrice $(a_{i,j})_{i,j\in[\![1,n]\!]} \in \mathscr{M}_n(\mathbb{K})$ sont les matrices $A_k = (a_{i,j})_{i,j\in[\![1,k]\!]} \in \mathscr{M}_k(\mathbb{K})$ où $k \in [\![1, n]\!]$. Les **déterminants principaux** sont les déterminants des matrices A_k, pour $k \in [\![1, n]\!]$.

[ROM21] p. 690

Théorème 31 (Décomposition lower-upper)**.** Soit $A \in \mathrm{GL}_n(\mathbb{K})$. Alors, A admet une décomposition

$$A = LU$$

(où L est une matrice triangulaire inférieure à diagonale unité et U une matrice triangulaire supérieure) si et seulement si tous les déterminants principaux de A sont non nuls. Dans ce cas, une telle décomposition est unique.

Corollaire 32. Soit $A \in \mathrm{GL}_n(\mathbb{K}) \cap \mathscr{S}_n(\mathbb{K})$. Alors, on a l'unique décomposition de A :

$$A = LD^tL$$

où L est une matrice triangulaire inférieure et D une matrice diagonale.

Application 33 (Décomposition de Cholesky)**.** Soit $A \in \mathcal{M}_n(\mathbb{R})$. Alors, $A \in \mathcal{S}_n^{++}(\mathbb{R})$ si et seulement s'il existe $B \in \mathrm{GL}_n(\mathbb{R})$ triangulaire inférieure telle que $A = B^t B$. De plus, une telle décomposition est unique si on impose la positivité des coefficients diagonaux de B.

Exemple 34. On a la décomposition de Cholesky : [GRI] p. 368

$$\begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

Proposition 35. Soit $A \in \mathrm{GL}_n(\mathbb{K})$ vérifiant les hypothèses du Théorème 31. On définit la suite (A_k) où $A_0 = A$ et $\forall k \in \mathbb{N}$, A_{k+1} est la matrice obtenue à partir de A_k à l'aide du pivot de Gauss sur la $(k+1)$-ième colonne. Alors, A_{n-1} est la matrice U de la décomposition $A = LU$ du Théorème 31. [C-G] p. 257

Remarque 36. Pour résoudre un système linéaire $AX = Y$, on se ramène à $A = LU$ en $O\left(\frac{2}{3}n^3\right)$. Puis, on résout deux systèmes triangulaires "en cascade" :

$$LX' = Y \text{ puis } UX = X'$$

ceux-ci demandant chacun $O(2n^2)$ opérations.

Théorème 37 (Décomposition PLU)**.** Soit $A \in \mathrm{GL}_n(\mathbb{K})$. Alors, il existe $P \in \mathrm{GL}_n(\mathbb{K})$, matrice de permutations, telle que $P^{-1}A$ admet une décomposition LU.

2. Décomposition QR

Théorème 38 (Décomposition QR)**.** Soit $A \in \mathrm{GL}_n(\mathbb{R})$. Alors, A admet une décomposition [ROM21] p. 692

$$A = QR$$

où Q est une matrice orthogonale et R est une matrice triangulaire supérieure à coefficients diagonaux strictement positifs. On a unicité d'une telle décomposition.

Corollaire 39 (Théorème d'Iwasawa)**.** Soit $A \in \mathrm{GL}_n(\mathbb{R})$. Alors, A admet une décomposition

$$A = QDR$$

où Q est une matrice orthogonale, D est une matrice diagonale à coefficients strictement positifs et R est une matrice triangulaire supérieure à coefficients diagonaux égaux à 1. On a unicité d'une telle décomposition.

Exemple 40. On a la factorisation QR suivante, [GRI] p. 272

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} = \left(\frac{1}{\sqrt{6}} \begin{pmatrix} 0 & 2 & \sqrt{2} \\ \sqrt{3} & -1 & \sqrt{2} \\ \sqrt{3} & 1 & -\sqrt{2} \end{pmatrix} \right) \left(\frac{1}{\sqrt{6}} \begin{pmatrix} 2\sqrt{3} & \sqrt{3} & 1 \\ 0 & 3 & 1 \\ 0 & 0 & 2\sqrt{2} \end{pmatrix} \right)$$

qui peut être obtenue via un procédé de Gram-Schmidt.

Remarque 41. Pour résoudre un système linéaire $AX = Y$, si l'on a trouvé une telle factorisation $A = QR$, on résout p. 368

$$RX = {}^tQY$$

c'est-à-dire, un seul système triangulaire (contre deux pour la factorisation LU).

III - Décomposition et topologie

Lemme 42. [C-G] p. 376

$$\forall A \in \mathcal{S}_n^{++}(\mathbb{R}) \, \exists ! B \in \mathcal{S}_n^{++}(\mathbb{R}) \text{ telle que } B^2 = A$$

[DEV]

Théorème 43 (Décomposition polaire)**.** L'application

$$\mu : \begin{array}{ccc} \mathcal{O}_n(\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R}) & \to & \mathrm{GL}_n(\mathbb{R}) \\ (O,S) & \mapsto & OS \end{array}$$

est un homéomorphisme.

Corollaire 44. Tout sous-groupe compact de $\mathrm{GL}_n(\mathbb{R})$ qui contient $\mathcal{O}_n(\mathbb{R})$ est $\mathcal{O}_n(\mathbb{R})$.

Corollaire 45. $\mathrm{GL}_n(\mathbb{R})^+$ est connexe. p. 401

155 Exponentielle de matrices. Applications.

I - Construction

Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Soit $n \geq 1$ un entier.

1. Algèbres de Banach

Lemme 1. Pour tout réel positif a, la série $\sum \frac{a^n}{n!}$ est convergente. [DAN] p. 278

Définition 2. Soit $\mathscr{A}$ une algèbre. p. 174

— On dit que $\|.\|$ est une norme d'algèbre sur $\mathscr{A}$ si :

(i) $(\mathscr{A}, \|.\|)$ est un espace vectoriel normé.

(ii) $\forall x, y \in \mathscr{A},\ \|x \times y\| \leq \|x\|\|y\|$.

— Soit $\|.\|$ une norme d'algèbre sur $\mathscr{A}$. Si $(\mathscr{A}, \|.\|)$ est un espace vectoriel complet, on dit que $\mathscr{A}$ est une **algèbre de Banach**.

Proposition 3. Soit $\|.\|$ une norme sur $\mathbb{K}^n$. Muni de la norme p. 183

$$|||.||| : M \mapsto \sup_{x \neq 0} \frac{\|Mx\|}{\|x\|}$$

l'algèbre $(\mathscr{M}_n(\mathbb{K}), |||.|||)$ est une algèbre de Banach.

Contre-exemple 4. Ce n'est pas vrai pour n'importe quelle norme : la norme infinie $\|.\|_\infty$ sur $\mathscr{M}_n(\mathbb{K})$ n'est pas une norme d'algèbre.

Proposition 5. Soit $\mathscr{A}$ une algèbre de Banach unitaire. Pour tout élément $A \in \mathscr{A}$, la série $\sum \frac{A^n}{n!}$ est convergente. p. 278

2. Exponentielle de matrices

Définition 6. Soit $A \in \mathscr{M}_n(\mathbb{K})$. On appelle **exponentielle** de A, et on note $\exp(A)$ ou e^A l'élément de $\mathscr{M}_n(\mathbb{K})$ suivant : p. 345

$$\exp(A) = \sum_{n=0}^{+\infty} \frac{A^n}{n!}$$

p. 356

Exemple 7. Soient $a_1, \dots, a_n \in \mathbb{K}$ et $D = \mathrm{Diag}(a_1, \dots, a_n) \in \mathcal{M}_3(\mathbb{K})$. Alors,

$$\exp(D) = \mathrm{Diag}(e^{a_1}, \dots, e^{a_n})$$

Remarque 8. En particulier, $\exp(0) = I_n$. **[GRI]** p. 378

3. Propriétés

Proposition 9. Soient $A, B \in \mathcal{M}_n(\mathbb{K})$ qui commutent. Alors,

$$e^{A+B} = e^A e^B$$

Corollaire 10. Soit $A \in \mathcal{M}_n(\mathbb{K})$. Alors, $e^A \in \mathrm{GL}_n(\mathbb{K})$ et,

$$\left(e^A\right)^{-1} = e^{-A}$$

Proposition 11. Soient $A, B \in \mathcal{M}_n(\mathbb{K})$ telles que $B = PAP^{-1}$ pour $P \in \mathrm{GL}_n(\mathbb{K})$. Alors,

$$e^{PAP^{-1}} = Pe^A P^{-1}$$

Lemme 12. Soit $A \in \mathcal{M}_n(\mathbb{K})$ une matrice triangulaire supérieure, de la forme $A = \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$. Alors,

$$e^A = \begin{pmatrix} e_1^\lambda & & * \\ & \ddots & \\ & & e_n^\lambda \end{pmatrix}$$

Proposition 13. Soit $A \in \mathcal{M}_n(\mathbb{K})$. Alors, **[ROM21]** p. 762

$$\det(\exp(A)) = e^{\mathrm{trace}(A)}$$

Proposition 14. $\exp : \mathcal{M}_n(\mathbb{K}) \to \mathrm{GL}_n(\mathbb{K})$ est continue. De plus, pour tout $A \in \mathcal{M}_n(\mathbb{K})$, $\exp(A)$ est un polynôme en A.

II - Calcul pratique

Proposition 15. Soit $N \in \mathcal{M}_n(\mathbb{K})$ nilpotente d'indice q. Alors,

$$e^N = \sum_{k=0}^{q-1} \frac{A^k}{k!}$$

[GOU21] p. 206

Théorème 16 (Décomposition de Dunford)**.** Soit $A \in \mathcal{M}_n(\mathbb{K})$. On suppose que π_A est scindé sur $\mathbb{K}$. Alors il existe un unique couple de matrices (D,N) tels que :

— D est diagonalisable et N est nilpotente.

— $A = D + N$.

— $DN = ND$.

Corollaire 17. Si A vérifie les hypothèse précédentes, pour tout $k \in \mathbb{N}$, $A^k = (D+N)^k = \sum_{i=0}^{m} \binom{k}{i} D^i N^{k-i}$, avec $m = \min(k,l)$ où l désigne l'indice de nilpotence de N.

Exemple 18. Soit $A \in \mathcal{M}_n(\mathbb{K})$ qui admet une décomposition de Dunford $A = D + N$ où D est diagonalisable et N est nilpotente d'indice q. Alors,

— $e^A = e^D e^N = e^D \sum_{k=0}^{q-1} \frac{N^k}{k!}$.

— La décomposition de Dunford de e^A est $e^A = e^D + e^D(e^N - I_n)$ avec e^D diagonalisable et $e^D(e^N - I_n)$ nilpotente.

[ROM21] p. 765

Application 19. Soit $A \in \mathcal{M}_n(\mathbb{K})$ dont le polynôme caractéristique est scindé sur $\mathbb{K}$. Alors A est diagonalisable si et seulement si e^A l'est.

Exemple 20. On a

$$\exp\left(\begin{pmatrix} 1 & 4 & -2 \\ 0 & 6 & -3 \\ -1 & 4 & 0 \end{pmatrix}\right) = \begin{pmatrix} -6e^2+3e^3 & -4e^2+4e^3 & 10e^2-6e^3 \\ -6e^2+3e^3 & -3e^2+4e^3 & 9e^2-6e^3 \\ -7e^2+3e^3 & -4e^2+4e^3 & 11e^2-6e^3 \end{pmatrix}$$

[GOU21] p. 209

III - Étude de l'exponentielle de matrices

1. Dérivabilité, différentiabilité

Proposition 21. Soit $A \in \mathcal{M}_n(\mathbb{K})$. L'application $t \mapsto e^{tA}$ est dérivable, de dérivée $t \mapsto Ae^{tA}$.

p. 195

Proposition 22 (Logarithme matriciel)**.** exp est différentiable en 0 et sa différentielle est I_n ; c'est un difféomorphisme local sur un voisinage de 0. Plus précisément, si $H \in \mathcal{M}_n(\mathbb{K})$ telle que $\|\|H\|\| \leq 1$, alors

$$\exp^{-1}(I_n + H) = \sum_{n=1}^{+\infty} (-1)^{n-1} \frac{H^n}{n}$$

On note alors $\ln(H) = \exp^{-1}(H)$.

[C-G] p. 384

Théorème 23. exp est de classe $\mathcal{C}^1$ sur $\mathcal{M}_n(\mathbb{K})$ avec, pour toutes matrices $A, H \in \mathcal{M}_n(\mathbb{K})$:

$$\mathrm{d}\exp_A(H) = \sum_{n=1}^{+\infty} \frac{1}{n!} \left(\sum_{\substack{i,j \in [\![0,n-1]\!] \\ i+j=n-1}} A^i H A^j \right)$$

[ROM21] p. 762

2. Image directe

a. Image de $\mathcal{M}_n(\mathbb{C})$

Exemple 24.

$$\forall k \in \mathbb{Z},\ e^{2ik\pi} = e^0 = 1$$

En particulier, exp n'est pas injective pour $n \geq 1$.

[C-G] p. 387

Lemme 25. Soit $M \in \mathrm{GL}_n(\mathbb{C})$. Alors $M^{-1} \in \mathbb{C}[M]$.

[I-P] p. 396

Théorème 26. $\exp : \mathcal{M}_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$ est surjective.

Application 27. $\exp(\mathcal{M}_n(\mathbb{R})) = \mathrm{GL}_n(\mathbb{R})^2$, où $\mathrm{GL}_n(\mathbb{R})^2$ désigne les carrés de $\mathrm{GL}_n(\mathbb{R})$.

Application 28. $\mathrm{GL}_n(\mathbb{C})$ est connexe par arcs.

[ROM21] p. 770

b. Image de $\mathcal{M}_n(\mathbb{R})$

Exemple 29.
$$\forall k \in \mathbb{Z}, \exp\left(\begin{pmatrix} 0 & -2k\pi \\ 2k\pi & 0 \end{pmatrix}\right) = \exp(0) = I_2$$
En particulier, exp n'est pas injective pour $n \geq 2$.

[C-G] p. 387

Proposition 30. En fait,
$$\exp(\mathcal{M}_n(\mathbb{R})) = \{M^2 \mid M \in \mathcal{M}_n(\mathbb{R})\}$$

Exemple 31. La matrice $\begin{pmatrix} -1 & 0 \\ 0 & -2 \end{pmatrix}$ n'est pas dans l'image de l'exponentielle réelle.

c. Images de $\mathcal{S}_n(\mathbb{R})$ et $\mathcal{H}_n(\mathbb{C})$

Lemme 32. Soit $M \in \mathcal{S}_n(\mathbb{R})$. Alors,
$$|||M||| = \rho(M)$$
où ρ est l'application qui a une matrice y associe son rayon spectral.

[I-P] p. 182

[DEV]

Théorème 33. L'application $\exp : \mathcal{S}_n(\mathbb{R}) \to \mathcal{S}_n^{++}(\mathbb{R})$ est un homéomorphisme.

Remarque 34. On a le même résultat pour $\exp : \mathcal{H}_n(\mathbb{C}) \to \mathcal{H}_n^{++}(\mathbb{C})$.

[C-G] p. 385

Application 35. On a des homéomorphismes :
$$\mathrm{GL}_n(\mathbb{R}) \sim \mathcal{O}_n(\mathbb{R}) \times \mathbb{R}^{\frac{n(n+1)}{2}} \text{ et } \mathrm{GL}_n(\mathbb{C}) \sim \mathcal{U}_n(\mathbb{C}) \times \mathbb{R}^{n^2}$$

d. Image du cône nilpotent $\mathcal{N}_n(\mathbb{C})$

Notation 36. On note $\mathcal{N}_n(\mathbb{C})$ le sous-ensemble de $\mathcal{M}_n(\mathbb{C})$ formé des matrices nilpotentes et $\mathcal{L}_n(\mathbb{C}) = \mathcal{N}_n(\mathbb{C}) - I_n$ le sous-ensemble de $\mathcal{M}_n(\mathbb{C})$ formé des matrices unipotentes.

[ROM21] p. 766

Proposition 37. Soit $A \in \mathcal{N}_n(\mathbb{C})$. Alors $e^A \in \mathcal{L}_n(\mathbb{C})$ et $\ln(e^{tA}) = tA$ pour tout $t \in \mathbb{R}$.

Théorème 38. L'exponentielle matricielle réalise une bijection de $\mathcal{N}_n(\mathbb{C})$ sur $\mathcal{L}_n(\mathbb{C})$ d'inverse le logarithme matriciel défini à la Théorème 22.

IV - Applications

1. Équations différentielles

Théorème 39 (Cauchy-Lipschitz linéaire)**.** Soient $A : I \to \mathcal{M}_n(\mathbb{K})$ et $B : I \to \mathbb{K}^d$ deux fonctions continues. Alors $\forall t_0 \in I$, le problème de Cauchy

$$\begin{cases} Y' = A(t)Y + B(t) \\ Y(t_0) = y_0 \end{cases}$$

admet une unique solution définie sur I tout entier.

[GOU20] p. 376

Proposition 40. Une équation différentielle linéaire homogène $Y' = AY$ (où $A \in \mathcal{M}_n(\mathbb{R})$ est constante en t) a ses solutions maximales définies sur $\mathbb{R}$ et le problème de Cauchy

$$\begin{cases} Y' = AY \\ Y(0) = y_0 \end{cases}$$

a pour (unique) solution $t \mapsto e^{tA}y_0$.

Exemple 41. Les solutions de

$$Y' = \begin{pmatrix} 1 & 0 & 1 \\ 0 & -1 & -1 \\ 0 & 2 & 1 \end{pmatrix} Y$$

sont les

$$t \mapsto \alpha e^t \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \beta e^{it} \begin{pmatrix} 1+i \\ 1-i \\ -2 \end{pmatrix} + \gamma e^{-it} \begin{pmatrix} 1-i \\ 1+i \\ -2 \end{pmatrix}$$

où $\alpha, \beta, \gamma \in \mathbb{C}$.

2. Équations matricielles

Lemme 42. Soit $\|.\|$ une norme d'algèbre sur $\mathcal{M}_n(\mathbb{C})$, et soit $A \in \mathcal{M}_n(\mathbb{C})$ une matrice dont les valeurs propres sont de partie réelle strictement négative. Alors il existe une fonction polynômiale $P : \mathbb{R} \to \mathbb{R}$ et $\lambda > 0$ tels que $\|e^{tA}\| \leq e^{-\lambda t} P(t)$.

[I-P] p. 177

[DEV]

Application 43 (Équation de Sylvester)**.** Soient A et $B \in \mathcal{M}_n(\mathbb{C})$ deux matrices dont les valeurs propres sont de partie réelle strictement négative. Alors pour tout $C \in \mathcal{M}_n(\mathbb{C})$, l'équation $AX + XB = C$ admet une unique solution X dans $\mathcal{M}_n(\mathbb{C})$.

156 Endomorphismes trigonalisables. Endomorphismes nilpotents.

Soit E un espace vectoriel de dimension finie n sur un corps $\mathbb{K}$. Tout au long de la leçon, on abusera du fait que $\mathscr{L}(E) \cong \mathscr{M}_n(\mathbb{K})$: les notions définies pour les endomorphismes sont valables pour les matrices.

I - Endomorphismes trigonalisables

1. Premiers outils de réduction

Définition 1. Soient $u \in \mathscr{L}(E)$ et $\lambda \in \mathbb{K}$. [GOU21] p. 171

- On dit que λ est **valeur propre** de u si $u - \lambda \mathrm{id}_E$ est non injective.
- Un vecteur $x \neq 0$ tel que $u(x) = \lambda x$ est un **vecteur propre** de u associé à la valeur propre λ.
- L'ensemble des valeurs propres de u est appelé **spectre** de u. On le note $\mathrm{Sp}(u)$.

Remarque 2. Soit $u \in \mathscr{L}(E)$.

- 0 est valeur propre de u si et seulement si $\mathrm{Ker}(f) \neq \{0\}$.
- On peut définir de la même manière les mêmes notions pour une matrice de $\mathscr{M}_n(\mathbb{K})$ (une valeur est propre pour une matrice si et seulement si elle l'est pour l'endomorphisme associé). On reprendra les mêmes notations.

Exemple 3. $\begin{pmatrix}1\\1\\1\end{pmatrix}$ est vecteur propre de $\begin{pmatrix}0 & 2 & -1\\3 & -2 & 0\\-2 & 2 & 1\end{pmatrix}$ associé à la valeur propre 1.

Proposition 4. Soit $u \in \mathscr{L}(E)$. En notant $\chi_u = \det(X\mathrm{id}_E - u)$, [ROM21] p. 644

$$\mathrm{Sp}(u) = \{\lambda \in \mathbb{K} \mid \chi_u(\lambda) = 0\}$$

Définition 5. Le polynôme χ_u précédent est appelé **polynôme caractéristique** de u.

Remarque 6. On peut définir la même notion pour une matrice $A \in \mathscr{M}_n(\mathbb{K})$, ces deux notions coïncidant bien si A est la matrice de u dans une base quelconque de E.

Exemple 7. Pour $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{K})$, on a $\chi_A = X^2 - \text{trace}(A)X + \det(A)$.

Lemme 8. Soit $u \in \mathcal{L}(E)$. p. 604

(i) $\text{Ann}(u) = \{P \in \mathbb{K}[X] \mid P(u) = 0\}$ est un sous-ensemble de $\mathbb{K}[u]$ non réduit au polynôme nul.

(ii) $\text{Ann}(u)$ est le noyau de $P \mapsto P(u)$: c'est un idéal de $\mathbb{K}[u]$.

(iii) Il existe un unique polynôme unitaire engendrant cet idéal.

Définition 9. On appelle **idéal annulateur** de u l'idéal $\text{Ann}(u)$. Le polynôme unitaire générateur est noté π_u et est appelé **polynôme minimal** de u.

Remarque 10. En reprenant les notations précédentes,

— π_u est le polynôme unitaire de plus petit degré annulant u.

— Si $A \in \mathcal{M}_n(\mathbb{K})$ est la matrice de u dans une base de E, on a $\text{Ann}(u) = \text{Ann}(A)$ et $\pi_u = \pi_A$.

Exemple 11. Un endomorphisme est nilpotent d'indice q si et seulement si son polynôme minimal est X^q.

Proposition 12. Soit $u \in \mathcal{L}(E)$. Soit F un sous-espace vectoriel de E stable par u. Alors, le polynôme minimal de l'endomorphisme $u_{|F} : F \to F$ divise π_u.

Proposition 13. Soit $u \in \mathcal{L}(E)$.

(i) Les valeurs propres de u sont racines de tout polynôme annulateur.

(ii) Les valeurs propres de u sont exactement les racines de π_u.

Remarque 14. Soit $u \in \mathcal{L}(E)$. π_u et χ_u partagent dont les mêmes racines. **[GOU21]** p. 186

Théorème 15 (Cayley-Hamilton)**.** Soit $u \in \mathcal{L}(E)$. Alors, **[ROM21]** p. 607

$$\pi_u \mid \chi_u$$

Théorème 16 (Lemme des noyaux)**.** Soit $P = P_1 \dots P_k \in \mathbb{K}[X]$ où les polynômes $P_1, \dots, P_k$ p. 609

sont premiers entre eux deux à deux. Alors, pour tout endomorphisme u de E,

$$\mathrm{Ker}(P(u)) = \bigoplus_{i=1}^{k} \mathrm{Ker}(P_i(u))$$

2. Trigonalisation

Définition 17. Soit $u \in \mathscr{L}(E)$. p. 675

- On dit que u est **trigonalisable** s'il existe une base de E dans laquelle la matrice de u est triangulaire supérieure.
- On dit qu'une matrice $A \in \mathscr{M}_n(\mathbb{K})$ est **trigonalisable** si elle est semblable à une matrice diagonale.

Remarque 18. Un endomorphisme u de E est trigonalisable si et seulement si sa matrice dans n'importe quelle base de E l'est.

Exemple 19. Une matrice à coefficients réels ayant des valeurs propres imaginaires pures n'est pas trigonalisable dans $\mathscr{M}_n(\mathbb{R})$.

Théorème 20. Un endomorphisme u de E est trigonalisable sur $\mathbb{K}$ si et seulement si χ_u est scindé sur $\mathbb{K}$.

Corollaire 21. Si $\mathbb{K}$ est algébriquement clos, tout endomorphisme de u est trigonalisable sur $\mathbb{K}$.

Proposition 22. Soit $u \in \mathscr{L}(E)$. Si u est trigonalisable, sa trace est la somme de ses valeurs propres et son déterminant est le produit de ses valeurs propres.

[DEV]

Théorème 23 (Trigonalisation simultanée)**.** Soit $(u_i)_{i\in I}$ une famille d'endomorphismes de E diagonalisables qui commutent deux-à-deux. Alors, il existe une base commune de trigonalisation.

II - Endomorphismes nilpotents

1. Définition, caractérisation

[BMP] p. 168

Définition 24. On note

$$\mathcal{N}(E) = \{u \in \mathcal{L}(E) \mid \exists p \in \mathbb{N} \text{ tel que } u^p = 0\}$$

l'ensemble des éléments **nilpotents** de $\mathcal{L}(E)$.

Exemple 25. Dans $\mathbb{K}_n[X]$, l'opérateur de dérivation $P \mapsto P'$ est nilpotent.

Définition 26. On appelle **indice de nilpotence** d'un endomorphisme $u \in \mathcal{N}(E)$ l'entier q tel que

$$q = \inf\{p \in \mathbb{N} \mid u^p = 0\}$$

Proposition 27. Soit $u \in \mathcal{L}(E)$. Alors,

$$u \text{ est nilpotent d'indice } p \iff \pi_u = X^p$$

En particulier, $p \leq n$.

Théorème 28. Soit $u \in \mathcal{L}(E)$. Les assertions suivantes sont équivalentes :

(i) $u \in \mathcal{N}(E)$.

(ii) $\chi_u = (-1)^n X^n$.

(iii) Il existe $p \in \mathbb{N}$ tel que $\pi_u = X^p$. Dans ce cas, p est l'indice de nilpotence de u.

(iv) u est trigonalisable avec zéros sur la diagonale.

(v) u est trigonalisable et sa seule valeur propre est 0.

(vi) 0 est la seule valeur propre de u dans toute extension algébrique de $\mathbb{K}$.

(vii) Si $\text{car}(\mathbb{K}) = 0$: u et λu sont semblables pour tout $\lambda \in \mathbb{K}^*$.

Contre-exemple 29. La matrice

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$$

n'est pas nilpotente, alors que $\chi_A = -X(X^2+1)$ n'admet que 0 comme valeur propre réelle.

Proposition 30. Soit $u \in \mathscr{L}(E)$. On suppose $\text{car}(\mathbb{K}) = 0$. Alors,

$$u \in \mathscr{N}(E) \iff \forall k \in \mathbb{N}, \text{trace}(u^k) = 0$$

2. Cône nilpotent

Proposition 31. $\mathscr{N}(E)$ est un cône : si $u \in \mathscr{N}(E)$, alors $\forall \lambda \in \mathbb{K}$, $\lambda u \in \mathscr{N}(E)$.

Remarque 32. $\mathscr{N}(E)$ n'est pas un sous-groupe additif de $\mathscr{L}(E)$. Par exemple,

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

A est somme de deux matrices nilpotentes, mais est inversible donc non nilpotente. En particulier, $\mathscr{N}(E)$ n'est ni un idéal, ni un sous-espace vectoriel de $\mathscr{L}(E)$.

Proposition 33.

$$\text{Vect}(\mathscr{N}(E)) = \text{Ker}(\text{trace})$$

Exemple 34. En dimension 2,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ est nilpotente} \iff -a^2 - bc = 0$$

Proposition 35. Soient $u, v \in \mathscr{L}(E)$ tels que $uv = vu$.

(i) Si $u, v \in \mathscr{N}(E)$, alors $u + v \in \mathscr{N}(E)$.

(ii) Si $u \in \mathscr{N}(E)$, alors $uv \in \mathscr{N}(E)$.

3. Unipotence

Définition 36. On note

$$\mathscr{U}(E) = \text{id}_E + \mathscr{N}(E)$$

l'ensemble des endomorphismes **unipotents** de E.

p. 174

Remarque 37. On dispose de caractérisations analogues au Théorème 28 pour les endomorphismes unipotents. Par exemple, un endomorphisme u de E est unipotent si et seulement si $\chi_u = (1 - X)^n$.

On se place dans le cas où $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ pour la fin de cette sous-section.

Proposition 38. Soit $u \in \mathcal{N}(E)$. Alors $e^u \in \mathcal{U}(E)$. [ROM21] p. 767

Théorème 39. L'exponentielle matricielle réalise une bijection de $\mathcal{N}(E)$ sur $\mathcal{U}(E)$ d'inverse le logarithme matriciel.

4. Sous-espaces caractéristiques, noyaux itérés

Soit $u \in \mathcal{L}(E)$ de polynôme caractéristique scindé, de la forme [GOU21] p. 201

$$\chi_u = \prod_{i=1}^{s} (X - \lambda_i)^{\alpha_i}$$

Définition 40. Soit $i \in [\![1, s]\!]$. On appelle **sous-espace caractéristique** de u associé à la valeur propre λ_i le sous-espace vectoriel $N_i = \mathrm{Ker}((u - \lambda_i \mathrm{id}_E)^{\alpha_i})$.

Proposition 41. Soit $i \in [\![1, s]\!]$.

(i) N_i est stable par u.

(ii) $\dim(N_i) = \alpha_i$.

(iii) $\chi_{u_{|N_i}} = (-X)^{\dim(N_i)} = (-X)^{\alpha_i}$.

(iv) $u_{|N_i}$ est nilpotent.

De plus, $E = \oplus_{i=1}^{s} N_i$.

Proposition 42. Soit $v \in \mathcal{L}(E)$.

(i) La suite de sous-espaces vectoriels $(\mathrm{Ker}(v^n))$ est décroissante, stationnaire.

(ii) La suite de sous-espaces vectoriels $(\mathrm{Im}(v^n))$ est croissante, stationnaire.

Définition 43. Un **bloc de Jordan** de taille m associé à $\lambda \in \mathbb{K}$ désigne la matrice $J_m(\lambda)$ suivante : [BMP] p. 171

$$J_m(\lambda) = \begin{pmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{pmatrix} \in \mathcal{M}_m(\mathbb{K})$$

Application 44 (Réduction de Jordan d'un endomorphisme nilpotent)**.** On suppose que u

est nilpotent. Alors il existe des entiers $n_1 \geq \cdots \geq n_p$ et une base $\mathscr{B}$ de E tels que :

$$\mathrm{Mat}(u, \mathscr{B}) = \begin{pmatrix} J_{n_1}(0) & & \\ & \ddots & \\ & & J_{n_p}(0) \end{pmatrix}$$

De plus, on a unicité dans cette décomposition.

III - Applications

1. Décomposition de Dunford

[DEV]

Théorème 45 (Décomposition de Dunford)**.** Soit $u \in \mathscr{L}(E)$. On suppose que π_u est scindé sur $\mathbb{K}$. Alors il existe un unique couple d'endomorphismes (d, n) tels que :

- d est diagonalisable et n est nilpotent.
- $u = d + n$.
- $dn = nd$.

[GOU21] p. 203

Corollaire 46. Si u vérifie les hypothèse précédentes, pour tout $k \in \mathbb{N}$, $u^k = (d+n)^k = \sum_{i=0}^{m} \binom{k}{i} d^i n^{k-i}$, avec $m = \min(k, l)$ où l désigne l'indice de nilpotence de n.

Remarque 47. On peut montrer de plus que d et n sont des polynômes en u.

Théorème 48 (Décomposition de Dunford multiplicative)**.** Soit $f \in \mathscr{L}(E)$. On suppose que π_f est scindé sur $\mathbb{K}$. Alors il existe un unique couple d'endomorphismes (d, u) tels que :

- d est diagonalisable et u est unipotente.
- $f = du$.
- $du = ud$.

[ROM21] p. 687

2. Invariants de similitude

Soient E un espace vectoriel de dimension finie n et $u \in \mathscr{L}(E)$.

[GOU21] p. 397

Définition 49. On dit que u est **cyclique** s'il existe $x \in E$ tel que $\{P(u)(x) \mid P \in \mathbb{K}[X]\} = E$.

Proposition 50. u est cyclique si et seulement si $\deg(\pi_u) = n$.

Définition 51. Soit $P = X^p + a_{p-1}X^{p-1} + \cdots + a_0 \in \mathbb{K}[X]$. On appelle **matrice compagnon** de P la matrice

$$\mathscr{C}(P) = \begin{pmatrix} 0 & \dots & \dots & 0 & -a_0 \\ 1 & 0 & \ddots & \vdots & -a_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{p-2} \\ 0 & \dots & 0 & 1 & -a_{p-1} \end{pmatrix}$$

Proposition 52. u est cyclique si et seulement s'il existe une base $\mathscr{B}$ de E telle que $\mathrm{Mat}(u, \mathscr{B}) = \mathscr{C}(\pi_u)$.

Théorème 53. Il existe $F_1, \dots, F_r$ des sous-espaces vectoriels de E tous stables par u tels que :

— $E = F_1 \oplus \cdots \oplus F_r$.

— $u_i = u_{|F_i}$ est cyclique pour tout i.

— Si $P_i = \pi_{u_i}$, on a $P_{i+1} \mid P_i$ pour tout i.

La famille de polynômes $P_1, \dots, P_r$ ne dépend que de u et non du choix de la décomposition. On l'appelle **suite des invariants de similitude** de u.

Théorème 54 (Réduction de Frobenius)**.** Si $P_1, \dots, P_r$ désigne la suite des invariants de u, alors il existe une base $\mathscr{B}$ de E telle que :

$$\mathrm{Mat}(u, \mathscr{B}) = \begin{pmatrix} \mathscr{C}(P_1) & & \\ & \ddots & \\ & & \mathscr{C}(P_r) \end{pmatrix}$$

On a d'ailleurs $P_1 = \pi_u$ et $P_1 \dots P_r = \chi_u$.

Corollaire 55. Deux endomorphismes de E sont semblables si et seulement s'ils ont la même suite d'invariants de similitude.

Application 56. Pour $n = 2$ ou 3, deux matrices sont semblables si et seulement si elles ont mêmes polynômes minimal et caractéristique.

Application 57. Soit $\mathbb{L}$ une extension de $\mathbb{K}$. Alors, si $A, B \in \mathscr{M}_n(\mathbb{K})$ sont semblables dans $\mathscr{M}_n(\mathbb{L})$, elles le sont aussi dans $\mathscr{M}_n(\mathbb{K})$.

3. Commutant d'une matrice

Soit $A \in \mathcal{M}_n(\mathbb{K})$.

Lemme 58. Si $\pi_A = \chi_A$, alors A est cyclique :

$$\exists x \in \mathbb{K}^n \setminus \{0\} \text{ tel que } (x, Ax, \dots, A^{n-1}x) \text{ est une base de } \mathbb{K}^n$$

p. 289

Notation 59. — On note $\mathcal{T}_n(\mathbb{K})$ l'ensemble des matrices carrées triangulaires supérieures d'ordre n à coefficients dans le corps $\mathbb{K}$.

— On note $\mathscr{C}(A)$ le commutant de A.

[FGN2] p. 160

Lemme 60.

$$\dim_{\mathbb{K}}(\mathscr{C}(A)) \geq n$$

Lemme 61. Le rang de A est invariant par extension de corps.

Théorème 62.

$$\mathbb{K}[A] = \mathscr{C}(A) \iff \pi_A = \chi_A$$

157 Matrices symétriques réelles, matrices hermitiennes.

Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ et soit $n \geq 1$ un entier.

I - Généralités

1. Espaces $\mathcal{S}_n(\mathbb{R})$ et $\mathcal{H}_n(\mathbb{C})$

Notation 1. Soit $M \in \mathcal{M}_{n,m}(\mathbb{K})$. On note

$$M^* = \begin{cases} {}^tM & \text{si } \mathbb{K} = \mathbb{R} \\ {}^t\overline{M} & \text{si } \mathbb{K} = \mathbb{C} \end{cases}$$

[GOU21] p. 243

Définition 2. Soit $M \in \mathcal{M}_n(\mathbb{R})$.

— On dit que M est **symétrique** si $M^* = M$. On note $\mathcal{S}_n(\mathbb{R})$ l'ensemble des matrices symétriques à coefficients réels.

— On dit que M est **antisymétrique** si $M^* = -M$. On note $\mathbb{A}_n(\mathbb{R})$ l'ensemble des matrices antisymétriques à coefficients réels.

p. 125

Proposition 3. (i) $\mathcal{S}_n(\mathbb{R})$ et $\mathcal{A}_n(\mathbb{R})$ sont des sous-espaces vectoriels de $\mathcal{M}_n(\mathbb{R})$ de dimensions respectives $\frac{n(n+1)}{2}$ et $\frac{n(n-1)}{2}$.

(ii) $\mathcal{M}_n(\mathbb{R}) = \mathcal{S}_n(\mathbb{R}) \oplus \mathcal{A}_n(\mathbb{R})$.

p. 240

Définition 4. Soit $M \in \mathcal{M}_n(\mathbb{C})$. On dit que M est **hermitienne** si $M^* = M$. On note $\mathcal{H}_n(\mathbb{C})$ l'ensemble des matrices hermitiennes à coefficients complexes.

Proposition 5.

$$\forall M \in \mathcal{H}_n(\mathbb{C})\, \exists! (S,A) \in \mathcal{S}_n(\mathbb{R}) \times \mathcal{A}_n(\mathbb{R}) \text{ tel que } M = S + iA$$

Corollaire 6. $\mathcal{H}_n(\mathbb{C})$ est un sous-espace vectoriel du $\mathbb{R}$-espace vectoriel $\mathcal{M}_n(\mathbb{C})$ de dimension n^2.

2. Positivité

Définition 7. Soit $\langle .,. \rangle$ un produit scalaire sur $\mathbb{K}^n$. [ROM21] p. 735

— Si $\mathbb{K} = \mathbb{R}$, une matrice symétrique $M \in \mathcal{S}_n(\mathbb{R})$ est dite **positive** si

$$\forall x \in \mathbb{R}^n, \langle x, Mx \rangle \geq 0$$

et elle est dite **définie positive** si l'inégalité précédente est stricte pour tout $x \neq 0$. On note respectivement $\mathcal{S}_n^+(\mathbb{R})$ et $\mathcal{S}_n^{++}(\mathbb{R})$ l'ensemble des matrices symétriques positives et définies positives.

— Si $\mathbb{K} = \mathbb{C}$, ces définitions sont valables. On note respectivement $\mathcal{H}_n^+(\mathbb{C})$ et $\mathcal{H}_n^{++}(\mathbb{C})$ l'ensemble des matrices hermitiennes positives et définies positives.

Proposition 8. Soit $M \in \mathcal{S}_n(\mathbb{R})$. Alors $M \in \mathcal{S}_n^+(\mathbb{R})$ (resp. $\mathcal{S}_n^{++}(\mathbb{R})$) si et seulement si toutes ses valeurs propres sont positives (resp. strictement positives).

Corollaire 9. Soit $M \in \mathcal{S}_n(\mathbb{R})$. Alors $M \in \mathcal{S}_n^+(\mathbb{R})$ si et seulement s'il existe $B \in \mathcal{M}_n(\mathbb{R})$ telle que $M = {}^tBB$.

Théorème 10 (Critère de Sylvester)**.** Une matrice symétrique est définie positive si et seulement si tous ses mineurs principaux sont strictement positifs.

Corollaire 11. $\mathcal{S}_n^{++}(\mathbb{R})$ est un ouvert de $\mathcal{M}_n(\mathbb{R})$.

Lemme 12. Soit $S \in \mathcal{S}_n(\mathbb{R})$. Alors, [I-P] p. 182

$$|||S|||_2 = \rho(S)$$

où ρ est l'application qui a une matrice y associe son rayon spectral.

[DEV] **Théorème 13.** L'application $\exp : \mathcal{S}_n(\mathbb{R}) \to \mathcal{S}_n^{++}(\mathbb{R})$ est un homéomorphisme.

3. Lien avec l'algèbre bilinéaire

Soit E un espace vectoriel sur $\mathbb{K}$ de dimension n.

[GOU21] p. 239

Définition 14. Soit $\varphi : E \times E \to \mathbb{K}$ une application.

— On dit que φ est une **forme bilinéaire** sur E si pour tout $x \in E$, $y \mapsto \varphi(x,y)$ et pour tout $y \in E$, $x \mapsto \varphi(x,y)$ sont linéaires.

— Si $\mathbb{K} = \mathbb{C}$, on dit que φ est une **forme sesquilinéaire** sur E si pour tout $x \in E$, $y \mapsto \varphi(x,y)$ est linéaire et pour tout $y \in E$, $x \mapsto \varphi(x,y)$ est antilinéaire (ie. $\forall x,y,z \in E$, $\forall \lambda \in \mathbb{C}$, $\varphi(x+y,z) = \varphi(x,z) + \varphi(y,z)$ et $\varphi(\lambda x, z) = \overline{\lambda}\varphi(x,z)$).

Exemple 15. — Toute forme sesquilinéaire sur E est une forme bilinéaire lorsque E est considéré comme un espace vectoriel sur $\mathbb{R}$.

— L'application

$$\begin{array}{ccc} \mathscr{C}([0,1],\mathbb{C})^2 & \to & \mathbb{C} \\ (f,g) & \mapsto & \int_0^1 \overline{f(t)} g(t)\,\mathrm{d}t \end{array}$$

est une forme sesquilinéaire sur $\mathscr{C}([0,1],\mathbb{C})$.

Définition 16. On définit la matrice d'une forme bilinéaire (ou sesquilinéaire) φ dans une base $(e_1,\dots,e_n)$ de E par

$$(\varphi(e_i,e_j))_{i,j\in[\![1,n]\!]} \in \mathscr{M}_n(\mathbb{K})$$

Remarque 17. Soit $\mathscr{B} = (e_1,\dots,e_n)$ une base de E. Soient $x = \sum_{i=1}^n x_i e_i \in E$ et $y = \sum_{i=1}^n y_i e_i \in E$. Soit φ une forme bilinéaire ou sesquilinéaire, dont on note M sa matrice dans le base $\mathscr{B}$. On a :

$$\varphi(x,y) = X^* M Y, \text{ où } X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \text{ et } Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

Définition 18. Soit φ une forme bilinéaire sur E. On dit que :

— φ est **symétrique** si $\forall x,y \in E$, $\varphi(x,y) = \varphi(y,x)$.

— φ est **antisymétrique** si $\forall x,y \in E$, $\varphi(x,y) = -\varphi(y,x)$.

— Si $\mathbb{K} = \mathbb{C}$, on dit que φ est **hermitienne** si $\forall x,y \in E$, $\varphi(x,y) = \overline{\varphi(y,x)}$.

Proposition 19. (i) Une forme bilinéaire est symétrique (resp. antisymétrique) si et seulement si sa matrice dans une base est symétrique (resp. antisymétrique).

(ii) Une forme sesquilinéaire est hermitienne si et seulement si sa matrice dans une base est hermitienne.

Définition 20. On appelle **forme quadratique** sur E toute application q de la forme

$$q : \begin{array}{ccc} E & \to & \mathbb{K} \\ x & \mapsto & \varphi(x,x) \end{array}$$

où φ est une forme bilinéaire symétrique sur E.

Proposition 21. Soit q une forme quadratique sur E. Il existe une unique forme bilinéaire symétrique φ telle que pour tout $x \in E$, $q(x) = \varphi(x,x)$.

φ est alors la **forme polaire** de q, et on a

$$\forall x, y \in E, \varphi(x,y) = \frac{1}{2}(q(x+y) - q(x) - q(y))$$

Exemple 22. La matrice symétrique

$$\begin{pmatrix} 3 & 1 & -\frac{3}{2} \\ 1 & 0 & 0 \\ -\frac{3}{2} & 0 & 0 \end{pmatrix}$$

définit la forme quadratique $q : (x,y,z) \mapsto 3x^2 + y^2 + 2xy - 3xz$.

II - Réductions, décompositions

1. Réductions

p. 254

Définition 23. Soit $M \in \mathcal{M}_n(\mathbb{K})$ telle que ${}^tMM = I_n$.

- Si $\mathbb{K} = \mathbb{R}$, on dit que M est **orthogonale**. On note $\mathcal{O}_n(\mathbb{R})$ l'ensemble des matrices orthogonales à coefficients réels.
- Si $\mathbb{K} = \mathbb{C}$, on dit que M est **unitaire**. On note $\mathcal{U}_n(\mathbb{C})$ l'ensemble des matrices unitaires à coefficients complexes.

Théorème 24 (Spectral)**.** Soit $M \in \mathcal{S}_n(\mathbb{R})$ (resp. $M \in \mathcal{H}_n(\mathbb{C})$). Alors il existe $C \in \mathcal{O}_n(\mathbb{R})$ (resp. $C \in \mathcal{U}_n(\mathbb{C})$) telle que

$$C^{-1}MC = C^*MC = D$$

où D est une matrice diagonale réelle.

Remarque 25. En reprenant les notations précédentes, cela revient à dire qu'un endomorphisme ayant M pour matrice dans une base est diagonalisable dans une base orthonormée.

Corollaire 26. Soient $M, N \in \mathcal{S}_n(\mathbb{R})$ (resp. $M \in \mathcal{H}_n(\mathbb{C})$) définies positives. Alors il existe C inversible telle que

$$C^*MC = I_n \text{ et } C^*NC = D$$

où D est une matrice diagonale réelle.

Application 27. p. 283

$$\forall A, B \in \mathcal{H}_n^{++}(\mathbb{C}),\ \det(A+B)^{\frac{1}{n}} \geq \det(A)^{\frac{1}{n}} + \det(B)^{\frac{1}{n}}$$

Comme application du Théorème 24, on a les résultats suivants.

[ROM21] p. 738

Application 28 (Norme euclidienne sur $\mathcal{S}_n(\mathbb{R})$)**.** Soit $A = (a_{i,j})_{i,j\in[\![1,n]\!]} \in \mathcal{S}_n(\mathbb{R})$ de valeurs propres $\lambda_1, \dots, \lambda_n \in \mathbb{R}$. On a

$$\sum_{i,j=1}^{n} a_{i,j}^2 = \sum_{i=1}^{n} \lambda_i^2$$

Application 29 (Diagonalisation simultanée)**.** Soit $(A_i)_{i\in I}$ une famille de matrices symétriques. Alors, il existe $P \in \mathcal{O}_n(\mathbb{R})$ telle que pour tout $i \in I$, la matrice ${}^tPA_iP$ est diagonale si et seulement si $A_iA_j = A_jA_i$ pour tout $i \neq j$.

[C-G] p. 376

Application 30 (Racine carrée dans $\mathcal{S}_n^{++}(\mathbb{R})$ et $\mathcal{H}_n^{++}(\mathbb{C})$)**.**

$$\forall A \in \mathcal{S}_n^{++}(\mathbb{R})\ \exists! B \in \mathcal{S}_n^{++}(\mathbb{R}) \text{ telle que } B^2 = A$$

et on a le même résultat en remplaçant $\mathcal{S}_n^{++}(\mathbb{R})$ par $\mathcal{H}_n^{++}(\mathbb{C})$.

Théorème 31 (Loi d'inertie de Sylvester)**.** Soit $A \in \mathcal{S}_n(\mathbb{R})$. Alors, il existe $P \in \mathrm{GL}_n(\mathbb{R})$ et un unique couple d'entiers (p, q) tels que p. 299

$${}^tPAP = \begin{pmatrix} I_p & 0 & 0 \\ 0 & -I_q & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Définition 32. Le couple (p, q) précédent est la **signature** de A.

Proposition 33. Soit q une forme quadratique de forme polaire sur $\mathbb{R}^n$. Alors les conditions suivantes sont équivalentes :

(i) φ est un produit scalaire.

(ii) q est de signature $(n, 0)$.

(iii) La matrice de φ dans une base de $\mathbb{R}^n$ est de la forme $S = {}^tPP$ avec $P \in \mathrm{GL}_n(\mathbb{R})$.

(iv) La matrice de φ dans une base de $\mathbb{R}^n$ est de la forme $S = {}^tPP$ avec $P \in \mathrm{GL}_n(\mathbb{R})$ triangulaire supérieure.

Remarque 34. Soit $M \in \mathcal{S}_n(\mathbb{R})$ de signature (p,q). Alors, p (resp. q) est le nombre de valeurs propres de M strictement positives (resp. strictement négatives). p. 270

Corollaire 35. Soient $A, B \in \mathcal{S}_n(\mathbb{R})$. Alors A et B sont congruentes si et seulement si elles sont de même signature.

Application 36. p. 348

$$\{PP^* \mid P \in \mathrm{GL}_n(\mathbb{K})\} = \begin{cases} \mathcal{S}_n^{++}(\mathbb{R}) & \text{si } \mathbb{K} = \mathbb{R} \\ \mathcal{H}_n^{++}(\mathbb{C}) & \text{si } \mathbb{K} = \mathbb{C} \end{cases}$$

2. Décompositions

[DEV]

Application 37 (Décomposition polaire)**.** L'application p. 376

$$\mu : \begin{array}{ccc} \mathcal{O}_n(\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R}) & \to & \mathrm{GL}_n(\mathbb{R}) \\ (O,S) & \mapsto & OS \end{array}$$

est un homéomorphisme.

Corollaire 38. Tout sous-groupe compact de $\mathrm{GL}_n(\mathbb{R})$ qui contient $\mathcal{O}_n(\mathbb{R})$ est $\mathcal{O}_n(\mathbb{R})$.

Définition 39. Les **sous-matrices principales** d'une matrice $(a_{i,j})_{i,j\in[\![1,n]\!]} \in \mathcal{M}_n(\mathbb{K})$ sont les matrices $A_k = (a_{i,j})_{i,j\in[\![1,k]\!]} \in \mathcal{M}_k(\mathbb{K})$ où $k \in [\![1,n]\!]$. Les **déterminants principaux** sont les déterminants des matrices A_k, pour $k \in [\![1,n]\!]$. [ROM21] p. 690

Théorème 40 (Décomposition lower-upper)**.** Soit $A \in \mathrm{GL}_n(\mathbb{K})$. Alors, A admet une décomposition

$$A = LU$$

(où L est une matrice triangulaire inférieure à diagonale unité et U une matrice triangulaire supérieure) si et seulement si tous les déterminants principaux de A sont non nuls. Dans ce cas, une telle décomposition est unique.

Corollaire 41. Soit $A \in \mathrm{GL}_n(\mathbb{K}) \cap \mathcal{S}_n(\mathbb{K})$. Alors, on a l'unique décomposition de A :

$$A = LD^tL$$

où L est une matrice triangulaire inférieure et D une matrice diagonale.

Application 42 (Décomposition de Cholesky)**.** Soit $A \in \mathcal{M}_n(\mathbb{R})$. Alors, $A \in \mathcal{S}_n^{++}(\mathbb{R})$ si et seulement s'il existe $B \in \mathrm{GL}_n(\mathbb{R})$ triangulaire inférieure telle que $A = B^tB$. De plus, une telle décomposition est unique si on impose la positivité des coefficients diagonaux de B.

Exemple 43. On a la décomposition de Cholesky : [GRI] p. 368

$$\begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

III - Applications

1. Géométrie différentielle

Lemme 44. Soit $A_0 \in \mathcal{S}_n(\mathbb{R})$ inversible. Alors il existe un voisinage V de A_0 dans $\mathcal{S}_n(\mathbb{R})$ et une application $\psi : V \to \mathrm{GL}_n(\mathbb{R})$ de classe $\mathcal{C}^1$ telle que [ROU] p. 209

$$\forall A \in V,\ A = {}^t\psi(A)A_0\psi(A)$$

Lemme 45 (Morse)**.** Soit $f : U \to \mathbb{R}$ une fonction de classe $\mathcal{C}^3$ (où U désigne un ouvert de $\mathbb{R}^n$ contenant l'origine). On suppose : p. 354

- $\mathrm{d}f_0 = 0$.
- La matrice symétrique $\mathrm{Hess}(f)_0$ est inversible.
- La signature de $\mathrm{Hess}(f)_0$ est $(p, n-p)$.

Alors il existe un difféomorphisme $\phi = (\phi_1, \dots, \phi_n)$ de classe $\mathcal{C}^1$ entre deux voisinage de l'origine de $\mathbb{R}^n$ $V \subseteq U$ et W tel que $\varphi(0) = 0$ et

$$\forall x \in U,\ f(x) - f(0) = \sum_{k=1}^{p} \phi_k^2(x) - \sum_{k=p+1}^{n} \phi_k^2(x)$$

Application 46. Soit S la surface d'équation $z = f(x,y)$ où f est de classe $\mathcal{C}^3$ au voisinage de l'origine. On suppose la forme quadratique $\mathrm{d}^2 f_0$ non dégénérée. Alors, en notant P le plan tangent à S en 0 : p. 341

(i) Si $\mathrm{d}^2 f_0$ est de signature $(2,0)$, alors S est au-dessus de P au voisinage de 0.

(ii) Si $\mathrm{d}^2 f_0$ est de signature $(0,2)$, alors S est en-dessous de P au voisinage de 0.

(iii) Si $\mathrm{d}^2 f_0$ est de signature $(1,1)$, alors S traverse P selon une courbe admettant un point double en $(0, f(0))$.

2. Résolution de systèmes linéaires

Proposition 47. Soit $A \in \mathrm{GL}_n(\mathbb{K})$ vérifiant les hypothèses du Théorème 40. On définit la suite (A_k) où $A_0 = A$ et $\forall k \in \mathbb{N}$, A_{k+1} est la matrice obtenue à partir de A_k à l'aide du pivot de Gauss sur la $(k+1)$-ième colonne. Alors, A_{n-1} est la matrice U de la décomposition $A = LU$ du Théorème 40.

[C-G] p. 257

Remarque 48. Pour résoudre un système linéaire $AX = Y$, on se ramène à $A = LU$ en $O\left(\frac{2}{3}n^3\right)$. Puis, on résout deux systèmes triangulaires "en cascade" :

$$LX' = Y \text{ puis } UX = X'$$

ceux-ci demandant chacun $O(2n^2)$ opérations.

158 Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie).

Soit E un espace vectoriel sur $\mathbb{R}$ de dimension finie n. On munit E d'un produit scalaire $\langle .,. \rangle$, qui en fait un **espace euclidien**. On note $\|.\|$ la norme associée à ce produit scalaire.

I - Conséquences du caractère euclidien de E

1. Adjoint d'un endomorphisme

Lemme 1 (Théorème de représentation de Riesz)**.** [ROM21] p. 718

$$\forall \varphi \in E^*, \exists! a \in E \text{ tel que } \forall x \in E, \varphi(x) = \langle x, a \rangle$$

Théorème 2.

$$\forall u \in \mathscr{L}(E), \exists! u^* \in \mathscr{L}(E) \text{ tel que } \forall x, y \in E, \langle u(x), y \rangle = \langle x, u^*(y) \rangle$$

Définition 3. Avec les notations du théorème précédent, on dit que u^* est **l'adjoint** de u.

Théorème 4. Soient $\mathscr{B} = (e_i)_{i \in I}$ une base de E et $G = (\langle e_i, e_j \rangle)_{i,j \in [\![1,n]\!]}$ la matrice de Gram correspondante. Si $u \in \mathscr{L}(E)$ a pour matrice A dans la base $\mathscr{B}$, alors la matrice de u^* dans la base $\mathscr{B}$ est

$$B = G^{-1}\,{}^tAG$$

En particulier, si $\mathscr{B}$ est orthonormée, on a $B = {}^tA$.

Proposition 5. p. 748

$$\forall u \in \mathscr{L}(E), |||u||| = |||u^*|||$$

Il en résulte que l'application linéaire (cf. Théorème 6) $u \mapsto u^*$ est continue pour la norme $|||.|||$ subordonnée à $\|.\|$.

2. Propriétés de l'adjoint

Proposition 6 (Propriétés de $u \mapsto u^*$)**.** Soient $u, v \in \mathscr{L}(E)$. On a : p. 719

(i) $\forall \lambda \in \mathbb{R}, (\lambda u + v)^* = \lambda u^* + v^*$.

(ii) $(u^*)^* = u$.

(iii) $(u \circ v)^* = v^* \circ u^*$.

(iv) $u \in \mathrm{GL}(E) \implies u^* \in \mathrm{GL}(E)$, et $(u^*)^{-1} = (u^{-1})^*$.

Proposition 7 (Propriétés de l'endomorphisme adjoint)**.** Soit $u \in \mathscr{L}(E)$. On a :

(i) $\det(u^*) = \det(u)$.

(ii) $\mathrm{Ker}(u^*) = \mathrm{Im}(u)^\perp$.

(iii) $\mathrm{Im}(u^*) = \mathrm{Ker}(u)^\perp$.

(iv) $\mathrm{rang}(u^*) = \mathrm{rang}(u)$.

(v) Si F est un sous-espace vectoriel de E stable par u, alors $F^\perp$ est stable par u^*.

Proposition 8. Soit $u \in \mathscr{L}(E)$. p. 751

$$u = 0 \iff \mathrm{trace}(u \circ u^*) = 0$$

II - Endomorphismes normaux

Définition 9. Un endomorphisme $u \in \mathscr{L}(E)$ est dit **normal** s'il est tel que $u \circ u^* = u^* \circ u$. p. 743

Remarque 10. En désignant par $A \in \mathscr{M}_n(\mathbb{R})$ la matrice de $u \in \mathscr{L}(E)$ dans une base orthonormée, u est normal si et seulement si,

$$^tAA = A\,^tA$$

ce qui se traduit en disant que la matrice A est normale.

Exemple 11. Les endomorphismes symétriques, anti-symétriques (Section III) et orthogonaux (Section IV) sont des endomorphismes normaux.

Proposition 12. $u \in \mathscr{L}(E)$ est normal si et seulement si $\|u(x)\| = \|u^*(x)\|$ pour tout $x \in E$ où $\|.\|$ est une norme euclidienne. p. 758

p. 743

Proposition 13. Soit $u \in \mathscr{L}(E)$ un endomorphisme normal.

(i) Si F est un sous-espace vectoriel de E stable par u, alors $F^\perp$ est stable par u.

(ii) Il existe un sous-espace vectoriel de E de dimension 1 ou 2 stable par u.

Proposition 14 (Réduction dans le cas $n = 2$)**.** On suppose $n = 2$. Soit $u \in \mathscr{L}(E)$ un endomorphisme normal.

— Si u a une valeur propre réelle : u est diagonalisable dans une base orthonormée.

— Sinon : il existe $\mathscr{B}$ une base orthonormée de E telle que la matrice de u dans $\mathscr{B}$ est

$$R(a,b) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

avec $b \neq 0$.

Théorème 15 (Réduction des endomorphismes normaux)**.** Soit $u \in \mathscr{L}(E)$ un endomorphisme normal. Alors, il existe $\mathscr{B}$ une base orthonormée de E telle que la matrice de u dans $\mathscr{B}$ est

$$\begin{pmatrix} D_p & 0 & 0 & \dots & 0 \\ 0 & R(a_1,b_1) & 0 & \dots & 0 \\ 0 & 0 & R(a_2,b_2) & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & R(a_r,b_r) \end{pmatrix}$$

où D_p est diagonale d'ordre p et $R(a,b)$ est définie à la Théorème 14.

III - Endomorphismes symétriques

1. Définitions et propriétés

Définition 16. Un endomorphisme $u \in \mathscr{L}(E)$ est dit **symétrique** s'il est tel que $u^* = u$. p. 732

Proposition 17. Un endomorphisme $u \in \mathscr{L}(E)$ est symétrique si et seulement si sa matrice dans une base orthonormée est symétrique.

Corollaire 18. $\mathscr{S}(E)$ est un sous-espace vectoriel de E de dimension $\frac{n(n+1)}{2}$.

Proposition 19. Si $u \in \mathscr{S}(E)$, alors $u^p \in \mathscr{S}(E)$ pour tout entier naturel p, et $v^* \circ u \circ v \in \mathscr{S}(E)$ pour tout $v \in \mathscr{L}(E)$.

Théorème 20 (Spectral)**.** Tout endomorphisme symétrique $u \in \mathcal{S}(E)$ se diagonalise dans une base orthonormée.

Corollaire 21. Toute matrice symétrique réelle se diagonalise dans une base orthonormée.

2. Endomorphismes symétriques positifs

Définition 22.
— Un endomorphisme $u \in \mathcal{L}(E)$ est dit **symétrique positif** (resp. **symétrique défini positif**) s'il est symétrique tel que $\langle x, u(x)\rangle \geq 0$ (resp. $\langle x, u(x)\rangle > 0$) pour tout $x \in E$. On note $\mathcal{S}^+(E)$ (resp. $\mathcal{S}^{++}(E)$) l'ensemble des endomorphismes symétriques positifs (resp. symétriques définis positifs).

— Une matrice $A \in \mathcal{M}_n(\mathbb{R})$ est dite **symétrique positive** (resp. **symétrique définie positive**) si elle est symétrique telle que $\langle x, Ax\rangle \geq 0$ (resp. $\langle x, Ax\rangle > 0$) pour tout $x \in E$. On note $\mathcal{S}_n^+(\mathbb{R})$ (resp. $\mathcal{S}_n^{++}(\mathbb{R})$) l'ensemble des matrices symétriques positives (resp. symétriques définies positives).

Théorème 23. Soit $u \in \mathcal{S}(E)$. Alors, $u \in \mathcal{S}^+(E)$ (resp. $u \in \mathcal{S}^{++}(E)$) si et seulement si toutes ses valeurs propres sont positives (resp. strictement positives).

Corollaire 24. Soit $A \in \mathcal{M}_n(\mathbb{R})$. Alors, $A \in \mathcal{S}_n^+(\mathbb{R})$ si et seulement s'il existe $B \in \mathcal{S}_n(\mathbb{R})$ telle que $A = {}^tBB$.

Exemple 25. p. 752

$$\begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix} = P^{-1}\begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -2 \end{pmatrix}P \text{ avec } P = \frac{1}{\sqrt{6}}\begin{pmatrix} \sqrt{2} & \sqrt{3} & 1 \\ \sqrt{2} & -\sqrt{3} & 1 \\ \sqrt{2} & 0 & -2 \end{pmatrix}$$

Lemme 26. Soit $M \in \mathcal{S}_n(\mathbb{R})$. Alors, [I-P] p. 182

$$|||M||| = \rho(M)$$

où ρ est l'application qui a une matrice y associe son rayon spectral.

[DEV]

Théorème 27. L'application $\exp : \mathcal{S}_n(\mathbb{R}) \to \mathcal{S}_n^{++}(\mathbb{R})$ est un homéomorphisme.

3. Endomorphismes antisymétriques

Définition 28. Un endomorphisme $u \in \mathscr{L}(E)$ est dit **anti-symétrique** s'il est tel que $u^* = -u$.

[ROM21] p. 718

Théorème 29. Soit $u \in \mathscr{L}(E)$ un endomorphisme anti-symétrique. Alors, les valeurs propres de u sont imaginaires pures (éventuellement nulles) et il existe $\mathscr{B}$ une base orthonormée de E telle que la matrice de u dans $\mathscr{B}$ est

p. 746

$$\begin{pmatrix} D_p & 0 & 0 & \dots & 0 \\ 0 & R(0,b_1) & 0 & \dots & 0 \\ 0 & 0 & R(0,b_2) & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & R(0,b_r) \end{pmatrix}$$

où D_p est diagonale d'ordre p et $R(a,b)$ est définie à la Théorème 14.

IV - Endomorphismes orthogonaux

1. Le groupe orthogonal

Définition 30. Un endomorphisme $u \in \mathscr{L}(E)$ est dit **orthogonal** (ou est une **isométrie**) s'il est tel que $\langle u(x), u(y)\rangle = \langle x, y\rangle$ pour tout $x, y \in E$. On note $\mathscr{O}(E)$ l'ensemble des endomorphismes orthogonaux de E.

p. 720

Exemple 31.
— Les seules homothéties qui sont des isométries sont $-\mathrm{id}_E$ et id_E.
— Si $n = 1$, on a $\mathscr{O}(E) = \{\pm \mathrm{id}_E\}$.

Proposition 32. Soit $u \in \mathscr{L}(E)$.

p. 743

$$u = \mathscr{O}(E) \iff \forall x \in E,\ \|u(x)\| \iff u \in \mathrm{GL}(E) \text{ et } u^{-1} = u^*$$

Théorème 33. Les isométries sont des automorphismes. Il en résulte que $\mathscr{O}(E)$ est un sous-groupe de $\mathrm{GL}(E)$.

p. 721

Remarque 34. Ce n'est pas vrai en dimension infinie.

Théorème 35. Un endomorphisme de E est une isométrie si et seulement s'il transforme toute base orthonormée de E en une base orthonormée.

Théorème 36. Un endomorphisme de E est une isométrie si et seulement si sa matrice A dans une base orthonormée est inversible, d'inverse ${}^tA$.

On dit alors que A est **orthogonale**.

Notation 37. On note $\mathcal{O}_n(\mathbb{R})$ le groupe des matrices orthogonales.

Théorème 38.

$$\forall u \in \mathcal{O}(E), \det(u) = \pm 1$$

Remarque 39. On a des résultats équivalents pour les matrices.

Théorème 40 (Réduction des endomorphismes orthogonaux)**.** Soit $u \in \mathcal{O}(E)$. Alors, il existe $\mathcal{B}$ une base orthonormée de E telle que la matrice de u dans $\mathcal{B}$ est

$$\begin{pmatrix} I_p & 0 & 0 & \dots & 0 \\ 0 & -I_q & 0 & \dots & 0 \\ 0 & 0 & R_1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & R_r \end{pmatrix}$$

où $R_i = R(\cos(\theta_i), \sin(\theta_i))$ avec $R(a,b)$ définie à la Théorème 14 et $\forall i \in [\![1, r]\!]$, $\theta_i \in]0, 2\pi[$.

Lemme 41. [C-G] p. 376

$$\forall A \in \mathcal{S}_n^{++}(\mathbb{R}) \; \exists! B \in \mathcal{S}_n^{++}(\mathbb{R}) \text{ telle que } B^2 = A$$

[DEV]

Théorème 42 (Décomposition polaire)**.** L'application

$$\mu : \begin{array}{ccc} \mathcal{O}_n(\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R}) & \to & \mathrm{GL}_n(\mathbb{R}) \\ (O,S) & \mapsto & OS \end{array}$$

est un homéomorphisme.

2. Étude en dimensions 2 et 3

Définition 43. On définit $\mathrm{SO}(E) = \{u \in \mathcal{O}(E) \mid \det(u) = 1\}$ et $\mathrm{SO}_n(\mathbb{R}) = \{A \in \mathcal{O}_n(\mathbb{R}) \mid \det(A) = 1\}$

[GRI] p. 241

Proposition 44. $\mathrm{SO}(E)$ est un sous-groupe distingué de $\mathcal{O}(E)$ d'indice 2 (de même que $\mathrm{SO}_n(\mathbb{R})$ dans $\mathcal{O}_n(\mathbb{R})$).

[ROM21] p. 724

Exemple 45.

$$\frac{1}{3}\begin{pmatrix} 2 & -1 & 2 \\ 2 & 2 & -1 \\ -1 & 2 & 2 \end{pmatrix} \in \mathrm{SO}_3(\mathbb{R})$$

[GRI] p. 241

Théorème 46. Soit $A \in \mathcal{O}_2(\mathbb{R})$. Alors :

— Si $A \in \mathrm{SO}_2(\mathbb{R})$:

$$\exists \theta \in \mathbb{R} \text{ tel que } A = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

(rotation d'angle θ).

— Si $A \notin \mathrm{SO}_2(\mathbb{R})$:

$$\exists \theta \in \mathbb{R} \text{ tel que } A = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix}$$

(symétrie orthogonale par rapport à la droite d'angle polaire $\frac{\theta}{2}$).

Théorème 47. On suppose $n = 3$. Soit $A \in \mathcal{O}_3(\mathbb{R})$ et u l'endomorphisme de E dont la matrice dans la base canonique est A. Alors, il existe $\mathcal{B}$ une base orthonormée de E telle que la matrice de u dans $\mathcal{B}$ est

$$\begin{pmatrix} \cos(\theta) & -\sin(\theta) & 0 \\ \sin(\theta) & \cos(\theta) & 0 \\ 0 & 0 & \epsilon \end{pmatrix}$$

avec $\epsilon = \pm 1$. On note E_ϵ le sous-espace vectoriel associé à la valeur propre ϵ.

— Si $\epsilon = 1$: $f \in \mathrm{SO}(E)$ est la rotation d'angle $2\cos(\theta) + 1$ autour de l'axe E_1.

— Si $\epsilon = -1$: $f \notin \mathrm{SO}(E)$ est la composée de la rotation d'angle $2\cos(\theta) - 1$ autour de l'axe E_{-1} avec la symétrie orthogonale par rapport à $E_{-1}^{\perp}$.

3. Propriétés topologiques

Proposition 48. $\mathcal{O}(E)$ est une partie compacte de $\mathcal{L}(E)$. **[ROM21]** p. 722

Proposition 49. $\mathrm{SO}(E)$ est connexe dans $\mathcal{O}(E)$.

Corollaire 50. $\mathcal{O}(E)$ est non-connexe. Ses composantes connexes sont $\mathrm{SO}(E)$ et $\{u \in \mathcal{O}(E) \mid \det(u) = -1\}$.

Proposition 51. Tout sous-groupe compact de $\mathrm{GL}(E)$ qui contient $\mathcal{O}(E)$ est égal à $\mathcal{O}(E)$. p. 756

Annexes

[GRI] p. 242

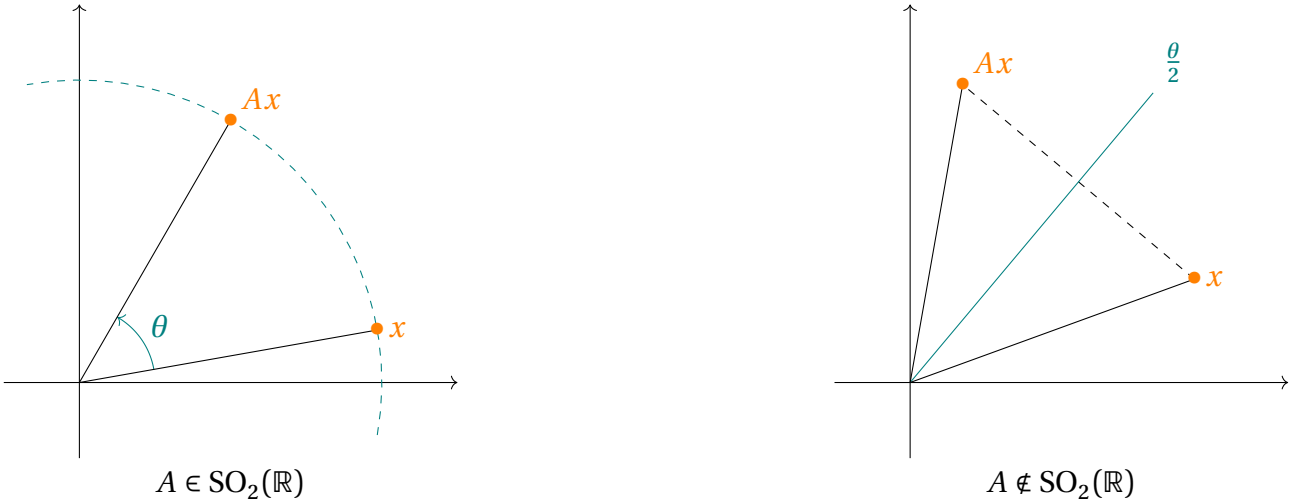


FIGURE I.9 – Le groupe $\mathcal{O}_2(\mathbb{R})$.

p. 244

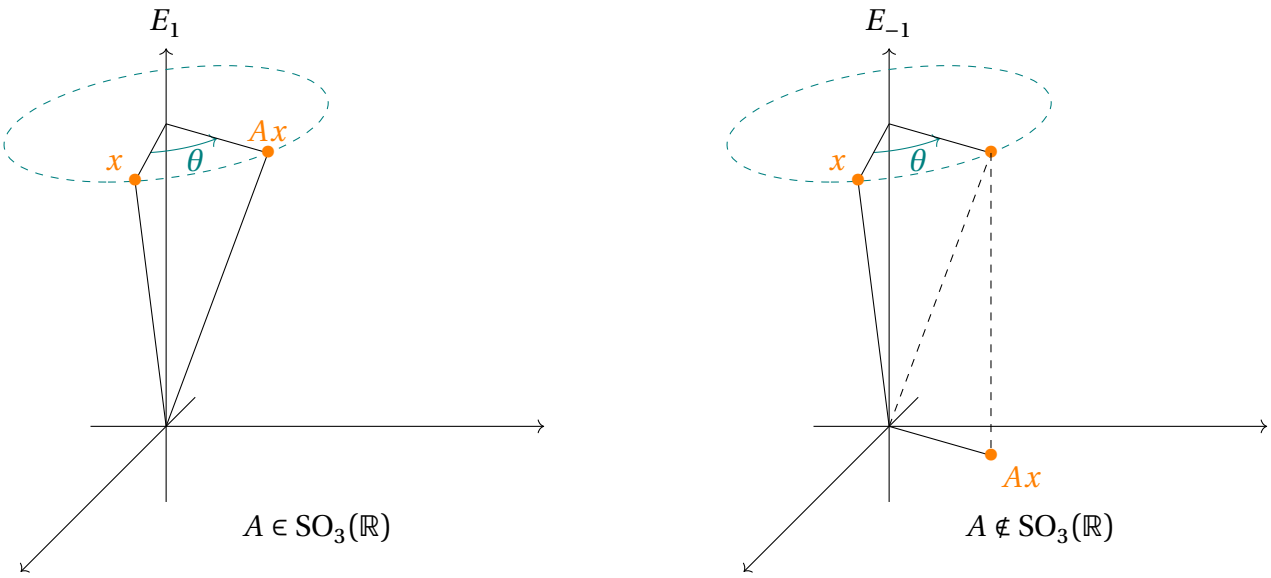


FIGURE I.10 – Le groupe $\mathcal{O}_3(\mathbb{R})$.

159 Formes linéaires et dualité en dimension finie. Exemples et applications.

Soit E un espace vectoriel sur un corps commutatif $\mathbb{K}$ de dimension finie n.

I - Dual d'un espace vectoriel

1. Formes linéaires, espace dual

Définition 1. Une **forme linéaire** sur E est une application linéaire de E dans $\mathbb{K}$. L'espace $\mathscr{L}(E,\mathbb{K})$ formé par l'ensemble des formes linéaires sur E est appelé **dual** de E et est noté E^*.

[ROM21] p. 441

Exemple 2.
— Soit $\mathscr{B} = (e_1, \dots, e_n)$ une base de E. Alors pour tout $j \in [\![1, n]\!]$, la projection

$$p_j : \sum_{i=1}^{n} x_i e_i \mapsto x_j$$

est une forme linéaire.

— Toute combinaison linéaire de formes linéaires est une forme linéaire.

Remarque 3. Une forme linéaire non nulle sur E est surjective.

Définition 4. On appelle **hyperplan** de E, le noyau d'une forme linéaire non nulle sur E.

Proposition 5.
(i) Un hyperplan de E est un sous-espace de E supplémentaire d'une droite.
(ii) Deux formes linéaires non nulles définissent le même hyperplan si et seulement si elles sont liées.

2. Bases duales

Définition 6. En reprenant les notations de la Théorème 2, les projections p_i sont les **formes linéaires coordonnées**. On note $\forall i \in [\![1, n]\!]$, $p_i = e_i^*$. La famille $\mathscr{B}^* = (e_1, \dots, e_n)$ est appelée **base duale** de $\mathscr{B}$.

[GOU21] p. 133

Remarque 7. Soit $\mathscr{B} = (e_1, \dots, e_n)$ une base de E. Pour tout $i, j \in [\![1, n]\!]$, on a

$$e_i^*(e_j) = \delta_{i,j} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{sinon} \end{cases}$$

Théorème 8. Soit $\mathscr{B} = (e_1, \dots, e_n)$ une base de E. Alors, la base duale $\mathscr{B}^*$ est une base de E^*.

Corollaire 9. (i) E^* est un espace vectoriel de dimension n.
(ii) Pour tout $\varphi \in E^*$, on a $\varphi = \sum_{n=1}^{n} \varphi(e_i) e_i^*$.

Corollaire 10. Tout hyperplan de E est de dimension $n-1$. **[ROM21]** p. 446

Exemple 11. Soit $U \subseteq \mathbb{R}^n$ un ouvert. Soit $f : U \to \mathbb{R}$ différentiable en $a \in U$. Alors, **[GOU20]** p. 325

$$\mathrm{d}f_a = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(a) e_i^*$$

où $(e_i^*)_{i \in [\![1,n]\!]}$ est la base duale de la base canonique $(e_i)_{i \in [\![1,n]\!]}$ de $\mathbb{R}^n$.

3. Bidual

Définition 12. On appelle **bidual** de E le dual E^*. On le note E^{**}. **[GOU21]** p. 133

Exemple 13. Pour $x \in E$, l'application $\mathrm{ev}_x : \varphi \mapsto \varphi(x)$ est un élément de E^{**}.

Théorème 14. $x \mapsto \mathrm{ev}_x$ est un isomorphisme entre les espaces E et E^{**}.

Remarque 15. Cet isomorphisme est canonique : il ne dépend pas du choix d'une base de E.

Corollaire 16. Soit $(f_1, \dots, f_n)$ une base de E^*. Il existe une unique base $(e_1, \dots, e_n)$ de E telle que, pour tout $i \in [\![1, n]\!]$, $e_i^* = f_i$.

Définition 17. En reprenant les notations précédentes, $(e_1, \dots, e_n)$ est appelée **base antéduale** de $(f_1, \dots, f_n)$.

Exemple 18. On suppose $n = 3$. Soient (e_1, e_2, e_3) une base de E et

$$f_1^* = 2e_1^* + e_2^* + e_3^*, f_2^* = -e_1^* + 2e_3^*, f_3^* = e_1^* + 3e_2^*$$

Alors, (f_1^*, f_2^*, f_3^*) est une base de E^*, dont une base antéduale est (f_1, f_2, f_3) où

$$f_1 = \frac{1}{13}(6e_1 - 2e_2 + 3e_3), f_2 = \frac{1}{13}(-3e_1 - e_2 + 5e_3), f_3 = \frac{1}{13}(-2e_1 + 5e_2 - e_3)$$

II - Orthogonalité au sens de la dualité

1. Orthogonal d'une partie, d'une famille

Définition 19. On dit qu'une forme linéaire $\varphi \in E^*$ et un vecteur $x \in E$ sont orthogonaux si $\varphi(x) = 0$.

[ROM21] p. 446

Définition 20.

— L'orthogonal dans E^* d'une partie non vide X de E est l'ensemble

$$X^\perp = \{\varphi \in E^* \mid \forall x \in X, \varphi(x) = 0\}$$

— L'orthogonal dans E d'une partie non vide Y de E^* est l'ensemble

$$Y^\circ = \{x \in E \mid \forall \varphi \in Y, \varphi(x) = 0\}$$

Théorème 21. Soient A, B des parties non vides de E et U, V des parties non vides de E^*.

(i) Si $A \subseteq B$, alors $B^\perp \subseteq A^\perp$.
(ii) Si $U \subseteq V$, alors $V^\circ \subseteq U^\circ$.
(iii) $A \subseteq (A^\perp)^\circ$.
(iv) $U \subseteq (U^\circ)^\perp$.
(v) $A^\perp = \text{Vect}(A)^\perp$.
(vi) $U^\circ = \text{Vect}(U)^\circ$.
(vii) $\{0\}^\perp = E^*, E^\perp = \{0\}, \{0\}^\circ = E$ et , $(E^*)^\circ = \{0\}$.

Corollaire 22.

(i) Pour tout sous-espace vectoriel F de E, on a

$$\dim(F) + \dim(F^\perp) = n$$

(ii) Pour tout sous-espace vectoriel G de E^*, on a

$$\dim(G) + \dim(F^\circ) = n$$

(iii) Pour tout sous-espace vectoriel F de E, et pour tout sous-espace vectoriel G de E^*, on a $F = (F^\perp)^\circ$ et $G = (G^\circ)^\perp$.

(iv) Pour toute partie X de E, on a $(X^\perp)^\circ = \mathrm{Vect}(X)$.

(v) Pour tous sous-espaces vectoriels F_1 et F_2 de E, on a :

$$(F_1 + F_2)^\perp = F_1^\perp \cap F_2^\perp \text{ et } (F_1 \cap F_2)^\perp = F_1^\perp + F_2^\perp$$

(vi) Pour tous sous-espaces vectoriels G_1 et G_2 de E^*, on a :

$$(G_1 + G_2)^\circ = G_1^\circ \cap G_2^\circ \text{ et } (G_1 \cap G_2)^\circ = G_1^\circ + G_2^\circ$$

Corollaire 23. Si $(\varphi_i)_{i\in[\![1,p]\!]}$ est une famille de formes linéaires sur E de rang r, le sous-espace vectoriel $F = \bigcap_{i=1}^p \mathrm{Ker}(\varphi_i)$ de E est alors de dimension $n-r$. Réciproquement, si F est un sous-espace vectoriel de E de dimension m, il existe alors une famille de formes linéaires $(\varphi_i)_{i\in[\![1,p]\!]}$ de rang $r = n-m$ telle que $F = \bigcap_{i=1}^p \mathrm{Ker}(\varphi_i)$.

2. Application transposée

Définition 24. Soient E et F deux espaces vectoriels sur $\mathbb{K}$. Soit $u \in \mathscr{L}(E,F)$. La **transposée** de $u \in \mathscr{L}(E,F)$ est l'application

p. 452

$$\begin{array}{rccc} {}^t u : & F^* & \to & E^* \\ & \varphi & \mapsto & \varphi \circ u \end{array}$$

Proposition 25. $u \mapsto {}^t u$ est linéaire, injective de $\mathscr{L}(E,F)$ dans $\mathscr{L}(F^*,E^*)$.

Théorème 26. Soient E, F et G trois espaces vectoriels sur $\mathbb{K}$. Soient $u \in \mathscr{L}(E,F)$ et $u \in \mathscr{L}(F,G)$. On a :

(i) ${}^t v \circ u = {}^t u \circ {}^t v$.

(ii) Pour $F = E$, ${}^t \mathrm{id}_E = \mathrm{id}_{E^*}$.

(iii) Si u est un isomorphisme de E sur F, alors ${}^t u$ est un isomorphisme de F^* sur E^* et $({}^t u)^{-1} = {}^t(u^{-1})$.

(iv) $\mathrm{Ker}({}^t u) = (\mathrm{Im}(u))^\perp$.

(v) u est surjective si et seulement si ${}^t u$ est injective.

(vi) $\mathrm{Im}({}^t u) = (\mathrm{Ker}(u))^\perp$.

(vii) u est injective si et seulement si ${}^t u$ est surjective.

(viii) Si E et F sont de dimension finie, alors u et ${}^t u$ ont même rang.

(ix) Si $A \in \mathcal{M}_n(\mathbb{K})$ est la matrice de u dans des bases $\mathcal{B}$ et $\mathcal{B}'$, alors ${}^t A$ est la matrice de ${}^t u$ dans les bases $\mathcal{B}'^*$ et $\mathcal{B}^*$.

Corollaire 27. Soient $\mathcal{B}$ et $\mathcal{B}'$ deux bases de E et P la matrice de passage de $\mathcal{B}$ à $\mathcal{B}'$. Alors, la matrice de passage de $\mathcal{B}^*$ à $\mathcal{B}'^*$ est

$$ {}^t P^{-1} $$

[GOU21] p. 136

Proposition 28. Soit $u \in \mathcal{L}(E)$. Alors un sous-espace vectoriel de E est stable par u si et seulement si son orthogonal l'est.

[DEV]

Application 29 (Trigonalisation simultanée)**.** Soit $(u_i)_{i\in I}$ une famille d'endomorphismes de E diagonalisables qui commutent deux-à-deux. Alors, il existe une base commune de trigonalisation.

p. 176

3. Lien avec l'orthogonalité au sens euclidien

Théorème 30 (de représentation de Riesz)**.** Soit $\langle .,. \rangle$ un produit scalaire sur E.

$$ \forall \varphi \in E^*, \exists! a \in E \text{ tel que } \forall x \in E, \varphi(x) = \langle x, a \rangle $$

[ROM21] p. 718

Ainsi, si E est muni d'un produit scalaire $\langle .,. \rangle$, on retrouve la notion classique d'orthogonalité euclidienne avec $\varphi : x \mapsto \langle x, a \rangle$.

p. 446

Exemple 31. L'application

$$ \begin{array}{ccc} \mathcal{M}_n(\mathbb{K}) & \to & \mathcal{M}_n(\mathbb{K})^* \\ A & \mapsto & (X \mapsto \operatorname{trace}(AX)) \end{array} $$

est un isomorphisme.

[GOU21] p. 138

III - Applications

1. Formule de Taylor

On suppose $\mathbb{K}$ de caractéristique nulle.

[ROM21] p. 442

Application 32 (Formule de Taylor)**.** Pour tout $j \in [\![0,n]\!]$, on définit :

$$e_j : \begin{array}{ccc} \mathbb{K}_n[X] & \to & \mathbb{K} \\ P & \mapsto & \frac{P^{(j)}(0)}{j!} \end{array}$$

Alors, $(e_i)_{i\in[\![0,n]\!]}$ est une base de $K_n[X]^*$, dont la base antéduale est $(X^i)_{i\in[\![0,n]\!]}$.

[GOU21] p. 64

Corollaire 33. On suppose $P \neq 0$. Alors $a \in \mathbb{K}$ est racine d'ordre h de P si et seulement si

$$\forall i \in [\![1, h-1]\!], P^{(i)}(a) = 0 \quad \text{et} \quad F^{(h)}(a) \neq 0$$

Exemple 34. Le polynôme $P_n = \sum_{i=0}^{n} \frac{1}{i!} X^i$ n'a que des racines simples dans $\mathbb{C}$.

Remarque 35. C'est encore vrai en caractéristique non nulle pour $h = 1$.

2. Invariants de similitude

Soient E un espace vectoriel de dimension finie n et $u \in \mathscr{L}(E)$.

[ROM21] p. 397

Définition 36. On dit que u est **cyclique** s'il existe $x \in E$ tel que $\{P(u)(x) \mid P \in \mathbb{K}[X]\} = E$.

Proposition 37. u est cyclique si et seulement si $\deg(\pi_u) = n$.

Définition 38. Soit $P = X^p + a_{p-1}X^{p-1} + \cdots + a_0 \in \mathbb{K}[X]$. On appelle **matrice compagnon** de P la matrice

$$\mathscr{C}(P) = \begin{pmatrix} 0 & \dots & \dots & 0 & -a_0 \\ 1 & 0 & \ddots & \vdots & -a_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{p-2} \\ 0 & \dots & 0 & 1 & -a_{p-1} \end{pmatrix}$$

Proposition 39. u est cyclique si et seulement s'il existe une base $\mathscr{B}$ de E telle que $\mathrm{Mat}(u, \mathscr{B}) = \mathscr{C}(\pi_u)$.

Théorème 40. Il existe $F_1, \dots, F_r$ des sous-espaces vectoriels de E tous stables par u tels que :

— $E = F_1 \oplus \cdots \oplus F_r$.

— $u_i = u_{|F_i}$ est cyclique pour tout i.

— Si $P_i = \pi_{u_i}$, on a $P_{i+1} \mid P_i$ pour tout i.

La famille de polynômes $P_1, \dots, P_r$ ne dépend que de u et non du choix de la décomposition. On l'appelle **suite des invariants de similitude** de u.

Théorème 41 (Réduction de Frobenius)**.** Si $P_1, \dots, P_r$ désigne la suite des invariants de u, alors il existe une base $\mathscr{B}$ de E telle que :

$$\mathrm{Mat}(u, \mathscr{B}) = \begin{pmatrix} \mathscr{C}(P_1) & & \\ & \ddots & \\ & & \mathscr{C}(P_r) \end{pmatrix}$$

On a d'ailleurs $P_1 = \pi_u$ et $P_1 \dots P_r = \chi_u$.

Corollaire 42. Deux endomorphismes de E sont semblables si et seulement s'ils ont la même suite d'invariants de similitude.

Application 43. Pour $n = 2$ ou 3, deux matrices sont semblables si et seulement si elles ont mêmes polynômes minimal et caractéristique.

Application 44. Soit $\mathbb{L}$ une extension de $\mathbb{K}$. Alors, si $A, B \in \mathscr{M}_n(\mathbb{K})$ sont semblables dans $\mathscr{M}_n(\mathbb{L})$, elles le sont aussi dans $\mathscr{M}_n(\mathbb{K})$.

3. Classification des formes quadratiques

Soit q une forme quadratique sur E.

p. 243

Lemme 45. Il existe une base q-orthogonale (ie. si φ est la forme polaire de q, une base B où $\forall e, e' \in B, \varphi(e, e') = 0$ si $e \neq e'$).

[DEV]

Théorème 46 (Loi d'inertie de Sylvester)**.**

$$\exists p, q \in \mathbb{N} \text{ et } \exists f_1, \dots, f_{p+q} \in E^* \text{ tels que } q = \sum_{i=1}^{p} |f_i|^2 - \sum_{i=p+1}^{p+q} |f_i|^2$$

où les formes linéaires f_i sont linéairement indépendantes et où $p + q \leq n$. De plus, ces entiers ne dépendent que de q et pas de la décomposition choisie.

Le couple (p,q) est la **signature** de q et le rang q est égal à $p+q$.

Exemple 47. La signature de la forme quadratique $q : (x,y,z) \mapsto x^2 - 2y^2 + xz + yz$ est $(2,1)$, donc son rang est 3.

162 Systèmes d'équations linéaires ; opérations élémentaires, aspects algorithmiques et conséquences théoriques.

Soit $\mathbb{K}$ un corps commutatif.

I - Généralités

1. Définitions

Définition 1. — On appelle **système linéaire** à p équations en n inconnues, un système d'équations de la forme

$$\begin{cases} a_{1,1}x_1 + \cdots + a_{1,n}x_n = b_1 \\ \vdots \\ a_{p,1}x_1 + \cdots + a_{1,n}x_n = b_p \end{cases} \qquad (S)$$

où $\forall i \in [\![1,p]\!]$, $\forall j \in [\![1,n]\!]$, $a_{i,j} \in \mathbb{K}$, $b_i \in \mathbb{K}$.

— On appelle **solution** de (S) tout vecteur $x = (x_1, \dots, x_n) \in \mathbb{K}^n$ dont les composantes $(x_i)_{i\in[\![1,n]\!]}$ satisfont toutes les équations.

— (S) est dit **compatible** s'il admet au moins une solution.

[GRI] p. 143

Exemple 2. Le système ci-dessous est linéaire,

$$\begin{cases} 2x + y - 2z + 3w = 1 \\ 3x + 2y - z + 2w = 4 \\ 3x + 3y + 3z - 3w = 5 \end{cases}$$

il n'est pas compatible.

p. 38

2. Écriture sous forme matricielle

Proposition 3. On considère le système (S) de la Théorème 1. On peut l'écrire sous forme matricielle

$$AX = B \qquad (S)$$

avec $A = (a_{i,j})_{\substack{i\in[\![1,p]\!] \\ j\in[\![1,n]\!]}} \in \mathcal{M}_{p,n}(\mathbb{K})$, $X = (x_j)_{j\in[\![1,n]\!]} \in \mathcal{M}_{n,1}(\mathbb{K})$ et $B = (b_i)_{i\in[\![1,p]\!]} \in \mathcal{M}_{p,1}(\mathbb{K})$.

p. 144

Définition 4. On appelle **rang** du système (S) le rang de la matrice A.

Proposition 5. Soit
$$AX = B$$
un système linéaire à n équations et n inconnues. Si A est inversible, on a une unique solution, donnée par $X = A^{-1}B$.

II - Étude de systèmes particuliers

1. Systèmes de Cramer

Définition 6. On appelle **système de Cramer**, un système linéaire à n équations et n inconnues $AX = B$.

Théorème 7 (Formules de Cramer)**.** Un système de Cramer $AX = B$ admet une unique solution donnée par $X = (x_i)_{i\in[\![1,n]\!]}$ où
$$\forall i \in [\![1,n]\!],\ x_i = \frac{\det(A_i)}{\det(A)}$$
avec A_i obtenue en remplaçant la i-ième colonne de A par B.

Exemple 8. Le système
$$\begin{cases} 2x - 5y + 2z = 7 \\ x + 2y - 4z = 3 \\ 3x - 4y - 6z = 5 \end{cases}$$
est de Cramer, son unique solution est $(5,1,1)$.

2. Équations de Sylvester

Lemme 9. Soit $\|.\|$ une norme d'algèbre sur $\mathcal{M}_n(\mathbb{C})$, et soit $A \in \mathcal{M}_n(\mathbb{C})$ une matrice dont les valeurs propres sont de partie réelle strictement négative. Alors il existe une fonction polynômiale $P : \mathbb{R} \to \mathbb{R}$ et $\lambda > 0$ tels que $\|e^{tA}\| \leq e^{-\lambda t}P(t)$.

[I-P] p. 177

[DEV]

Application 10 (Équation de Sylvester)**.** Soient A et $B \in \mathcal{M}_n(\mathbb{C})$ deux matrices dont les valeurs propres sont de partie réelle strictement négative. Alors pour tout $C \in \mathcal{M}_n(\mathbb{C})$, l'équation $AX + XB = C$ admet une unique solution X dans $\mathcal{M}_n(\mathbb{C})$.

III - Méthodes générales de résolution

1. Théorème de Rouché-Fontené

Lemme 11. Soit $A \in \mathcal{M}_{p,n}(\mathbb{K})$. Soit $r = \text{rang}(A)$. Il existe un déterminant Δ d'ordre r extrait de A.

[GOU21] p. 144

Définition 12. — Le déterminant Δ précédent est le **déterminant principal** de A.

— Les équations (resp. inconnues) dont les indices sont deux des lignes (resp. colonnes) de Δ s'appellent les **équations principales** (resp. **inconnues principales**).

— Si $\Delta = \det(a_{i,j})_{\substack{i\in I\\ j\in J}}$, on appelle **déterminants caractéristiques** les déterminants d'ordre $r+1$ de la forme

$$\left|\begin{array}{c|c} (a_{i,j})_{\substack{i\in I\\ j\in J}} & (b_i)_{i\in I} \\ \hline (a_{k,j})_{j\in J} & b_k \end{array}\right| \text{ avec } k \notin J.$$

Théorème 13 (Rouché-Fontené)**.** Un système de rang r

$$AX = B$$

avec $A \in \mathcal{M}_{p,n}(\mathbb{K})$, $X \in \mathcal{M}_{n,1}(\mathbb{K})$ et $B \in \mathcal{M}_{1,p}(\mathbb{K})$ admet des solutions si et seulement si $p = r$ ou les $p-r$ déterminants caractéristiques sont nuls. Le système est alors équivalent au système des équations principales. Les inconnues principales étant déterminées par un système de Cramer à l'aide des inconnues non principales.

Exemple 14. Si,

$$(S) \iff \begin{cases} x+2y+z+t=1 \\ x-z-t=1 \\ -x+y+z+2t=m \end{cases} \qquad m \in \mathbb{R}$$

on a $\text{rang}(A) = 2$, (S) admet des solutions si et seulement si $m = -1$, et

$$(S) \iff \begin{cases} x+2y = 1+z-t \\ x = 1+z+t \end{cases} \iff \begin{cases} x = 1+z+t \\ y = -t \end{cases}$$

2. Algorithme du pivot de Gauss

a. Opérations élémentaires

[ROM21] p. 186

Définition 15. Soit $A = (a_{i,j})_{\substack{i\in[\![1,n]\!]\\ j\in[\![1,m]\!]}} \in \mathcal{M}_{n,m}(\mathbb{K})$.

— On dit que A est **échelonnée en lignes** si elle est nulle ou si elle est non nulle et il existe un entier r compris entre 1 et n tel que :

  — Les r premières lignes de A sont non nulles.

  — Les $n-r$ dernières lignes de A sont nulles.

  — En notant $\forall i \in [\![1,n]\!]$, $d_i = \min\{j \in [\![1,m]\!] \mid a_{i,j} \neq 0\}$, on a

$$1 \leq d_1 < d_2 < \cdots < d_r \leq m$$

— On dit que A est **échelonnée en colonnes** si ${}^tA$ est échelonnée en lignes.

Proposition 16. Avec les notations précédentes, si A est échelonnée en lignes, alors $\text{rang}(A) = r$.

Définition 17. On dit qu'un système linéaire $AX = B$ est **échelonné** si la matrice A est échelonnée en lignes.

Théorème 18. (i) La multiplication à gauche par une matrice de dilatation $D_i(\lambda)$ (obtenue à partir de la matrice identité en remplaçant le coefficient 1 à la i-ième ligne par λ) a pour effet de multiplier la ligne i par λ.

(ii) La multiplication à gauche par une matrice de transvection $T_{i,j}(\lambda)$ (obtenue à partir de la matrice identité en remplaçant le coefficient 0 à la i-ième ligne et j-ième colonne par λ) a pour effet de multiplier la ligne i par la somme de la ligne i et de la ligne j multipliée par λ.

(iii) La multiplication à droite fait des effets similaires sur les colonnes.

Remarque 19. Pour effectuer une permutation des lignes i et j, il suffit de multiplier à gauche par

$$D_j(-1)T_{i,j}(1)T_{j,i}(-1)T_{i,j}(1)$$

Définition 20. On appelle **opération élémentaire** une des opérations citées précédemment.

Théorème 21. Une opération élémentaire sur les lignes d'un système linéaire le transforme en un système équivalent.

b. Résolution pratique

On cherche à résoudre le système linéaire de n équations à m inconnues :

$$\begin{cases} a_{1,1}x_1 + \cdots + a_{1,m}x_m = b_1 \\ \vdots \\ a_{n,1}x_1 + \cdots + a_{1,n}x_m = b_n \end{cases} \tag{S}$$

mis sous forme matricielle $AX = B$. On suppose $A \neq 0$ (sinon l'ensemble des solutions de (S) est $\mathbb{K}^n$). On note L_i la ligne numéro i de A pour tout $i \in [\![1, m]\!]$.

Théorème 22 (Échelonnement par pivot)**.** (i) Si les premières colonnes $C_1, \ldots, C_{d_1}$ de la matrice A sont nulles, les variables $x_1, \ldots, x_d$ peuvent être quelconques et on passe à la colonne $d_1 + 1$, ce qui nous donne un système de n équations à $m - d$ inconnues. On suppose donc que la première colonne de la matrice A n'est pas nulle et en permutant la ligne 1 avec une des lignes suivantes on se ramène à un système $A^{(1)}X = B^{(1)}$ avec $a^{(1)}_{1,1} \neq 0$. On élimine alors x_1 des lignes 2 à n en effectuant les opérations élémentaires $L_i \leftarrow L_i - \frac{a^{(1)}_{1,1}}{a^{(1)}_{1,1}} L_i$ pour $i \in [\![2, n]\!]$, ce qui donne le système :

$$\begin{cases} a^{(1)}_{1,1}x_1 + a^{(1)}_{1,2}x_2 + \cdots + a^{(1)}_{1,m}x_m = b^{(1)}_1 \\ a^{(2)}_{2,2}x_2 + \cdots + a^{(2)}_{2,m}x_m = b^{(2)}_2 \\ \vdots \\ a^{(2)}_{n,2}x_1 + \cdots + a^{(2)}_{1,n}x_m = b^{(2)}_n \end{cases}$$

(ii)
- Si l'un des coefficients $a^{(2)}_{i,2}$ est non nul (pour $i \in [\![1, n]\!]$), on recommence avec un procédé analogue pour éliminer x_2 des équations 3 à n.
- Si tous les coefficients $a^{(2)}_{i,2}$ sont nuls, on passe alors à la colonne suivante. Et on recommence ainsi de suite.

(iii) Au bout d'un nombre fini d'étapes, on aboutit à un système échelonné qui est équivalent au système (S).

Une fois le système échelonné, on peut procéder à la résolution.

Théorème 23 (Remontée)**.** Trois cas de figure sont possibles.

(i) Soit on a obtenu un système de Cramer triangulaire supérieur d'ordre $n = m = r$. Un tel système a une unique solution et se résout alors "en remontée". Dans ce cas, A est de rang $n = m$.

(ii) Soit on a obtenu un système de $r \leq n$ équations à $m > r$ inconnues. Les r premières inconnues sont les inconnues principales et les autres inconnues non principales. Ces dernières sont alors utilisées comme paramètres en second membre et on résout le système d'inconnues principales $x_1, \ldots, x_r$. L'ensemble des solutions est un espace

affine de dimension $n-r$ et le rang de la matrice est r.

(iii) Soit on a obtenu un système de n équations à $r = m < n$ inconnues, de la forme :

$$\begin{cases} \alpha_{1,1}x_1 + \alpha_{1,2}x_2 + \cdots + \alpha_{1,m}x_m = \beta_1 \\ \alpha_{2,2}x_2 + \cdots + \alpha_{2,m}x_m = \beta_2 \\ \vdots \\ \alpha_{n,2}x_1 + \cdots + \alpha_{1,n}x_m = \beta_m \\ 0 = \beta_{m+1} \\ \vdots \\ 0 = \beta_n \end{cases}$$

si l'un des β_i pour $i \in [\![m+1, n]\!]$ est non nul, alors le système est incompatible. Sinon, le système des équations principales est un système de Cramer, qui admet une unique solution. Dans ce cas, la matrice est de rang m.

Exemple 24. [GRI] p. 38

$$\begin{cases} x+2y-z=1 \\ 2x+3y+z=2 \\ x+4y-6z=2 \end{cases} \iff \begin{cases} x+2y-z=1 \\ -y+3z=0 \\ 2y-5z=1 \end{cases} \iff \begin{cases} x+2y-z=1 \\ -y+3z=0 \\ z=1 \end{cases}$$

On a pour unique solution $(-4,3,1)$.

c. Comparaison avec les formules de Cramer

Théorème 25. L'algorithme du pivot de Gauss pour résoudre un système $AX = B$ a un complexité de $O(n^3)$. L'utilisation des formules de Cramer se fait en $O(n(n+1)!)$. [FFN] p. 38

3. Conséquences théoriques

a. Familles libres

Proposition 26. La méthode du pivot permet de décider si une famille est libre (en échelonnant la matrice formée des vecteurs de cette famille). [GRI] p. 44

Exemple 27. La famille

$$\begin{pmatrix}1\\-2\\-3\end{pmatrix}, \begin{pmatrix}2\\3\\-1\end{pmatrix}, \begin{pmatrix}3\\2\\1\end{pmatrix}$$

est libre.

b. Rang, équivalence

Proposition 28. Soit $M \in \mathcal{M}_{n,m}(\mathbb{K})$ de rang r. Par des opérations élémentaires sur des lignes et des colonnes de M, on peut la transformer en

$$\begin{pmatrix}I_r & 0\\0 & 0\end{pmatrix}$$

[C-G] p. 24

c. Commutant d'une matrice

Soit $A \in \mathcal{M}_n(\mathbb{K})$.

Lemme 29. Si $\pi_A = \chi_A$, alors A est cyclique :

$$\exists x \in \mathbb{K}^n \setminus \{0\} \text{ tel que } (x, Ax, \dots, A^{n-1}x) \text{ est une base de } \mathbb{K}^n$$

[GOU21] p. 289

Notation 30.
— On note $\mathcal{T}_n(\mathbb{K})$ l'ensemble des matrices carrées triangulaires supérieures d'ordre n à coefficients dans le corps $\mathbb{K}$.
— On note $\mathscr{C}(A)$ le commutant de A.

[FGN2] p. 160

Lemme 31.

$$\dim_{\mathbb{K}}(\mathscr{C}(A)) \geq n$$

Lemme 32. Le rang de A est invariant par extension de corps.

[DEV]

Théorème 33.

$$\mathbb{K}[A] = \mathscr{C}(A) \iff \pi_A = \chi_A$$

IV - Décompositions

1. Décomposition LU

Définition 34. Les **sous-matrices principales** d'une matrice $(a_{i,j})_{i,j\in[\![1,n]\!]} \in \mathcal{M}_n(\mathbb{K})$ sont les matrices $A_k = (a_{i,j})_{i,j\in[\![1,k]\!]} \in \mathcal{M}_k(\mathbb{K})$ où $k \in [\![1,n]\!]$. Les **déterminants principaux** sont les déterminants des matrices A_k, pour $k \in [\![1,n]\!]$.

[ROM21] p. 690

Théorème 35 (Décomposition lower-upper)**.** Soit $A \in \mathrm{GL}_n(\mathbb{K})$. Alors, A admet une décomposition

$$A = LU$$

(où L est une matrice triangulaire inférieure à diagonale unité et U une matrice triangulaire supérieure) si et seulement si tous les déterminants principaux de A sont non nuls. Dans ce cas, une telle décomposition est unique.

Corollaire 36. Soit $A \in \mathrm{GL}_n(\mathbb{K}) \cap \mathcal{S}_n(\mathbb{K})$. Alors, on a l'unique décomposition de A :

$$A = LD^tL$$

où L est une matrice triangulaire inférieure et D une matrice diagonale.

Application 37 (Décomposition de Cholesky)**.** Soit $A \in \mathcal{M}_n(\mathbb{R})$. Alors, $A \in \mathcal{S}_n^{++}(\mathbb{R})$ si et seulement s'il existe $B \in \mathrm{GL}_n(\mathbb{R})$ triangulaire inférieure telle que $A = B^tB$. De plus, une telle décomposition est unique si on impose la positivité des coefficients diagonaux de B.

Exemple 38. On a la décomposition de Cholesky :

$$\begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

[GRI] p. 368

Proposition 39. Soit $A \in \mathrm{GL}_n(\mathbb{K})$ vérifiant les hypothèses du Théorème 35. On définit la suite (A_k) où $A_0 = A$ et $\forall k \in \mathbb{N}$, A_{k+1} est la matrice obtenue à partir de A_k à l'aide du pivot de Gauss sur la $(k+1)$-ième colonne. Alors, A_{n-1} est la matrice U de la décomposition $A = LU$ du Théorème 35.

[C-G] p. 257

Remarque 40. Pour résoudre un système linéaire $AX = Y$, on se ramène à $A = LU$ en $O\left(\frac{2}{3}n^3\right)$. Puis, on résout deux systèmes triangulaires "en cascade" :

$$LX' = Y \text{ puis } UX = X'$$

ceux-ci demandant chacun $O(2n^2)$ opérations.

Théorème 41 (Décomposition PLU)**.** Soit $A \in \mathrm{GL}_n(\mathbb{K})$. Alors, il existe $P \in \mathrm{GL}_n(\mathbb{K})$, matrice de permutations, telle que $P^{-1}A$ admet une décomposition LU.

2. Décomposition QR

Théorème 42 (Décomposition QR)**.** Soit $A \in \mathrm{GL}_n(\mathbb{R})$. Alors, A admet une décomposition

$$A = QR$$

où Q est une matrice orthogonale et R est une matrice triangulaire supérieure à coefficients diagonaux strictement positifs. On a unicité d'une telle décomposition.

[ROM21] p. 692

Corollaire 43 (Théorème d'Iwasawa)**.** Soit $A \in \mathrm{GL}_n(\mathbb{R})$. Alors, A admet une décomposition

$$A = QDR$$

où Q est une matrice orthogonale, D est une matrice diagonale à coefficients strictement positifs et R est une matrice triangulaire supérieure à coefficients diagonaux égaux à 1. On a unicité d'une telle décomposition.

Exemple 44. On a la factorisation QR suivante,

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} = \left(\frac{1}{\sqrt{6}} \begin{pmatrix} 0 & 2 & \sqrt{2} \\ \sqrt{3} & -1 & \sqrt{2} \\ \sqrt{3} & 1 & -\sqrt{2} \end{pmatrix} \right) \left(\frac{1}{\sqrt{6}} \begin{pmatrix} 2\sqrt{3} & \sqrt{3} & 1 \\ 0 & 3 & 1 \\ 0 & 0 & 2\sqrt{2} \end{pmatrix} \right)$$

qui peut être obtenue via un procédé de Gram-Schmidt.

[GRI] p. 272

Remarque 45. Pour résoudre un système linéaire $AX = Y$, si l'on a trouvé une telle factorisation $A = QR$, on résout

$$RX = {}^tQY$$

c'est-à-dire, un seul système triangulaire (contre deux pour la factorisation LU).

p. 368

170 Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.

Soit E un espace vectoriel sur un corps $\mathbb{K}$ et de dimension finie n.

I - Généralités

1. Définitions

Définition 1. Soit $\varphi : E \times E \to \mathbb{K}$ une application. [GOU21] p. 239

— On dit que φ est une **forme bilinéaire** sur E si pour tout $x \in E$, $y \mapsto \varphi(x,y)$ et pour tout $y \in E$, $x \mapsto \varphi(x,y)$ sont linéaires.

— Si de plus $\varphi(x,y) = \varphi(y,x)$ pour tout $x, y \in E$, on dit que φ est **symétrique**.

Définition 2. On appelle **forme quadratique** sur E toute application q de la forme

$$q : x \mapsto \varphi(x,x)$$

où φ est une forme bilinéaire sur E.

Exemple 3. Sur $\mathbb{R}^3$, $(x,y,z) \mapsto 3x^2 + y^2 + 2xy - 3xz$ définit une forme quadratique.

Proposition 4. Soit q une forme quadratique sur E. Il existe une unique forme bilinéaire symétrique φ telle que $q(x) = \varphi(x,x)$ pour tout $x \in E$. φ est la **forme polaire** de q, et on a

$$\forall x, y \in E,\ \varphi(x,y) = \frac{1}{2}(q(x+y) - q(x) - q(y)) = \frac{1}{4}(q(x+y) - q(x-y))$$

Exemple 5. Sur $\mathcal{M}_n(\mathbb{R})$, $A \mapsto \operatorname{trace}(A)^2$ est une forme quadratique, dont la forme polaire est $(A,B) \mapsto \operatorname{trace}(A)\operatorname{trace}(B)$. p. 248

2. Représentation matricielle

Définition 6. Soient q une forme quadratique sur E et $\mathscr{B} = (e_1, \dots, e_n)$ une base de E. On appelle **matrice** de q dans $\mathscr{B}$ la matrice $\mathrm{Mat}(q, \mathscr{B})$ définie par

$$\mathrm{Mat}(q, \mathscr{B}) = (\varphi(e_i, e_j))_{i,j \in [\![1,n]\!]}$$

où φ est la forme polaire de q. Le **rang** de q désigne le rang de cette matrice.

p. 229

Exemple 7. La matrice de la forme quadratique de l'Théorème 3 est

$$\begin{pmatrix} 3 & 1 & -\frac{3}{2} \\ 1 & 1 & 0 \\ -\frac{3}{2} & 0 & 0 \end{pmatrix}$$

Proposition 8. Soient $\mathscr{B}$ et $\mathscr{B}'$ deux bases de E dont on note P la matrice de passage entre ces bases. Soit q une forme quadratique sur E. Alors,

$$\mathrm{Mat}(q, \mathscr{B}) = {}^tP \mathrm{Mat}(q, \mathscr{B}') P$$

Remarque 9. En particulier, en reprenant les notations précédentes, $\mathrm{Mat}(q, \mathscr{B})$ et $\mathrm{Mat}(q, \mathscr{B}')$ sont équivalentes : le rang de q est bien défini et ne dépend pas de la base considérée.

II - Orthogonalité et isotropie

Soit q une forme quadratique sur E de forme polaire φ.

1. Définitions et propriétés

Définition 10. — On appelle **cône isotrope** de q l'ensemble

$$C_q = \{x \in E \mid q(x) = 0\}$$

— q est dite **définie** si $C_q = \{0\}$.

— Les vecteurs de C_q sont dits **isotropes** pour q.

Exemple 11. La forme quadratique définie sur $\mathbb{R}^3$ par $(x, y, z) \mapsto 4x^2 + 3y^2 + 5xy - 3xz + 8yz$ n'est pas définie car $(0, 0, 1)$ est un vecteur isotrope non nul.

[GRI] p. 303

[GOU21] p. 242

Définition 12. — Deux vecteurs $x, y \in E$ sont dits q-**orthogonaux** si $\varphi(x,y) = 0$. On note cela $x \perp y$.

— Si $A \subseteq E$, on appelle **orthogonal** de A l'ensemble $A^\perp = \{y \in E \mid \forall x \in A,\ x \perp y\}$.

Proposition 13. (i) Si $A \subseteq E$, $A^\perp = (\mathrm{Vect}(A))^\perp$.

(ii) Si $A \subseteq E$, $A \subseteq A^{\perp\perp}$.

(iii) Si $A \subseteq B \subseteq E$, $B^\perp \subseteq A^\perp$.

Définition 14. — On appelle **noyau** de q le sous-espace vectoriel

$$\mathrm{Ker}(q) = E^\perp$$

— On dit que q est **non-dégénérée** si $\mathrm{Ker}(q) = \{0\}$ et **dégénérée** si $\mathrm{Ker}(q) \neq \{0\}$.

Proposition 15. On a $\mathrm{Ker}(q) \subseteq C_q$. En particulier, si q est définie, alors q est non dégénérée.

Exemple 16. Sur $\mathbb{R}^2$, $(x,y) \mapsto x^2 - y^2$ est une forme quadratique non dégénérée mais non définie non plus.

Proposition 17. Soit F un sous-espace vectoriel de E.

(i) $\dim(E) = \dim(F) + \dim(F^\perp) - \dim(F \cap \mathrm{Ker}(q))$.

(ii) $F^{\perp\perp} = F + \mathrm{Ker}(q)$.

(iii) Si la restriction de q à F $q_{|F}$ est définie, alors $E = F \oplus F^\perp$.

(iv) Si q est définie, $F = F^{\perp\perp}$.

Proposition 18. Soit A la matrice de q dans une base $\mathscr{B}$. Alors,

$$\mathrm{Ker}(A) = \mathrm{Ker}(q)$$

Corollaire 19. q est non dégénérée si et seulement si $\det(\mathrm{Mat}(q,\mathscr{B})) \neq 0$ pour une base quelconque $\mathscr{B}$ de E.

[GRI] p. 296

Exemple 20. Sur $\mathbb{R}^4$, $(x,y) \mapsto x^2 + y^2 + z^2 - t^2$ est non dégénérée (car de déterminant -1).

2. Bases q-orthogonales

Définition 21. Une base de E est dite **q-orthogonale** si ses vecteurs sont deux à deux q-orthogonaux.

[GOU21] p. 243

Remarque 22. Si $(e_1, \dots, e_n)$ est une base q-orthogonale, alors

$$\forall (x_1, \dots, x_n) \in \mathbb{K}^n,\ q\left(\sum_{i=1}^{n} x_i e_i\right) = \sum_{i=1}^{n} x_i^2 q(e_i)$$

Théorème 23. Il existe une base q-orthogonale de E.

Remarque 24. Si $\mathscr{B} = (e_1, \dots, e_n)$ est une base q-orthogonale, en posant $\lambda_i = q(e_i)$ pour tout $i \in [\![1, n]\!]$, on a

$$\forall x \in E,\ q(x) = q\left(\sum_{i=1}^{n} e_i^*(x) e_i\right) = \sum_{i=1}^{n} \lambda_i (e_i^*(x))^2$$

où $(e_1^*, \dots, e_n^*)$ est la base duale de $\mathscr{B}$.

Théorème 25 (Méthode de Gauss)**.** On écrit

$$q(x_1, \dots, x_n) = \sum_{i=1}^{n} a_{i,i} x_i^2 + \sum_{1 \le i < j \le n} a_{i,j} x_i x_j$$

et on cherche à écrire q comme combinaison linéaire de carrés de formes linéaires indépendantes. On a deux cas :

(i) Il existe $i \in [\![1, n]\!]$ tel que $a_{i,i} \neq 0$. On peut suppose $i = 1$, on pose alors $a = a_{1,1}$. On réécrit q sous la forme :

$$\begin{aligned} q(x_1, \dots, x_n) &= a x_1^2 + x_1 B(x_2, \dots, x_n) + C(x_2, \dots, x_n) \\ &= a\left(x_1 + \frac{B(x_2, \dots, x_n)}{2a}\right)^2 + \left(C(x_2, \dots, x_n) - \frac{B(x_2, \dots, x_n)^2}{4a}\right) \end{aligned}$$

où B est une forme linéaire et C une forme quadratique. On itère alors le procédé avec $C - \frac{B^2}{4a}$.

(ii) Sinon. Si $q = 0$, c'est terminé. Sinon, il existe un $a_{i,j}$ non nul. On peut suppose $(i, j) = (1, 2)$, on pose alors $a = a_{1,2}$. On réécrit q sous la forme :

$$q(x_1, \dots, x_n) = a x_1 x_2 + x_1 B(x_3, \dots, x_n) + x_2 C(x_3, \dots, x_n) + D(x_3, \dots, x_n)$$

où B et C sont des formes linéaires et D une forme quadratique. En utilisant une

identité remarquable :

$$\begin{aligned} q &= a\left(x_1 + \frac{C}{a}\right)\left(x_2 + \frac{B}{a}\right) + \left(D - \frac{BA}{a}\right) \\ &= \frac{a}{4}\left(\left(x_1 + x_2 + \frac{B+C}{a}\right)^2 - \left(x_1 - x_2 + \frac{C-B}{a}\right)^2\right) + \left(D - \frac{BC}{a}\right) \end{aligned}$$

On itère alors le procédé avec $D - \frac{BC}{a}$.

Exemple 26. Sur $\mathbb{R}^3$,

$$\begin{aligned} q(x,y,z) &= x^2 - 2y^2 + xz + yz \\ &= \left(x + \frac{z}{2}\right)^2 - \frac{z^2}{4} - 2y^2 + yz \\ &= \left(x + \frac{z}{2}\right)^2 - 2\left(y - \frac{z}{4}\right)^2 + \frac{z^2}{8} - \frac{z^2}{4} \\ &= \left(x + \frac{z}{2}\right)^2 - 2\left(y - \frac{z}{4}\right)^2 - \frac{z^2}{8} \end{aligned}$$

III - Classification des formes quadratiques

Soit q une forme quadratique sur E.

1. Si $\mathbb{K} = \mathbb{C}$

On suppose $\mathbb{K} = \mathbb{C}$.

Théorème 27. Il existe une base $\mathscr{B} = (e_1, \dots, e_n)$ de E telle que, si $x = \sum_{i=1}^n x_i e_i \in E$, on a

$$q(x) = \sum_{i=1}^n x_i^2$$

[GRI] p. 308

Remarque 28. En reprenant les notations précédentes,

$$\mathrm{Mat}(q, \mathscr{B}) = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$$

où r est le rang de q et I_r la matrice identité de taille r.

Corollaire 29. Il existe une base q-orthonormée (ie. $q(e_i) = 1$ pour tout $i \in [\![1, n]\!]$) si et seulement si $\mathrm{rang}(q) = n$ (ie. q est non dégénérée).

2. Si $\mathbb{K} = \mathbb{R}$

On suppose $\mathbb{K} = \mathbb{R}$.

Définition 30. q est dite **positive** (resp. **négative**) si pour tout $x \in E$, $q(x) \geq 0$ (resp. $q(x) \leq 0$). [GOU21] p. 246

[DEV]

Théorème 31 (Loi d'inertie de Sylvester)**.**

$$\exists p, q \in \mathbb{N} \text{ et } \exists f_1, \dots, f_{p+q} \in E^* \text{ tels que } q = \sum_{i=1}^{p} |f_i|^2 - \sum_{i=p+1}^{q} |f_i|^2$$

où les formes linéaires f_i sont linéairement indépendantes et où $p + q \leq n$. De plus, ces entiers ne dépendent que de q et pas de la décomposition choisie.

Le couple (p, q) est la **signature** de q et le rang q est égal à $p + q$.

Remarque 32. En reprenant les notations précédentes, il existe donc une base $\mathscr{B}$ telle que

$$\mathrm{Mat}(q, \mathscr{B}) = \begin{pmatrix} I_p & 0 & 0 \\ 0 & -I_q & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

où r est le rang de q et I_r la matrice identité de taille r.

Corollaire 33. On note $\mathrm{sign}(q)$ la signature de q. [GRI] p. 310

(i) q est définie positive si et seulement si $\mathrm{sign}(q) = (n, 0)$ si et seulement s'il existe des bases q-orthonormées.

(ii) q est définie négative si et seulement si $\mathrm{sign}(q) = (0, n)$.

(iii) q est non dégénérée si et seulement si $\mathrm{sign}(q) = (p, n - p)$.

Exemple 34. En reprenant l'Théorème 26, on a $\mathrm{sign}(q) = (1, 2)$: q est de rang 3. [GOU21] p. 247

Proposition 35. Si q est définie, alors ou bien q est positive, ou bien q est négative.

3. Si $\mathbb{K} = \mathbb{F}_{p^n}$

On suppose $\mathbb{K} = \mathbb{F}_{p^n}$ où $p, n \in \mathbb{N}$ avec p premier.

Définition 36. On appelle **discriminant** de q le déterminant de sa matrice dans une base de E.

[PER] p. 130

Théorème 37. Soit $\alpha \in \mathbb{F}_{p^n}$ un non-résidu quadratique modulo p^n. Alors, on a deux classes d'équivalence de formes quadratiques non dégénérées sur E, de matrices congrues à :

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & \ddots & 1 & 0 \\ 0 & \dots & \dots & 0 & \alpha \end{pmatrix} \text{ ou } \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & \ddots & 1 & 0 \\ 0 & \dots & \dots & 0 & 1 \end{pmatrix}$$

q est de l'un ou l'autre type suivant que son discriminant est, ou non, un carré de $\mathbb{F}_{p^n}$.

IV - Applications

1. Produit scalaire

On suppose de nouveau $\mathbb{K} = \mathbb{R}$.

Définition 38. On appelle **produit scalaire** sur E la forme polaire d'une forme quadratique définie positive.

[GOU21] p. 252

Proposition 39 (Inégalité de Cauchy-Schwarz)**.** Soit q une forme quadratique positive sur E de forme polaire φ. Alors,

$$\forall x, y \in E, \varphi(x,y)^2 \leq q(x)q(y)$$

Si de plus q est définie, il y a égalité si et seulement si x et y sont colinéaires.

p. 246

Proposition 40 (Inégalité de Minkowski)**.** Soit q une forme quadratique positive sur E. Alors,

$$\forall x, y \in E, \sqrt{q(x+y)} \leq \sqrt{q(x)}\sqrt{q(y)}$$

Corollaire 41. Soit φ un produit scalaire sur E. Alors,

$$\|.\|_\varphi : x \mapsto \sqrt{\varphi(x,x)}$$

est une norme sur E.

Proposition 42 (Identité du parallélogramme)**.** En reprenant les notations précédentes,

$$\forall x, y \in E,\ \|x+y\|_\varphi^2 + \|x-y\|_\varphi^2 = 2(\|x\|_\varphi^2 \|y\|_\varphi^2)$$

et cette identité caractérise les normes issues d'un produit scalaire.

[LI] p. 62

2. Racines de polynômes

Soit $P \in \mathbb{R}[X]$ un polynôme de degré n.

[C-G] p. 356

Notation 43. On note :

— $x_1, \dots, x_t$ les racines complexes de P de multiplicités respectives $m_1, \dots, m_t$.

— $s_0 = n$ et $\forall k \geq 1$, $s_k = \sum_{i=1}^t m_i x_i^k$.

Proposition 44. $\sigma = \sum_{i,j \in [\![0,n-1]\!]} s_{i+j} X_i X_j$ définit une forme quadratique sur $\mathbb{C}^n$ ainsi qu'une forme quadratique $\sigma_\mathbb{R}$ sur $\mathbb{R}^n$.

[DEV]

Théorème 45 (Formes de Hankel)**.** On note (p,q) la signature de $\sigma_\mathbb{R}$, on a :

— $t = p+q$.

— Le nombre de racines réelles distinctes de P est $p-q$.

3. En analyse

Soit $U \subseteq \mathbb{R}^n$ un ouvert.

Lemme 46. Soit $A_0 \in \mathcal{S}_n(\mathbb{R})$ inversible. Alors il existe un voisinage V de A_0 dans $\mathcal{S}_n(\mathbb{R})$ et une application $\psi : V \to \mathrm{GL}_n(\mathbb{R})$ de classe $\mathcal{C}^1$ telle que

$$\forall A \in V,\ A = {}^t\psi(A) A_0 \psi(A)$$

[ROU] p. 209

Lemme 47 (Morse)**.** Soit $f : U \to \mathbb{R}$ une fonction de classe $\mathcal{C}^3$ (où U désigne un ouvert de $\mathbb{R}^n$ contenant l'origine). On suppose :

— $\mathrm{d}f_0 = 0$.

— La matrice symétrique $\mathrm{Hess}(f)_0$ est inversible.

— La signature de $\mathrm{Hess}(f)_0$ est $(p, n-p)$.

Alors il existe un difféomorphisme $\phi = (\phi_1, \dots, \phi_n)$ de classe $\mathcal{C}^1$ entre deux voisinage de

p. 354

l'origine de $\mathbb{R}^n$ $V \subseteq U$ et W tel que $\varphi(0) = 0$ et

$$\forall x \in U,\ f(x) - f(0) = \sum_{k=1}^{p} \phi_k^2(x) - \sum_{k=p+1}^{n} \phi_k^2(x)$$

p. 341

Application 48. Soit S la surface d'équation $z = f(x,y)$ où f est de classe $\mathscr{C}^3$ au voisinage de l'origine. On suppose la forme quadratique $\mathrm{d}^2 f_0$ non dégénérée. Alors, en notant P le plan tangent à S en 0 :

(i) Si $\mathrm{d}^2 f_0$ est de signature $(2,0)$, alors S est au-dessus de P au voisinage de 0.

(ii) Si $\mathrm{d}^2 f_0$ est de signature $(0,2)$, alors S est en-dessous de P au voisinage de 0.

(iii) Si $\mathrm{d}^2 f_0$ est de signature $(1,1)$, alors S traverse P selon une courbe admettant un point double en $(0, f(0))$.

171 Formes quadratiques réelles. Coniques. Exemples et applications.

Soit E un espace vectoriel sur $\mathbb{R}$ de dimension finie n.

I - Formes quadratiques réelles

1. Définitions

Définition 1. Soit $\varphi : E \times E \to \mathbb{K}$ une application. [GOU21] p. 239

- On dit que φ est une **forme bilinéaire** sur E si pour tout $x \in E$, $y \mapsto \varphi(x,y)$ et pour tout $y \in E$, $x \mapsto \varphi(x,y)$ sont linéaires.
- Si de plus $\varphi(x,y) = \varphi(y,x)$ pour tout $x, y \in E$, on dit que φ est **symétrique**.

Définition 2. On appelle **forme quadratique** sur E toute application q de la forme

$$q : x \mapsto \varphi(x,x)$$

où φ est une forme bilinéaire sur E.

Exemple 3. Sur $\mathbb{R}^3$, $(x,y,z) \mapsto 3x^2 + y^2 + 2xy - 3xz$ définit une forme quadratique.

Proposition 4. Soit q une forme quadratique sur E. Il existe une unique forme bilinéaire symétrique φ telle que $q(x) = \varphi(x,x)$ pour tout $x \in E$. φ est la **forme polaire** de q, et on a

$$\forall x, y \in E,\ \varphi(x,y) = \frac{1}{2}(q(x+y) - q(x) - q(y)) = \frac{1}{4}(q(x+y) - q(x-y))$$

Exemple 5. Sur $\mathcal{M}_n(\mathbb{R})$, $A \mapsto \operatorname{trace}(A)^2$ est une forme quadratique, dont la forme polaire est $(A,B) \mapsto \operatorname{trace}(A)\operatorname{trace}(B)$. p. 248

2. Représentation matricielle

Définition 6. Soient q une forme quadratique sur E et $\mathscr{B} = (e_1, \dots, e_n)$ une base de E. On appelle **matrice** de q dans $\mathscr{B}$ la matrice $\mathrm{Mat}(q, \mathscr{B})$ définie par

$$\mathrm{Mat}(q, \mathscr{B}) = (\varphi(e_i, e_j))_{i,j \in [\![1,n]\!]}$$

où φ est la forme polaire de q. Le **rang** de q désigne le rang de cette matrice.

p. 229

Exemple 7. La matrice de la forme quadratique de l'Théorème 3 est

$$\begin{pmatrix} 3 & 1 & -\frac{3}{2} \\ 1 & 1 & 0 \\ -\frac{3}{2} & 0 & 0 \end{pmatrix}$$

Proposition 8. Soient $\mathscr{B}$ et $\mathscr{B}'$ deux bases de E dont on note P la matrice de passage entre ces bases. Soit q une forme quadratique sur E. Alors,

$$\mathrm{Mat}(q, \mathscr{B}) = {}^tP \mathrm{Mat}(q, \mathscr{B}')P$$

Remarque 9. En particulier, en reprenant les notations précédentes, $\mathrm{Mat}(q, \mathscr{B})$ et $\mathrm{Mat}(q, \mathscr{B}')$ sont équivalentes : le rang de q est bien défini et ne dépend pas de la base considérée.

II - Orthogonalité et isotropie

Soit q une forme quadratique sur E de forme polaire φ.

Définition 10. — On appelle **cône isotrope** de q l'ensemble

$$C_q = \{x \in E \mid q(x) = 0\}$$

— q est dite **définie** si $C_q = \{0\}$.

— Les vecteurs de C_q sont dits **isotropes** pour q.

Exemple 11. La forme quadratique définie sur $\mathbb{R}^3$ par $(x, y, z) \mapsto 4x^2 + 3y^2 + 5xy - 3xz + 8yz$ n'est pas définie car $(0, 0, 1)$ est un vecteur isotrope non nul.

[GRI] p. 303

Définition 12. — Deux vecteurs $x, y \in E$ sont dits q-**orthogonaux** si $\varphi(x, y) = 0$. On note cela $x \perp y$.

[GOU21] p. 242

— Si $A \subseteq E$, on appelle **orthogonal** de A l'ensemble $A^\perp = \{y \in E \mid \forall x \in A,\ x \perp y\}$.

Proposition 13. (i) Si $A \subseteq E$, $A^\perp = (\mathrm{Vect}(A))^\perp$.
(ii) Si $A \subseteq E$, $A \subseteq A^{\perp\perp}$.
(iii) Si $A \subseteq B \subseteq E$, $B^\perp \subseteq A^\perp$.

Définition 14. — On appelle **noyau** de q le sous-espace vectoriel

$$\mathrm{Ker}(q) = E^\perp$$

— On dit que q est **non-dégénérée** si $\mathrm{Ker}(q) = \{0\}$ et **dégénérée** si $\mathrm{Ker}(q) \neq \{0\}$.

Proposition 15. On a $\mathrm{Ker}(q) \subseteq C_q$. En particulier, si q est définie, alors q est non dégénérée.

Exemple 16. Sur $\mathbb{R}^2$, $(x,y) \mapsto x^2 - y^2$ est une forme quadratique non dégénérée mais non définie non plus.

Proposition 17. Soit F un sous-espace vectoriel de E.
(i) $\dim(E) = \dim(F) + \dim(F^\perp) - \dim(F \cap \mathrm{Ker}(q))$.
(ii) $F^{\perp\perp} = F + \mathrm{Ker}(q)$.
(iii) Si la restriction de q à F $q_{|F}$ est définie, alors $E = F \oplus F^\perp$.
(iv) Si q est définie, $F = F^{\perp\perp}$.

Proposition 18. Soit A la matrice de q dans une base $\mathscr{B}$. Alors,

$$\mathrm{Ker}(A) = \mathrm{Ker}(q)$$

Corollaire 19. q est non dégénérée si et seulement si $\det(\mathrm{Mat}(q,\mathscr{B})) \neq 0$ pour une base quelconque $\mathscr{B}$ de E.

[GRI] p. 296

Exemple 20. Sur $\mathbb{R}^4$, $(x,y) \mapsto x^2 + y^2 + z^2 - t^2$ est non dégénérée (car de déterminant -1).

III - Classification

1. Bases orthogonales

Définition 21. Une base de E est dite q-**orthogonale** si ses vecteurs sont deux à deux q-orthogonaux.

[GOU21] p. 243

Remarque 22. Si $(e_1,\dots,e_n)$ est une base q-orthogonale, alors

$$\forall (x_1,\dots,x_n)\in\mathbb{K}^n,\ q\left(\sum_{i=1}^n x_i e_i\right)=\sum_{i=1}^n x_i^2 q(e_i)$$

Théorème 23. Il existe une base q-orthogonale de E.

Remarque 24. Si $\mathscr{B}=(e_1,\dots,e_n)$ est une base q-orthogonale, en posant $\lambda_i=q(e_i)$ pour tout $i\in[\![1,n]\!]$, on a

$$\forall x\in E,\ q(x)=q\left(\sum_{i=1}^n e_i^*(x)e_i\right)=\sum_{i=1}^n \lambda_i (e_i^*(x))^2$$

où $(e_1^*,\dots,e_n^*)$ est la base duale de $\mathscr{B}$.

2. Algorithme de Gauss

Théorème 25 (Méthode de Gauss)**.** On écrit

$$q(x_1,\dots,x_n)=\sum_{i=1}^n a_{i,i}x_i^2+\sum_{1\le i<j\le n} a_{i,j}x_i x_j$$

et on cherche à écrire q comme combinaison linéaire de carrés de formes linéaires indépendantes. On a deux cas :

(i) Il existe $i\in[\![1,n]\!]$ tel que $a_{i,i}\neq 0$. On peut suppose $i=1$, on pose alors $a=a_{1,1}$. On réécrit q sous la forme :

$$\begin{aligned} q(x_1,\dots,x_n) &= ax_1^2+x_1B(x_2,\dots,x_n)+C(x_2,\dots,x_n)\\ &= a\left(x_1+\frac{B(x_2,\dots,x_n)}{2a}\right)^2+\left(C(x_2,\dots,x_n)-\frac{B(x_2,\dots,x_n)^2}{4a}\right)\end{aligned}$$

où B est une forme linéaire et C une forme quadratique. On itère alors le procédé avec $C-\frac{B^2}{4a}$.

(ii) Sinon. Si $q=0$, c'est terminé. Sinon, il existe un $a_{i,j}$ non nul. On peut suppose $(i,j)=$

$(1,2)$, on pose alors $a = a_{1,2}$. On réécrit q sous la forme :

$$q(x_1,\dots,x_n) = ax_1x_2 + x_1B(x_3,\dots,x_n) + x_2C(x_3,\dots,x_n) + D(x_3,\dots,x_n)$$

où B et C sont des formes linéaires et D une forme quadratique. En utilisant une identité remarquable :

$$\begin{aligned} q &= a\left(x_1 + \frac{C}{a}\right)\left(x_2 + \frac{B}{a}\right) + \left(D - \frac{BA}{a}\right) \\ &= \frac{a}{4}\left(\left(x_1 + x_2 + \frac{B+C}{a}\right)^2 - \left(x_1 - x_2 + \frac{C-B}{a}\right)^2\right) + \left(D - \frac{BC}{a}\right) \end{aligned}$$

On itère alors le procédé avec $D - \frac{BC}{a}$.

Exemple 26. Sur $\mathbb{R}^3$,

$$\begin{aligned} q(x,y,z) &= x^2 - 2y^2 + xz + yz \\ &= \left(x + \frac{z}{2}\right)^2 - \frac{z^2}{4} - 2y^2 + yz \\ &= \left(x + \frac{z}{2}\right)^2 - 2\left(y - \frac{z}{4}\right)^2 + \frac{z^2}{8} - \frac{z^2}{4} \\ &= \left(x + \frac{z}{2}\right)^2 - 2\left(y - \frac{z}{4}\right)^2 - \frac{z^2}{8} \end{aligned}$$

3. Signature

Définition 27. q est dite **positive** (resp. **négative**) si pour tout $x \in E$, $q(x) \geq 0$ (resp. $q(x) \leq 0$).

[DEV]

Théorème 28 (Loi d'inertie de Sylvester)**.**

$$\exists p,q \in \mathbb{N} \text{ et } \exists f_1,\dots,f_{p+q} \in E^* \text{ tels que } q = \sum_{i=1}^{p} |f_i|^2 - \sum_{i=p+1}^{p+q} |f_i|^2$$

où les formes linéaires f_i sont linéairement indépendantes et où $p+q \leq n$. De plus, ces entiers ne dépendent que de q et pas de la décomposition choisie.

Le couple (p,q) est la **signature** de q et le rang q est égal à $p+q$.

Remarque 29. En reprenant les notations précédentes, il existe donc une base $\mathscr{B}$ telle que

$$\mathrm{Mat}(q,\mathscr{B}) = \begin{pmatrix} I_p & 0 & 0 \\ 0 & -I_q & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

où r est le rang de q et I_r la matrice identité de taille r.

Corollaire 30. On note $\mathrm{sign}(q)$ la signature de q. [GRI] p. 310

(i) q est définie positive si et seulement si $\mathrm{sign}(q) = (n,0)$ si et seulement s'il existe des bases q-orthonormées.

(ii) q est définie négative si et seulement si $\mathrm{sign}(q) = (0,n)$.

(iii) q est non dégénérée si et seulement si $\mathrm{sign}(q) = (p, n-p)$.

Exemple 31. En reprenant l'Théorème 26, on a $\mathrm{sign}(q) = (1,2)$: q est de rang 3. [GOU21] p. 247

Proposition 32. Si q est définie, alors ou bien q est positive, ou bien q est négative.

IV - Applications

1. Coniques

On suppose $E = \mathbb{R}^2$ et muni d'un produit scalaire $\langle .,. \rangle$. [GRI] p. 427

a. Aspect algébrique

Définition 33. On appelle **conique** un ensemble

$$\mathscr{C} = \{v \in E \mid q(v) + \varphi(v) = k,\ k \in \mathbb{R}\}$$

où q est une forme quadratique non nulle et φ une forme linéaire sur E.

On gardera les notations de cette définition pour la suite.

Remarque 34.
— En changeant éventuellement le signe des deux membres de l'équation, on peut supposer que a signature de q est $(2,0)$, $(1,1)$ ou $(1,0)$.
— Si (e_1, e_2) est la base de E, avec $v = xe_1 + ye_2$, on trouve que l'équation d'une conique est du type

$$\alpha x^2 + 2\beta xy + \gamma y^2 + \lambda x + \mu y = k,\ k \in \mathbb{R}$$

Proposition 35. Il existe une base orthogonale (v_1, v_2) pour q et $\langle .,. \rangle$. Dans cette base, l'équation de la conique est du type

$$ax^2 + by^2 - 2rx - 2sy = k,\ k \in \mathbb{R} \qquad (E)$$

Définition 36. En reprenant les notations précédentes, les directions définies par v_1 et v_2 sont appelés **directions principales** de la conique.

Théorème 37 (Classification des coniques)**.** (i) Si q est non dégénérée : On peut réécrire l'équation (E) de manière équivalente sous la forme

$$ax^2 + by^2 = h$$

avec $a, b, h \in \mathbb{R}$.

- Si $\text{sign}(q) = (2,0)$: si $h = 0$, $\mathscr{C}$ se réduit à un point ; si $h < 0$, $\mathscr{C} = \emptyset$. Supposons que $h > 0$, alors $\mathscr{C}$ est une ellipse, de centre $\left(\frac{r}{a}, \frac{s}{b}\right)$.
- Si $\text{sign}(q) = (1,1)$: si $h \neq 0$, $\mathscr{C}$ est une hyperbole. Si $h = 0$, $\mathscr{C}$ se réduit aux deux droites d'équation $y = \pm\sqrt{\left|\frac{a}{b}\right|}x$.

(ii) Si q est dégénérée : On a $ab = 0$ et sign(q) = (1,0) ; on peut réécrire l'équation (E) de manière équivalente sous la forme

$$a\left(x - \frac{r}{a}\right)^2 - 2sy = h$$

avec $h \in \mathbb{R}$.

- Si $s \neq 0$: $\mathscr{C}$ est une parabole.
- Si $s = 0$: si $h = 0$, $\mathscr{C}$ se réduit à la droite $x = 0$; si $h < 0$, $\mathscr{C} = \emptyset$. Supposons que $h > 0$, alors $\mathscr{C}$ est constituée des deux droites parallèles d'équation $x = \pm h$.

b. Aspect géométrique

Proposition 38. En se plaçant dans le plan affine $\mathbb{R}^2$, plongé dans $\mathbb{R}^3$, une conique est l'intersection d'un cône et d'un plan.

[ROM21] p. 494

2. En analyse

Soit $U \subseteq \mathbb{R}^n$ un ouvert.

a. Optimisation

Soit $f : U \to \mathbb{R}$ de classe $\mathscr{C}^2$ sur U.

Théorème 39. On suppose $\mathrm{d}f_a = 0$ (a est un **point critique** de f). Alors : [GOU20] p. 336

(i) Si f admet un minimum (resp. maximum) relatif en a, $\mathrm{Hess}(f)_a$ est positive (resp. négative).

(ii) Si $\mathrm{Hess}(f)_a$ définit une forme quadratique définie positive (resp. définie négative), f admet un minimum (resp. maximum) relatif en a.

Exemple 40. On suppose $\mathrm{d}f_a = 0$. On pose $(r,s,t) = \left(\frac{\partial^2}{\partial x_i \partial x_j} f\right)_{i+j=2}$. Alors :

(i) Si $rt - s^2 > 0$ et $r > 0$ (resp. $r < 0$), f admet une minimum (resp. maximum) relatif en a.

(ii) Si $rt - s^2 < 0$, f n'a pas d'extremum en a.

(iii) Si $rt - s^2 = 0$, on ne peut rien conclure.

Exemple 41. La fonction $(x,y) \mapsto x^4 + y^2 - 2(x-y)^2$ a trois points critiques qui sont des minimum locaux : $(0,0)$, $(\sqrt{2}, -\sqrt{2})$ et $(-\sqrt{2}, \sqrt{2})$.

Contre-exemple 42. $x \mapsto x^3$ a sa hessienne positive en 0, mais n'a pas d'extremum en 0.

b. Homéomorphismes

Lemme 43. Soit $A_0 \in \mathscr{S}_n(\mathbb{R})$ inversible. Alors il existe un voisinage V de A_0 dans $\mathscr{S}_n(\mathbb{R})$ et une application $\psi : V \to \mathrm{GL}_n(\mathbb{R})$ de classe $\mathscr{C}^1$ telle que [ROU] p. 209

$$\forall A \in V,\ A = {}^t\psi(A) A_0 \psi(A)$$

Lemme 44 (Morse)**.** Soit $f : U \to \mathbb{R}$ une fonction de classe $\mathscr{C}^3$ (où U désigne un ouvert de $\mathbb{R}^n$ contenant l'origine). On suppose : p. 354

— $\mathrm{d}f_0 = 0$.

— La matrice symétrique $\mathrm{Hess}(f)_0$ est inversible.

— La signature de $\mathrm{Hess}(f)_0$ est $(p, n-p)$.

Alors il existe un difféomorphisme $\phi = (\phi_1, \dots, \phi_n)$ de classe $\mathscr{C}^1$ entre deux voisinage de l'origine de $\mathbb{R}^n$ $V \subseteq U$ et W tel que $\varphi(0) = 0$ et

$$\forall x \in U,\ f(x) - f(0) = \sum_{k=1}^{p} \phi_k^2(x) - \sum_{k=p+1}^{n} \phi_k^2(x)$$

Application 45. Soit S la surface d'équation $z = f(x,y)$ où f est de classe $\mathscr{C}^3$ au voisinage de l'origine. On suppose la forme quadratique $\mathrm{d}^2 f_0$ non dégénérée. Alors, en notant P le plan tangent à S en 0 : p. 341

(i) Si $\mathrm{d}^2 f_0$ est de signature $(2,0)$, alors S est au-dessus de P au voisinage de 0.

(ii) Si $\mathrm{d}^2 f_0$ est de signature $(0,2)$, alors S est en-dessous de P au voisinage de 0.

(iii) Si $\mathrm{d}^2 f_0$ est de signature $(1,1)$, alors S traverse P selon une courbe admettant un point double en $(0, f(0))$.

3. Racines de polynômes

Soit $P \in \mathbb{R}[X]$ un polynôme de degré n.

[C-G] p. 356

Notation 46. On note :

— $x_1, \dots, x_t$ les racines complexes de P de multiplicités respectives $m_1, \dots, m_t$.

— $s_0 = n$ et $\forall k \geq 1$, $s_k = \sum_{i=1}^{t} m_i x_i^k$.

Proposition 47. $\sigma = \sum_{i,j \in [\![0,n-1]\!]} s_{i+j} X_i X_j$ définit une forme quadratique sur $\mathbb{C}^n$ ainsi qu'une forme quadratique $\sigma_{\mathbb{R}}$ sur $\mathbb{R}^n$.

[DEV]

Théorème 48 (Formes de Hankel)**.** On note (p,q) la signature de $\sigma_{\mathbb{R}}$, on a :

— $t = p + q$.

— Le nombre de racines réelles distinctes de P est $p - q$.

Annexes

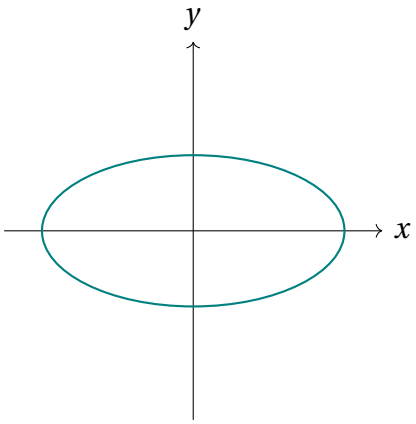


FIGURE I.11 – Une ellipse ($\text{sign}(q) = (2,0)$).

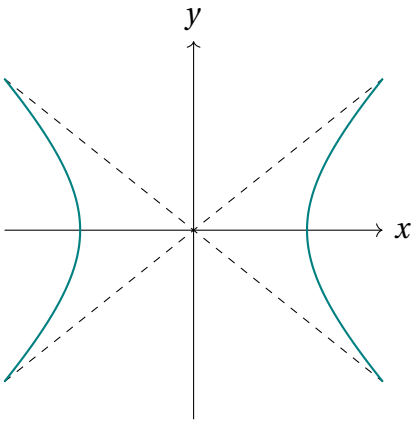


FIGURE I.12 – Une hyperbole ($\text{sign}(q) = (1,1)$).

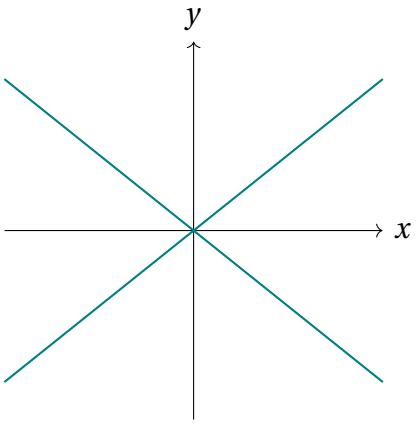


FIGURE I.13 – Une hyperbole dégénérée en deux droites sécantes ($\text{sign}(q) = (1,1)$).

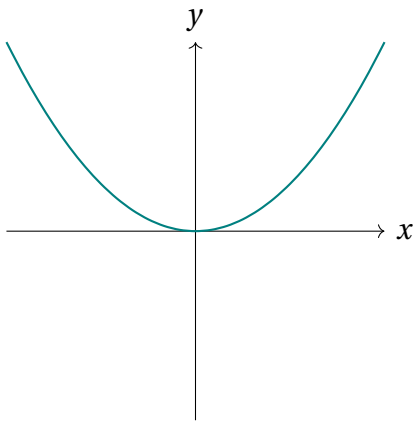


FIGURE I.14 – Une parabole ($\text{sign}(q) = (1,0)$).

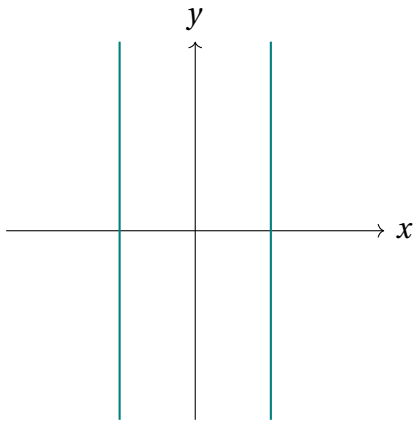


FIGURE I.15 – Une parabole dégénérée en deux droites parallèles ($\text{sign}(q) = (1,0)$).

190 Méthodes combinatoires, problèmes de dénombrement.

I - Dénombrement

1. Principes de base

Définition 1. On dit qu'un ensemble E est **fini** s'il est vide ou s'il existe $n \in \mathbb{N}^*$ tel qu'il existe une bijection de $[\![1, n]\!]$ dans E. Dans ce cas, l'entier n ne dépend pas de la bijection, on l'appelle **cardinal** de E. Il est noté $|E|$. Si E est vide, on pose $|E| = 0$.

[GOU21] p. 299

Proposition 2. Soient E et F deux ensembles.

(i) Si E est fini et s'il existe une injection de E vers F, alors E est fini et $|E| \leq |F|$.

(ii) Si E est fini et s'il existe une surjection de E vers F, alors F est fini et $|E| \geq |F|$.

(iii) Si E et s'il existe une bijection de E vers F, alors F est fini et $|E| = |F|$.

Corollaire 3. Soit B un ensemble fini et $A \subseteq B$. Alors A est fini et $|A| \leq |B|$. Si $|A| = |B|$, alors $A = B$.

Corollaire 4 (Principe des tiroirs)**.** Soient E et F deux ensembles finis avec $|E| > |F|$. Si φ est une application de E vers F, alors il existe $y \in F$ ayant au moins deux antécédents par φ dans E.

Remarque 5 (Interprétation). Si on doit ranger $n+1$ chaussettes dans n tiroirs, alors un des tiroirs (au moins) contiendra deux chaussettes ou plus.

Proposition 6. Soient A et B deux ensembles finis. Alors,

(i) $|A \cup B| = |A| + |B| - |A \cap B|$.

(ii) $|A \smallsetminus B| = |A| - |A \cap B|$.

Proposition 7 (Formule du crible de Poincaré)**.** Soient $A_1, \dots, A_n$ des ensembles finis. Alors,

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \leq i_1 < \cdots < i_k \leq n} |A_{i_1} \cap \dots \cap A_{i_k}$$

[G-K] p. 401

Exemple 8. Pour $n = 3$, on a

$$|A_1 \cap A_2 \cap A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_2 \cap A_3| - -|A_1 \cap A_3| + |A_1 \cup A_2 \cup A_3|$$

Lemme 9 (des bergers)**.** Soient A et B deux ensembles. On suppose A fini. Soit $\varphi : A \to B$ surjective telle que tout élément de B admet exactement a antécédents par φ. Alors,

$$|A| = \frac{|B|}{a}$$

2. Combinatoire

a. Listes

Proposition 10. Soient n ensembles finis $E_1, \dots, E_n$. Le produit cartésien $E_1 \times \cdots \times E_n$ est un ensemble fini et vérifie $|E_1 \times \cdots \times E_n| = |E_1| \times \cdots \times |E_n|$. En particulier, pour un ensemble E fini, on a $|E^n| = |E|^n$.

[GOU21] p. 301

Définition 11. Soit E un ensemble et $p \in \mathbb{N}^*$. On appelle p-**liste** (ou p-**uplet**) de E, tout élément $(x_1, \dots, x_p)$ de E^p.

Remarque 12.
— Si E est fini, il y a $|E|^p$ p-listes de E.
— Dans une liste, l'ordre des éléments importe.

Exemple 13. Dans un jeu de 52 cartes, le nombre de façons de tirer 10 cartes avec remise est 52^{10}.

b. Arrangements

Définition 14. Soit E un ensemble fini de cardinal n. Soit p un entier inférieur à n. On appelle p-**arrangement** de E toute p-liste de E d'éléments distincts.

Proposition 15. En reprenant les notations précédentes, le nombre de p-arrangements de E est

$$A_n^p = n(n-1)\dots(n-p+1) = \frac{n!}{(n-p)!}$$

Remarque 16. — Si $p = n$, on trouve que le nombre de n-arrangements est $n!$.
— Dans les arrangements, l'ordre des éléments importe, mais ceux-ci sont distincts.

Exemple 17. Dans un jeu de 52 cartes, le nombre de façons de tirer 10 cartes sans remise est $A_{52}^{10} = 52 \times \cdots \times 43$.

Application 18 (Nombre d'applications entre deux ensembles finis)**.** Soient E et F deux ensembles finis.

(i) L'ensemble des applications de E vers F, noté F^E est fini, de cardinal $|F|^{|E|}$.

(ii) Lorsque $|E| \leq |F|$, l'ensemble des applications injectives de E dans F est fini, de cardinal A_n^p.

(iii) L'ensemble des bijections de E vers E appelées permutations de E, noté $\mathscr{S}(E)$, est fini et de cardinal $|E|!$.

Corollaire 19. Soit E un ensemble fini. Le nombre total de parties de E est $|\mathscr{P}(E)| = 2^{|E|}$.

c. Combinaisons

Définition 20. Soit E un ensemble fini de cardinal n. Soit $p \in \mathbb{N}$. On appelle **p-combinaison** de E toute partie de E de cardinal p. Ce nombre ne dépend que de n et de p, on le note $\binom{n}{p}$.

Proposition 21. Soient $n, p \in \mathbb{N}$. Alors,

$$\binom{n}{p} = \begin{cases} \frac{n!}{p!(n-p)!} & \text{si } p \leq n \\ 0 & \text{sinon} \end{cases}$$

Remarque 22. Dans les combinaisons, l'ordre des éléments n'importe pas, mais ceux-ci sont distincts.

Exemple 23. Dans un jeu de 52 cartes, le nombre de façons de tirer 10 cartes simultanément est $\binom{52}{10}$.

Définition 24. Soit E un ensemble fini de cardinal n. Soit p un entier inférieur à n. On appelle **p-combinaison avec répétition** les p-listes dans lesquelles ont autorise les répétions, mais dans lesquelles l'ordre ne compte pas.

Proposition 25. En reprenant les notations précédentes, il y a $\binom{n+p-1}{p}$ p-combinaisons avec répétition.

Proposition 26. Soit $n \in \mathbb{N}$.

(i) On a :

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

(ii) Soient a et b deux éléments d'une algèbre qui commutent. Alors,

$$(a+b)^n \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Application 27. Soit (F_n) la suite de Fibonacci définie par $F_0 = 0$, $F_1 = 1$ et $\forall n \geq 2$, $F_n = F_{n-1} + F_{n-2}$. Alors, p. 311

$$\forall n \in \mathbb{N}, F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right) = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n-k}{k}$$

II - En théorie des groupes

Soit G un groupe fini.

1. Actions de groupes

Soit X un ensemble fini. On considère une action $\cdot$ de G sur X. **[ULM21]** p. 71

Proposition 28. Soit $x \in X$. Alors :

- $|G \cdot x| = (G : \mathrm{Stab}_G(x))$.
- $|G| = |\mathrm{Stab}_G(x)||G \cdot x|$.
- $|G \cdot x| = \frac{|G|}{|\mathrm{Stab}_G(x)|}$

Théorème 29 (Formule des classes)**.** Soit Ω un système de représentants d'orbites de l'action de G sur X. Alors,

$$|X| = \sum_{\omega \in \Omega} |G \cdot \omega| = \sum_{\omega \in \Omega} (G : \mathrm{Stab}_G(\omega)) = \sum_{\omega \in \Omega} \frac{|G|}{|\mathrm{Stab}_G(\omega)|}$$

Définition 30. On définit :

— $X^G = \{x \in X \mid \forall g \in G,\ g \cdot x = x\}$ l'ensemble des points de X laissés fixes par tous les éléments de G.

— $X^g = \{x \in X \mid g \cdot x = x\}$ l'ensemble des points de X laissés fixes par $g \in G$.

Théorème 31 (Formule de Burnside)**.** Le nombre r d'orbites de X sous l'action de G est donné par

$$r = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

Application 32. Deux colorations des faces d'un cube sont les mêmes si on peut passer de l'une à l'autre par une isométrie du dodécaèdre. Alors, le nombre de colorations distinctes d'un cube avec c couleurs est

$$\frac{c^2}{24}(c^4 + 3^2 + 12c + 8)$$

[I-P] p. 121

2. p-groupes

Définition 33. On dit que G est un **p-groupe** s'il est d'ordre une puissance d'un nombre premier p.

[ROM21] p. 22

Proposition 34. Soit p un nombre premier. Si G est un p-groupe opérant sur un ensemble X, alors,

$$|X^G| \equiv |X| \mod p$$

où X^G désigne l'ensemble des points fixes de X sous l'action de G.

Corollaire 35. On note $G \cdot h_1, \dots, G \cdot h_r$ les classes de conjugaison de G. Alors,

$$\begin{aligned} |G| &= |Z(G)| + \sum_{\substack{i=1 \\ |G \cdot h_i| = 2}}^{r} |G \cdot h_i| \\ &= |Z(G)| + \sum_{\substack{i=1 \\ |G \cdot h_i| = 2}}^{r} \frac{|G|}{|\mathrm{Stab}_G(h_i)|} \end{aligned}$$

Corollaire 36. Soit p un nombre premier. Le centre d'un p-groupe non trivial est non trivial.

Corollaire 37. Soit p un nombre premier. Un groupe d'ordre p^2 est toujours abélien.

Application 38 (Théorème de Cauchy)**.** On suppose G non trivial et fini. Soit p un premier divisant l'ordre de G. Alors il existe un élément d'ordre p dans G.

[DEV]

Application 39 (Premier théorème de Sylow)**.** On suppose G fini d'ordre np^α avec $n, \alpha \in \mathbb{N}$ et p premier tel que $p \nmid n$. Alors, il existe un sous-groupe de G d'ordre p^α.

[GOU21] p. 44

III - En théorie des corps finis

Soit $q = p^n$ avec p premier et $n \geq 2$.

1. Polynômes irréductibles

Théorème 40.

$$\mathbb{F}_q = \mathbb{F}_p[X]/(P)$$

où $P \in \mathbb{F}_p[X]$ est un polynôme irréductible de degré n sur $\mathbb{F}_p$.

[GOZ] p. 87

Corollaire 41. (i) Il existe des polynômes irréductibles de tout degré dans $\mathbb{F}_p[X]$.

(ii) Si $P \in \mathbb{F}_p[X]$ est un polynôme irréductible sur $\mathbb{F}_p$ de degré n, alors P divise $X^q - X$. En particulier, il est scindé sur $\mathbb{F}_q$. Donc son corps de rupture $\mathbb{F}_q = \mathbb{F}_p[X]/(P)$ est aussi son corps de décomposition.

Théorème 42. Pour tout $j \in \mathbb{N}^*$, on note $I(p,q)$ l'ensemble des polynômes irréductibles unitaires de degré j sur $\mathbb{F}_p$. Alors,

$$X^q - X = \prod_{d|n} \prod_{Q \in I(p,q)} Q$$

Corollaire 43.

$$q = \sum_{d|n} d|I(p,d)|$$

Définition 44. On définit la **fonction de Möbius**, notée μ, par

$$\mu : \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z} \\ n & \mapsto & \begin{cases} 1 & \text{si } n = 1 \\ (-1)^k & \text{si } n = p_1 \dots p_k \text{ avec } p_1, \dots, p_k \text{ premiers distincts} \\ 0 & \text{sinon} \end{cases} \end{array}$$

Théorème 45 (Formule d'inversion de Möbius)**.** Soient f et g des fonctions de $\mathbb{N}^*$ dans $\mathbb{C}$ telles que $\forall n \in \mathbb{N}^*, f(n) = \sum_{d|n} g(d)$. Alors,

$$\forall n \in \mathbb{N}^*, g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$$

Corollaire 46.

$$\forall n \in \mathbb{N}^*, |I(p,q)| = \frac{1}{n}\sum_{d|n} \mu(d) p^{\frac{n}{d}} = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) p^d$$

2. Carrés dans les corps finis

Proposition 47. On note $\mathbb{F}_q^2 = \{x^2 \mid x \in \mathbb{F}_q\}$ et $\mathbb{F}_q^{*2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$. Alors $\mathbb{F}_q^{*2}$ est un sous-groupe de $\mathbb{F}_q^*$. p. 93

Proposition 48. (i) Si $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$, donc $\mathbb{F}_q^{*2} = \mathbb{F}_q^*$.

(ii) Si $p > 2$, alors :

- $\mathbb{F}_q^{*2}$ est le noyau de l'endomorphisme de $\mathbb{F}_q^*$ défini par $x \mapsto x^{\frac{q-1}{2}}$.
- $\mathbb{F}_q^{*2}$ est un sous-groupe d'indice 2 de $\mathbb{F}_q^*$.
- $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$ et $|\mathbb{F}_q^2| = \frac{q+1}{2}$.
- $(-1) \in \mathbb{F}_q^{*2} \iff q \equiv 1 \mod 4$.

3. Groupe linéaire sur un corps fini

Soit V un espace vectoriel de dimension finie n sur un corps $\mathbb{K}$.

[PER] p. 119

Définition 49.

- Le **groupe linéaire** de V, $\mathrm{GL}(V)$ est le groupe des applications linéaires de V dans lui-même qui sont inversibles.
- Le **groupe spécial linéaire** de V, $\mathrm{SL}(V)$ est le sous-groupe de $\mathrm{GL}(V)$ constitué des applications de déterminant 1.
- Les quotients de ces groupes par leur centre sont respectivement notés $\mathrm{PGL}(V)$ et $\mathrm{PSL}(V)$.

Proposition 50. On se place dans le cas où $\mathbb{K} = \mathbb{F}_q$. Alors, les groupes précédents sont finis, et : p. 124

(i) $|\mathrm{GL}(V)| = q^{\frac{n(n-1)}{2}}((q^n-1)\dots(q-1))$.

(ii) $|\mathrm{PGL}(V)| = |\mathrm{SL}(V)| = \frac{|\mathrm{GL}(V)|}{q-1}$.

(iii) $|\mathrm{PSL}(V)| = |\mathrm{SL}(V)| = \frac{|\mathrm{GL}(V)|}{(q-1)\mathrm{pgcd}(n,q-1)}$.

IV - En analyse

1. Probabilités sur un ensemble fini

Soit $(\Omega, \mathscr{A}, \mathbb{P})$ un espace probabilisé.

[G-K] p. 137

Définition 51. Soit $E \subseteq \Omega$ fini. On appelle loi uniforme sur E la loi discrète définie sur $\mathscr{P}(\Omega)$ par

$$\begin{array}{ccc} \mathscr{P}(\Omega) & \to & [\![0,1]\!] \\ A & \mapsto & \frac{|A\cap E|}{|E|} \end{array}$$

Remarque 52. Il s'agit du nombre de cas favorables sur le nombre de cas possibles. Ainsi, X suit la loi uniforme sur E si on a $\forall x \in E, \mathbb{P}(X=x) = \frac{1}{|E|}$ et $\forall x \notin E, \mathbb{P}(X=x) = 0$.

C'est, par exemple, la loi suivie par une variable aléatoire représentant le lancer d'un dé non truqué avec $E = [\![1,6]\!]$.

Définition 53. Une variable aléatoire X suit une **loi de Bernoulli** de paramètre $p \in [0,1]$, notée $\mathscr{B}(p)$, si $\mathbb{P}(X=1) = p$ et $\mathbb{P}(X=0) = 1-p$.

Proposition 54. En reprenant les notations précédentes, X est une loi discrète et on a

$$\mathbb{P}_X = (1-p)\delta_0 + p\delta_1$$

Définition 55. Une variable aléatoire X suit une **loi de binomiale** de paramètres $n \in \mathbb{N}$ et $p \in [0,1]$, notée $\mathscr{B}(n,p)$, si X est la somme de n variables aléatoires indépendantes qui suivent des lois de Bernoulli de paramètre p.

Proposition 56. En reprenant les notations précédentes, X est une loi discrète et on a

$$\forall k \in \mathbb{N}, \mathbb{P}(X=k) = \binom{n}{k} p^k (1-p)^{n-k}$$

Remarque 57. Il s'agit du nombre de succès pour n tentatives.

C'est, par exemple, la loi suivie par une variable aléatoire représentant le nombre de "Pile" obtenus lors d'un lancer de pièce équilibrée.

2. Utilisation des séries pour dénombrer

Théorème 58 (Dérangements)**.** Soit $n \in \mathbb{N}^*$. On note $\mathscr{D}_n$ l'ensemble des permutations de $[\![1, n]\!]$ sans point fixe. Alors,

$$|\mathscr{D}_n| = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} = \left\lfloor \frac{n!}{e} + \frac{1}{2} \right\rfloor$$

[GOU21] p. 312

Exemple 59. n personnes laissent leur chapeau à un vestiaire. En repartant, chaque personne prend un chapeau au hasard. La probabilité que personne ne reprenne son propre chapeau est d'environ $\frac{1}{e}$.

[DEV]

Théorème 60 (Nombres de Bell)**.** Pour tout $n \in \mathbb{N}^*$, on note B_n le nombre de partitions de $[\![1, n]\!]$. Par convention on pose $B_0 = 1$. Alors,

$$\forall k \in \mathbb{N}^*, B_k = \frac{1}{e} \sum_{n=0}^{+\infty} \frac{n^k}{n!}$$

p. 314

191 Exemples d'utilisation de techniques d'algèbre en géométrie.

I - Utilisation des nombres complexes

On se place dans un plan affine euclidien $\mathscr{P}$ muni d'un repère orthonormé $\mathscr{R} = (O, \vec{i}, \vec{j})$.

1. Module, argument

[ROM21] p. 97

Théorème 1. L'application

$$\begin{array}{ccc} \mathscr{R} & \to & \mathbb{C} \\ (x,y) & \mapsto & x+iy \end{array}$$

est une bijection.

En utilisant cette identification entre $\mathscr{P}$ et $\mathbb{C}$, on peut identifier tout point du plan à un nombre complexe.

Théorème 2. Soient A et B deux points dont on note a et b les complexes associés.

(i) $|a| = OA$.

(ii) $|b-a| = AB$.

(iii) Soit $r \in \mathbb{R}_*^+$. L'ensemble des nombres complexes z tels que $|z-a| = r$ (resp. $|z-a| < r$ / $|z-a| \leq r$) est le cercle (resp. le disque ouvert / fermé) de centre A et de rayon r.

(iv) Un point M d'affixe z est sur la médiatrice de $[AB]$ si et seulement si $|z-a| = |z-b|$.

Proposition 3 (Inégalité triangulaire)**.** Soient $z_1, \dots, z_n \in \mathbb{C}^*$ avec $n \geq 2$, on a

$$\left| \sum_{k=1}^{n} z_k \right| \leq \sum_{k=1}^{n} |z_k|$$

l'égalité étant réalisée si et seulement si $z_1, \dots, z_n$ sont linéairement liés.

Remarque 4. En reprenant les notations précédentes, et en désignant par $M_1, \dots, M_n$ les points associés aux complexes $z_1, \dots, z_n$, l'égalité

$$\left\| \sum_{k=1}^{n} \overrightarrow{OM_k} \right\| = \sum_{k=1}^{n} \left\| \overrightarrow{OM_k} \right\|$$

est équivalente à dire que les points $O, M_1, \dots, M_n$ sont alignés.

Théorème 5. Si z est un nombre complexe de module 1, il existe un unique réel $\theta \in [-\pi, \pi[$ tel que

$$z = \cos(\theta) + i\sin(\theta)$$

Définition 6. On dit qu'un réel θ est un **argument** du nombre complexe z non nul si

$$\frac{z}{|z|} = \cos(\theta) + i\sin(\theta)$$

Théorème 7. Soient $\overrightarrow{v_1}$ et $\overrightarrow{v_2}$ deux vecteurs non nuls du plan. On note z_1 et z_2 les complexes associés.

(i) Si θ_1 est un argument de z_1, alors c'est également une mesure de l'angle orienté $\widehat{(\vec{i}, \overrightarrow{v_1})}$.

(ii) Un argument de $\frac{z_2}{z_1}$ est une mesure de l'angle orienté $\theta = \widehat{(\overrightarrow{v_1}, \overrightarrow{v_2})}$ et on a :

$$\cos(\theta) = \frac{\langle \overrightarrow{v_1}, \overrightarrow{v_2} \rangle}{\|\overrightarrow{v_1}\| \|\overrightarrow{v_2}\|} \text{ et } \sin(\theta) = \frac{\det(\overrightarrow{v_1}, \overrightarrow{v_2})}{\|\overrightarrow{v_1}\| \|\overrightarrow{v_2}\|}$$

où $\langle ., . \rangle$ désigne le produit scalaire canonique.

2. Le triangle dans le plan complexe

Définition 8. Un **vrai triangle** dans le plan $\mathscr{P}$ est la donnée de trois points non alignés A, B et C. Un tel triangle est noté $\mathscr{T} = ABC$. p. 105

Soit $\mathscr{T} = ABC$ un vrai triangle. On note a, b et c les complexes associés respectivement à A, B et C.

Théorème 9. L'aire de ABC est

$$\frac{1}{2}\left|\det\left(\overrightarrow{AB}, \overrightarrow{AC}\right)\right|$$

Proposition 10. Le trois médianes de $\mathscr{T}$ concourent au point dont le complexe associé est

$$\frac{a+b+c}{3}$$

Définition 11. Le point précédent est appelé **centre de gravité** de $\mathscr{T}$. C'est aussi l'**isobarycentre** des points A, B et C.

Proposition 12. Le trois hauteurs de $\mathscr{T}$ concourent au point dont le complexe associé est

$$a_\Omega + b_\Omega + c_\Omega$$

où a_Ω, b_Ω, c_Ω sont les complexes associés aux points A, B et C considérés dans le repère $(\Omega, \vec{i}, \vec{j})$ avec Ω centre du cercle circonscrit au triangle $\mathscr{T}$.

Définition 13. Le point précédent est appelé **orthocentre** de $\mathscr{T}$.

Proposition 14. Dans un vrai triangle, orthocentre, centre du cercle circonscrit et centre de gravité sont alignés.

3. Droites et cercles dans le plan complexe

Théorème 15. Toute équation de la forme

$$\alpha z\overline{z} + \overline{\beta}z + \beta\overline{z} + \gamma = 0,\ \alpha, \gamma \in \mathbb{R},\ \beta \in \mathbb{C}$$

représente dans $\mathscr{P}$:

(i) $\mathscr{P}$ tout entier si $\alpha = \beta = \gamma = 0$.

(ii) $\varnothing$ si :

— $\alpha = \beta = 0$ et $\gamma \neq 0$;

— ou $\alpha \neq 0$ et $|\beta|^2 - \alpha\gamma < 0$.

(iii) Une droite dirigée par le vecteur $\vec{v}$ représentant le complexe $i\beta$ si $\alpha = 0$ et $\beta \neq 0$.

(iv) Le cercle dont le centre est associé au complexe $-\frac{\beta}{\alpha}$ et de rayon $\frac{\sqrt{|\beta|^2 - \alpha\gamma}}{|\alpha|}$ si $\alpha \neq 0$ et $|\beta|^2 - \alpha\gamma \geq 0$.

Corollaire 16 (Théorème d'Appolonius)**.** Soient a et b deux nombres complexes distincts et $\lambda \in \mathbb{R}^+$. L'ensemble

$$E_\lambda = \{z \in \mathbb{C} \mid |z - b| = \lambda |z - a|\}$$

est identifié dans $\mathscr{P}$;

— À la médiatrice du segment $[AB]$ pour $\lambda = 1$.

— Au cercle de centre le complexe associé à $\frac{b - \lambda^2 a}{1 - \lambda^2}$ et de rayon $\frac{\lambda |a - b|}{|1 - \lambda^2|}$ pour $\lambda \neq 1$.

Théorème 17. Soient A, B, C et D des points deux à deux distincts associés respectivement aux complexes a, b, c et d. Ces points sont alignés si et seulement si

$$\frac{c - b}{c - a}\frac{d - a}{d - b} \in \mathbb{R}^+$$

Corollaire 18 (Théorème de Ptolémée)**.** Soient A, B, C et D des points deux à deux distincts. Le quadrilatère convexe $ABCD$ est inscriptible dans un cercle si et seulement si

$$AC \times BD = AB \times CD + AD \times BC$$

II - Utilisation de la théorie des groupes

1. Actions de groupe

a. Cadre général

Soit X un ensemble fini. On considère une action $\cdot$ de G sur X.

[ULM21] p. 71

Proposition 19. Soit $x \in X$. Alors :

— $|G \cdot x| = (G : \mathrm{Stab}_G(x))$.

— $|G| = |\mathrm{Stab}_G(x)||G \cdot x|$.

— $|G \cdot x| = \frac{|G|}{|\mathrm{Stab}_G(x)|}$

Théorème 20 (Formule des classes)**.** Soit Ω un système de représentants des orbites de l'action de G sur X. Alors,

$$|X| = \sum_{\omega \in \Omega} |G \cdot \omega| = \sum_{\omega \in \Omega} (G : \mathrm{Stab}_G(\omega)) = \sum_{\omega \in \Omega} \frac{|G|}{|\mathrm{Stab}_G(\omega)|}$$

Définition 21. On définit :

— $X^G = \{x \in X \mid \forall g \in G,\ g \cdot x = x\}$ l'ensemble des points de X laissés fixes par tous les éléments de G.

— $X^g = \{x \in X \mid g \cdot x = x\}$ l'ensemble des points de X laissés fixes par $g \in G$.

Théorème 22 (Formule de Burnside)**.** Le nombre r d'orbites de X sous l'action de G est donné par

$$r = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

Application 23. Deux colorations des faces d'un cube sont les mêmes si on peut passer de l'une à l'autre par une isométrie du dodécaèdre. Alors, le nombre de colorations distinctes d'un cube avec c couleurs est

$$\frac{c^2}{24}(c^4 + 3^2 + 12c + 8)$$

[I-P] p. 121

b. Espaces affines

On peut réécrire le définition d'un espace affine en termes d'actions de groupes.

[ROM21] p. 73

Définition 24. Soit E un espace vectoriel sur $\mathbb{R}$. Un **espace affine** $\mathscr{E}$ est un ensemble non vide qui agit (à droite) sur E de manière simplement transitive. On note $\cdot$ l'action correspondante. Les éléments de $\mathscr{E}$ sont appelés **points** et les éléments de E sont appelés **vecteurs**.

Remarque 25. Ainsi, pour tout couple $(x,y) \in \mathscr{E}$, il existe un unique $u \in E$ tel que $y = x \cdot u$. On note alors $u = \overrightarrow{xy}$.

Le reste de la théorie découle de cette remarque.

2. Groupe diédral

[ULM21] p. 8

Définition 26. Pour un entier $n \geq 1$, le **groupe diédral** D_n est le sous-groupe, de $\mathrm{GL}_2(\mathbb{R})$ engendré par la symétrie axiale s et la rotation d'angle $\theta = \frac{2\pi}{n}$ définies respectivement par les matrices

$$S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ et } R = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

Exemple 27. $D_1 = \{\mathrm{id}, s\}$.

Proposition 28. (i) D_n est un groupe d'ordre $2n$.
(ii) $r^n = s^2 = \mathrm{id}$ et $sr = r^{-1}s$.

Proposition 29. Un groupe non cyclique d'ordre 4 est isomorphe à D_2. p. 28

Exemple 30. S_2 est isomorphe à D_2. p. 65

Proposition 31. Un groupe fini d'ordre $2p$ avec p premier est soit cyclique, soit isomorphe à D_p. p. 28

Exemple 32. S_3 est isomorphe à D_3.

Proposition 33. Les sous-groupes de D_n sont soit cyclique, soit isomorphes à un D_m où $m \mid n$. p. 47

[ROM21] p. 84

Théorème 34. On désigne par Γ_n l'ensemble des sommets d'un polygone à n côtés et par $\mathrm{Is}(\Gamma_n)$ l'ensemble des isométries qui conservent Γ_n. Alors,

$$\mathrm{Is}(\Gamma_n) = D_n$$

Exemple 35. Les isométries conservant un triangle équilatéral sont les éléments de D_3.

III - Utilisation de la théorie des corps

On note $\mathscr{P}$ un plan affine euclidien muni d'un repère orthonormé direct $\mathscr{R} = (O, \vec{i}, \vec{j})$. On s'autorise à identifier chaque point $M \in \mathscr{P}$ avec ses coordonnées $(x, y) \in \mathbb{R}^2$ dans $\mathscr{R}$. [GOZ] p. 47

Définition 36. On dit qu'un point $M \in \mathscr{P}$ est **constructible** (sous-entendu *à la règle et au compas*) si on peut le construire en utilisant uniquement la règle et le compas, en supposant O et $I = (1,0)$ déjà construits.

Proposition 37. Soient A, B deux points constructibles distincts.

(i) Si A est constructible, son symétrique par rapport à O l'est aussi.

(ii) $J = (0,1)$ est constructible.

(iii) Si C est un point constructible, on peut construire à la règle et au compas la perpendiculaire à (AB) passant par C.

(iv) Si C est un point constructible, on peut construire à la règle et au compas la parallèle à (AB) passant par C.

Proposition 38. Soit $x \in \mathbb{R}$.

$$(x,0) \text{ est constructible} \iff (0,x) \text{ est constructible}$$

Définition 39. Un nombre vérifiant la proposition précédente est dit **nombre constructible**.

Proposition 40. (i) Tout élément de $\mathbb{Q}$ est constructible.

(ii) (x,y) est constructible si et seulement si x et y le sont.

Théorème 41. L'ensemble $\mathbb{E}$ des nombres constructibles est un sous-corps de $\mathbb{R}$ stable par racine carrée.

[DEV]

Théorème 42 (Wantzel)**.** Soit $t \in \mathbb{R}$. t est constructible si et seulement s'il existe une suite fini $(L_0, \dots, L_p)$ de sous-corps de $\mathbb{R}$ vérifiant :

(i) $L_0 = \mathbb{Q}$.

(ii) $\forall i \in [\![1, p-1]\!]$, L_i est une extension quadratique de L_{i-1}.

(iii) $t \in L_p$.

Corollaire 43. (i) Si x est constructible, le degré de l'extension $\mathbb{Q}[x]$ sur $\mathbb{Q}$ est de la forme 2^s pour $s \in \mathbb{N}$.

(ii) Tout nombre constructible est algébrique.

Contre-exemple 44. — $\sqrt[3]{2}$ est algébrique, non constructible.

— $\sqrt{\pi}$ est transcendant et n'est donc pas constructible.

Application 45 (Quadrature du cercle)**.** Il est impossible de construire, à la règle et au compas, un carré ayant même aire qu'un disque donné.

Application 46 (Duplication du cube)**.** Il est impossible de construire, à la règle et au compas, l'arête d'un cube ayant un volume double de celui d'un cube donné.

IV - Utilisation de l'algèbre linéaire

1. Déterminant et volume

Théorème 47. L'aire $\mathcal{A}(v, w)$ du parallélogramme engendré par deux vecteurs $v, w \in \mathbb{R}^n$ est égale à

$$\mathcal{A}(v, w) = |\det(v, w)|$$

[GRI] p. 130

Corollaire 48. Soient $v_1, \dots, v_n \in \mathbb{R}^n$. On note $\mathcal{V}(v_1, \dots, v_n)$ le volume du parallélépipède rectangle engendré par $v_1, \dots, v_n$ (ie. l'ensemble $\{z \in \mathbb{R}^n \mid z = \sum_{i=1}^n \lambda_i v_i, \lambda_i \in [0,1]\}$). On a alors :

$$\mathcal{V}(v_1, \dots, v_n) = |\det(v_1, \dots, v_n)|$$

2. Étude d'une suite de polygones

Proposition 49 (Déterminant circulant)**.** Soient $n \in \mathbb{N}^*$ et $a_1, \dots, a_n \in \mathbb{C}$. On pose $\omega = e^{\frac{2i\pi}{n}}$. Alors

$$\begin{vmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \dots & a_0 \end{vmatrix} = \prod_{j=0}^{n-1} P(\omega^j)$$

où $P = \sum_{k=0}^{n-1} a_k X^k$.

[GOU21] p. 153

[DEV]

Application 50 (Suite de polygones)**.** Soit P_0 un polygone dont les sommets sont $\{z_{0,1}, \dots, z_{0,n}\}$. On définit la suite de polygones (P_k) par récurrence en disant que, pour tout $k \in \mathbb{N}^*$, les sommets de P_{k+1} sont les milieux des arêtes de P_k.

Alors la suite (P_k) converge vers l'isobarycentre de P_0.

[I-P] p. 389

3. Groupe spécial orthogonal en dimension 2 et 3

Définition 51. On définit $\mathrm{SO}(E) = \{u \in \mathcal{O}(E) \mid \det(u) = 1\}$ et $\mathrm{SO}_n(\mathbb{R}) = \{A \in \mathcal{O}_n(\mathbb{R}) \mid \det(A) = 1\}$

[GRI] p. 241

Proposition 52. $\mathrm{SO}(E)$ est un sous-groupe distingué de $\mathcal{O}(E)$ d'indice 2 (de même que $\mathrm{SO}_n(\mathbb{R})$ dans $\mathcal{O}_n(\mathbb{R})$).

[ROM21] p. 724

Exemple 53.

$$\frac{1}{3}\begin{pmatrix} 2 & -1 & 2 \\ 2 & 2 & -1 \\ -1 & 2 & 2 \end{pmatrix} \in \mathrm{SO}_3(\mathbb{R})$$

[GRI] p. 241

Théorème 54. Soit $A \in \mathcal{O}_2(\mathbb{R})$. Alors :

— Si $A \in \mathrm{SO}_2(\mathbb{R})$:

$$\exists \theta \in \mathbb{R} \text{ tel que } A = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

(rotation d'angle θ).

— Si $A \notin \mathrm{SO}_2(\mathbb{R})$:

$$\exists \theta \in \mathbb{R} \text{ tel que } A = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix}$$

(symétrie orthogonale par rapport à la droite d'angle polaire $\frac{\theta}{2}$).

Théorème 55. Soit $A \in \mathcal{O}_3(\mathbb{R})$ et u l'endomorphisme de E dont la matrice dans la base canonique est A. Alors, il existe $\mathcal{B}$ une base orthonormée de E telle que la matrice de u dans $\mathcal{B}$ est

$$\begin{pmatrix} \cos(\theta) & -\sin(\theta) & 0 \\ \sin(\theta) & \cos(\theta) & 0 \\ 0 & 0 & \epsilon \end{pmatrix}$$

avec $\epsilon = \pm 1$. On note E_ϵ le sous-espace vectoriel associé à la valeur propre ϵ.

- Si $\epsilon = 1$: $f \in \mathrm{SO}(E)$ est la rotation d'angle $2\cos(\theta)+1$ autour de l'axe E_1.
- Si $\epsilon = -1$: $f \notin \mathrm{SO}(E)$ est la composée de la rotation d'angle $2\cos(\theta)-1$ autour de l'axe E_{-1} avec la symétrie orthogonale par rapport à $E_{-1}^{\perp}$.

Théorème 56. Soit G un sous-groupe fini de $\mathrm{SO}_3(\mathbb{R})$. Alors, G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, D_n, A_4, S_4 ou A_5 (où $n \geq 2$). **[ULM21]** p. 138

Application 57 (Solides de Platon)**.** Il y a cinq polyèdres réguliers : le tétraèdre, le cube, l'octaèdre, le dodécaèdre et l'icosaèdre.

Annexes

[I-P]
p. 389

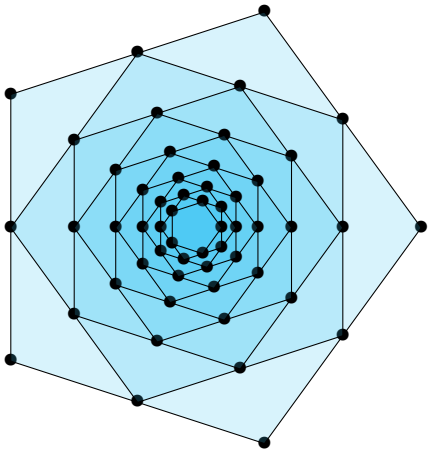
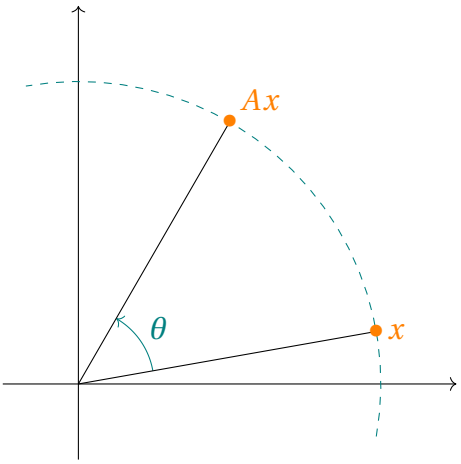
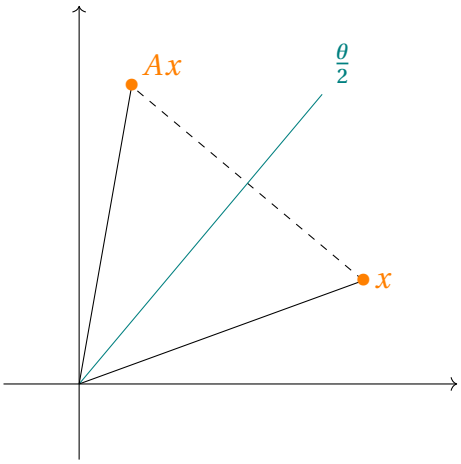


FIGURE I.16 – La suite de polygones.

[GRI]
p. 242



$A \in \mathrm{SO}_2(\mathbb{R})$



$A \notin \mathrm{SO}_2(\mathbb{R})$

FIGURE I.17 – Le groupe $\mathcal{O}_2(\mathbb{R})$.

p. 244

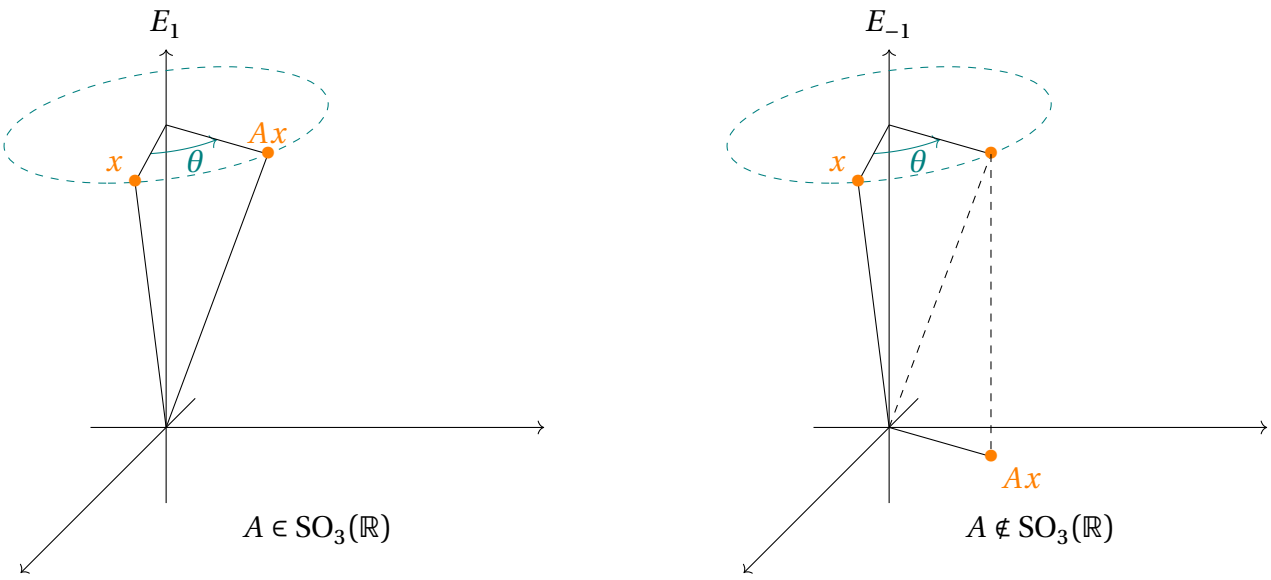


FIGURE I.18 – Le groupe $\mathcal{O}_3(\mathbb{R})$.

201 Espaces de fonctions. Exemples et applications.

I - Espaces de fonctions continues sur un compact

1. Continuité et compacité

Proposition 1. Soient (E,d) et (E',d') deux espaces métriques. On suppose E compact. Si $f : E \to E'$ est continue, alors $f(E)$ est compact. [DAN] p. 55

Contre-exemple 2. Cela ne marche pas si f n'est pas continue. Par exemple, $\arcsin([-1,1]) = \mathbb{R}$.

Proposition 3. Sous les mêmes hypothèses et en supposant f bijective, f^{-1} est continue (ie. f est un homéomorphisme).

Théorème 4 (Des bornes)**.** Une application continue sur un compact est bornée et atteint ses bornes.

Théorème 5 (Heine)**.** Une application continue sur un compact y est uniformément continue.

Corollaire 6. Toute fonction périodique continue sur $\mathbb{R}$ y est uniformément continue.

2. Convergences simple et uniforme

Définition 7. Soient (f_n) et f respectivement une suite de fonctions et une fonction définies sur un ensemble X à valeurs dans un espace métrique (E,d). On dit que : [GOU20] p. 231

— (f_n) **converge simplement** vers f si

$$\forall x \in X,\ \forall \epsilon > 0,\ \exists N \in \mathbb{N} \text{ tel que } \forall n \geq N,\ d(f_n(x), f(x)) < \epsilon$$

— (f_n) **converge uniformément** vers f si

$$\forall \epsilon > 0,\ \exists N \in \mathbb{N} \text{ tel que } \forall n \geq N,\ \forall x \in X,\ d(f_n(x), f(x)) < \epsilon$$

Proposition 8. La convergence uniforme entraîne la convergence simple.

Contre-exemple 9. La réciproque est fausse. Il suffit en effet de considérer la suite (f_n) définie pour tout $n \in \mathbb{N}$ et pour tout $x \in [0,1]$ par $f_n(x) = x^n$ converge simplement sur $[0,1]$ mais pas uniformément.

Théorème 10 (Critère de Cauchy uniforme)**.** Soit (f_n) une suite de fonctions définies sur un ensemble X à valeurs dans un espace métrique (E,d). Alors (f_n) converge uniformément si

$$\forall \epsilon > 0, \exists N \in \mathbb{N} \text{ tel que } \forall p > q \geq N, \forall x \in X,\ d(f_p(x), f_q(x)) < \epsilon$$

Corollaire 11. Une limite uniforme sur $\mathbb{R}$ de fonctions polynômiales est une fonction polynômiale. p. 237

Notation 12. — Pour toute fonction g bornée sur un ensemble X et à valeurs dans un espace vectoriel normé $(E, \|.\|)$, on note p. 232

$$\|g\|_\infty = \sup_{x \in X} \|g(x)\|$$

— On note $\mathscr{B}(X,E)$ l'ensemble des applications bornées de X dans E.

Proposition 13. En reprenant les notations précédentes, une suite de fonctions (f_n) de $\mathscr{B}(X,E)$ converge uniformément vers $f \in \mathscr{B}(X,E)$ si $\|f_n - f\|_\infty \longrightarrow_{n \to +\infty} 0$.

Proposition 14. Si E est de Banach, alors $(\mathscr{B}(X,E), \|.\|_\infty)$ est de Banach.

Théorème 15 (Théorèmes de Dini)**.** (i) Soit (f_n) une suite *croissante* de fonctions réelles *continues* définies sur un segment I de $\mathbb{R}$. Si (f_n) converge simplement vers une fonction *continue* sur I, alors la convergence est uniforme. p. 238

(ii) Soit (f_n) une suite de *fonctions croissantes* réelles *continues* définies sur un segment I de $\mathbb{R}$. Si (f_n) converge simplement vers une fonction *continue* sur I, alors la convergence est uniforme.

3. Densité

[DEV]

Théorème 16 (Weierstrass)**.** Toute fonction continue $f : [a,b] \to \mathbb{R}$ (avec $a, b \in \mathbb{R}$ tels que $a \leq b$) est limite uniforme de fonctions polynômiales sur $[a,b]$.

p. 304

On a une version plus générale de ce théorème.

Théorème 17 (Stone-Weierstrass)**.** Soit K un espace compact et $\mathscr{A}$ une sous-algèbre de l'algèbre de Banach réelle $\mathscr{C}(K,\mathbb{R})$. On suppose de plus que :

(i) $\mathscr{A}$ sépare les points de K (ie. $\forall x \in K, \exists f \in A$ telle que $f(x) \neq f(y)$).

(ii) $\mathscr{A}$ contient les constantes.

Alors $\mathscr{A}$ est dense dans $\mathscr{C}(K,\mathbb{R})$.

[LI] p. 46

Remarque 18. Il existe aussi une version "complexe" de ce théorème, où il faut supposer de plus que $\mathscr{A}$ est stable par conjugaison.

Exemple 19. La suite de polynômes réels (r_n) définie par récurrence par

$$r_0 = 0 \text{ et } \forall n \in \mathbb{N}, r_{n+1} : t \mapsto r_n(t) + \frac{1}{2}(t - r_n(t)^2)$$

converge vers $\sqrt{.}$ sur $[0,1]$.

II - Espaces L_p

Soit $(X, \mathscr{A}, \mu)$ un espace mesuré. Les résultats qui vont suivre sont, par extension, également valable pour les fonctions à valeurs dans $\mathbb{C}$.

[G-K] p. 209

1. Espaces $\mathscr{L}_p$

Définition 20.

— Pour $p \in [1, +\infty[$, on note $\mathscr{L}_p(X, \mathscr{A}, \mu))$ (où $\mathscr{L}_p$ en l'absence d'ambiguïté) l'ensemble des applications f mesurables de $(X, \mathscr{A}, \mu)$ dans $(\mathbb{R}, \mathscr{B}(R))$ telles que

$$\int_X |f(x)|^p \, \mathrm{d}\mu(x) < +\infty$$

on note alors $\|f\|_p = \left(\int_X |f(x)|^p \, \mathrm{d}\mu(x)\right)^{\frac{1}{p}}$.

— On note de même $\mathscr{L}_\infty$ l'ensemble des applications mesurables de $(X, \mathscr{A}, \mu)$ dans $(\mathbb{R}, \mathscr{B}(R))$ de sup-essentiel borné. On note alors $\|f\|_\infty$ pour $f \in \mathscr{L}_\infty$.

[B-P] p. 163

Exemple 21. Si μ est la mesure de comptage sur $(\mathscr{P}(\mathbb{N}),\mathbb{N})$, alors

$$\mathscr{L}_p = \ell_p = \left\{(u_n) \in \mathbb{R}^n \mid \sum_{n\geq 0} |u_n|^p < +\infty\right\}$$

Proposition 22. $\mathscr{L}_p$ est un sous-espace vectoriel de l'espace vectoriel des fonctions de X dans $\mathbb{R}$.

Théorème 23 (Inégalité de Hölder)**.** Soient $p,q \in]1,+\infty[$ tels que $\frac{1}{p}+\frac{1}{q}=1$, $f \in \mathscr{L}_p$ et $g \in \mathscr{L}_q$. Alors $fg \in \mathscr{L}_1$ et

$$\|fg\|_1 \leq \|f\|_p \|g\|_q$$

[G-K] p. 209

Remarque 24. C'est encore vrai pour $q = +\infty$ en convenant que $\frac{1}{+\infty} = 0$.

Application 25. On considère la fonction Γ d'Euler. Alors,

$$\forall \theta \in]0,1[, \forall x,y>0,\ \Gamma(\Theta x + (1-\Theta)y) \leq \Gamma(x)^\theta \Gamma(y)^{1-\theta}$$

et en particulier, Γ est log-convexe sur $\mathbb{R}_*^+$.

Théorème 26 (Inégalité de Minkowski)**.**

$$\forall f,g \in \mathscr{L}_p,\ \|f+g\|_p \leq \|f\|_p + \|g\|_p$$

L'application $\|.\|_p$ définit donc une semi-norme sur $\mathscr{L}_p$ pour $p \in [1,+\infty]$. L'idée dans la sous-section suivante sera de construire un espace dans lequel l'axiome de séparation n'est pas pris en défaut.

2. Construction des espaces L_p

Définition 27. On définit pour tout $p \in [1,+\infty]$,

$$L_p = \mathscr{L}_p / V$$

où $V = \{v \in \mathscr{L}_p \mid v = 0 \text{ pp.}\}$.

Proposition 28. Dans un espace de mesure finie,

$$1 \leq p < q \leq +\infty \implies L_q \subseteq L_p$$

Contre-exemple 29. La fonction $\mathbb{1}$ est dans $L_\infty(\mathbb{R}, \mathscr{B}(\mathbb{R}), \lambda)$ mais dans aucun $L_p(\mathbb{R}, \mathscr{B}(\mathbb{R}), \lambda)$ pour tout $p \in [1, +\infty[$.

Théorème 30. Pour tout $p \in [1, +\infty]$, (L_p), $\|.\|_p$ est un espace vectoriel normé.

Théorème 31 (Riesz-Fischer)**.** Pour tout $p \in [1, +\infty]$, L_p est complet pour la norme $\|.\|_p$.

3. Convolution et régularisation dans L_1

Définition 32. Soient f et g deux fonctions de $\mathbb{R}^d$ dans $\mathbb{R}$. On dit que **la convolée** (ou **le produit de convolution**) de f et g en $x \in \mathbb{R}$ **existe** si la fonction

[AMR08] p. 75

$$\begin{array}{ccc} \mathbb{R} & \to & \mathbb{C} \\ t & \mapsto & f(x-t)g(t) \end{array}$$

est intégrable sur $\mathbb{R}^d$ pour la mesure de Lebesgue. On pose alors :

$$(f * g)(x) = \int_{\mathbb{R}^d} f(x-t)g(t)\,\mathrm{d}t$$

Exemple 33. Soient $a < b \in \mathbb{R}_*^+$. Alors $\mathbb{1}_{[-a,a]} * \mathbb{1}_{[-b,b]}$ existe pour tout $x \in \mathbb{R}$ et

$$\left(\mathbb{1}_{[-a,a]} * \mathbb{1}_{[-b,b]}\right)(x) = \begin{cases} 2a & \text{si } 0 \le |x| \le b-a \\ b+a-|x| & \text{si } b-a \le |x| \le b+a \\ 0 & \text{sinon} \end{cases}$$

Proposition 34. Dans $L_1(\mathbb{R}^d)$, dès qu'il a un sens, le produit de convolution de deux fonctions est commutatif, bilinéaire et associatif.

Théorème 35 (Convolution dans $L_1(\mathbb{R}^d)$)**.** Soient $f, g \in L_1(\mathbb{R}^d)$. Alors :

(i) pp. en $x \in \mathbb{R}^d$, $t \mapsto f(x-t)g(t)$ est intégrable sur $\mathbb{R}^d$.

(ii) $f * g$ est intégrable sur $\mathbb{R}^d$.

(iii) $\|f * g\|_1 \le \|f\|_1 \|g\|_1$.

(iv) L'espace vectoriel normé $(L_1(\mathbb{R}^d), \|.\|_1)$ muni de $*$ est une algèbre de Banach commutative.

Proposition 36. L'algèbre $(L_1(\mathbb{R}^d), +, *, \cdot)$ n'a pas d'élément unité.

p. 114

Application 37.

$$f * f = f \iff f = 0$$

Définition 38. On appelle **approximation de l'identité** toute suite (ρ_n) de fonctions mesurables de $L_1(\mathbb{R}^d)$ telles que

(i) $\forall n \in \mathbb{N}, \int_{\mathbb{R}^d} \rho_n \, \mathrm{d}\lambda_d = 1$.

(ii) $\sup_{n\geq 1} \|\rho_n\| < +\infty$.

(iii) $\forall \epsilon > 0, \lim_{n\to+\infty} \int_{\mathbb{R}\setminus B(0,\epsilon)} \rho_n(x)\,\mathrm{d}x = 0$.

[B-P] p. 306

Exemple 39. $\forall n \in \mathbb{N}$, on note :

$$a_n = \int_{-1}^{1} (1-t^2)^n \,\mathrm{d}t \text{ et } p_n : t \mapsto \frac{(1-t^2)^n}{a_n} \mathbb{1}_{[-1,1]}(t)$$

Alors, (p_n) est une approximation positive de l'identité.

[GOU20] p. 304

Application 40. (i) $\mathscr{C}_K^\infty(\mathbb{R}^d)$ est dense dans $\mathscr{C}_K(\mathbb{R}^d)$ pour $\|.\|_\infty$.

(ii) $\mathscr{C}_K^\infty(\mathbb{R}^d)$ est dense dans $L_p(\mathbb{R}^d)$ pour $\|.\|_p$ avec $p \in [1, +\infty[$.

[AMR08] p. 96

III - Espace L_2

1. Propriétés hilbertiennes

Définition 41. On considère la forme bilinéaire suivante sur L_2 :

$$\langle .,. \rangle : (f,g) \mapsto \int_X f\overline{g}\,\mathrm{d}\mu$$

C'est un produit scalaire hermitien, ce qui confère à $(L_2, \langle .,. \rangle)$ une structure d'espace de Hilbert.

[BMP] p. 92

On peut donc énoncer quelques propriétés dont hérite L_2.

Théorème 42. Pour tout sous-espace vectoriel fermé F de L_2,

$$L_2 = F \oplus F^\perp$$

p. 98

Corollaire 43. Un sous-espace vectoriel F de L_2 est dense dans L_2 si et seulement si $F^\perp = \{0\}$.

Théorème 44. Soit $(e_n)_{n\in I}$ une famille orthonormée dénombrable de L_2. Les propriétés suivantes sont équivalentes :

(i) La famille orthonormée $(e_n)_{n\in I}$ est une base hilbertienne de H.

(ii) $\forall f \in L_2,\ f = \sum_{n=0}^{+\infty} \langle f, e_n\rangle e_n$.

(iii) $\forall f \in L_2,\ \|f\|_2 = \sum_{n=0}^{+\infty} |\langle f, e_n\rangle|^2$.

2. Polynômes orthogonaux

Soit I un intervalle de $\mathbb{R}$. On pose $\forall n \in \mathbb{N},\ g_n : x \mapsto x^n$.

p. 110

Définition 45. On appelle **fonction poids** une fonction $\rho : I \to \mathbb{R}$ mesurable, positive et telle que $\forall n \in \mathbb{N}, \rho g_n \in L_1(I)$.

Soit $\rho : I \to \mathbb{R}$ une fonction poids.

Notation 46. On note $L_2(I,\rho)$ l'espace des fonctions de carré intégrable pour la mesure de densité ρ par rapport à la mesure de Lebesgue.

Proposition 47. Muni de

$$\langle .,. \rangle : (f,g) \mapsto \int_I f(x)\overline{g(x)}\rho(x)\,\mathrm{d}x$$

$L_2(I,\rho)$ est un espace de Hilbert.

Théorème 48. Il existe une unique famille (P_n) de polynômes unitaires orthogonaux deux-à-deux telle que $\deg(P_n) = n$ pour tout entier n. C'est la famille de **polynômes orthogonaux** associée à ρ sur I.

Exemple 49 (Polynômes de Hermite)**.** Si $\forall x \in I,\ \rho(x) = e^{-x^2}$, alors

$$\forall n \in \mathbb{N},\ \forall x \in I,\ P_n(x) = \frac{(-1)^n}{2^n} e^{x^2} \frac{\partial}{\partial x^n}\left(e^{-x^2}\right)$$

Lemme 50. On suppose que $\forall n \in \mathbb{N},\ g_n \in L_1(I,\rho)$ et on considère (P_n) la famille des polynômes orthogonaux associée à ρ sur I. Alors $\forall n \in \mathbb{N},\ g_n \in L_2(I,\rho)$. En particulier, l'algorithme de Gram-Schmidt a bien du sens et (P_n) est bien définie.

p. 140

Application 51. On considère (P_n) la famille des polynômes orthogonaux associée à ρ sur I

et on suppose qu'il existe $a > 0$ tel que

$$\int_I e^{a|x|}\rho(x)\,\mathrm{d}x < +\infty$$

alors (P_n) est une base hilbertienne de $L_2(I,\rho)$ pour la norme $\|.\|_2$.

Contre-exemple 52. On considère, sur $I = \mathbb{R}_*^+$, la fonction poids $\rho : x \mapsto x^{-\ln(x)}$. Alors, la famille des g_n n'est pas totale. La famille des polynômes orthogonaux associée à ce poids particulier n'est donc pas totale non plus : ce n'est pas une base hilbertienne.

IV - Dualité

Définition 53. On appelle **forme linéaire** d'un espace vectoriel E sur un corps $\mathbb{K}$ toute application linéaire de E dans $\mathbb{K}$ et on note E^* appelé **dual** de E l'ensemble des formes linéaires de E.

On note E' le **dual topologique** de E, qui est le sous-espace de E^* constitué des formes linéaires continues.

[GOU21] p. 132

Théorème 54 (de représentation de Riesz)**.** L'application

$$\Phi : \begin{array}{ccc} H & \to & H' \\ y & \mapsto & (x \mapsto \langle x, y\rangle) \end{array}$$

est une isométrie linéaire bijective de H sur son dual topologique H'.

[BMP] p. 103

Exemple 55. Dans le cas $L_2(X,\mu)$,

$$\forall \varphi \in L_2', \exists! g \in H, \text{ telle que } \forall f \in L_2, \varphi(f) = \int_X f(g)\overline{g(x)}\,\mathrm{d}\mu(x)$$

[DEV]

Théorème 56 (Dual de L_p)**.** On se place dans un espace mesuré de mesure finie. On note $\forall p \in]1,2[$. L'application

$$\varphi : \begin{array}{ccc} L_q & \to & (L_p)' \\ g & \mapsto & \left(\varphi_g : f \mapsto \int_X f g\,\mathrm{d}\mu\right) \end{array} \qquad \text{où } \frac{1}{p} + \frac{1}{q} = 1$$

est une isométrie linéaire surjective. C'est donc un isomorphisme isométrique.

[Z-Q] p. 222

[LI] p. 140

Remarque 57. Plus généralement, si l'on identifie g et φ_g :

— L_q est le dual topologique de L_p pour $p \in]1, +\infty[$.

— L_∞ est le dual topologique de L_1 si μ est σ-finie.

203 Utilisation de la notion de compacité.

I - Diverses caractérisations de la compacité

1. Caractérisation topologique

Définition 1. Un espace métrique (E,d) est **compact** s'il vérifie la propriété de Borel-Lebesgue : [GOU20] p. 27

De toute recouvrement de E par des ouverts de E, on peut en extraire un sous-recouvrement fini.

Exemple 2. Tout espace métrique fini est compact.

Proposition 3. Un espace métrique (E,d) est compact si de toute famille de fermés de E d'intersection vide, on peut extraire une sous-famille d'intersection vide.

Proposition 4. (i) Une réunion finie de parties compactes est compacte.
(ii) Une intersection quelconque de parties compactes est compacte.

2. Caractérisation séquentielle

Soit (E,d) un espace métrique.

[DAN] p. 51

Théorème 5 (Bolzano-Weierstrass)**.** (E,d) est compact si toute suite de E admet une sous-suite convergente dans E.

Exemple 6. Tout segment $[a,b]$ de $\mathbb{R}$ est compact, mais $\mathbb{R}$ n'est pas compact.

Proposition 7. (i) Un espace métrique compact est complet.
(ii) Un espace métrique compact est borné.

Proposition 8. Soit $A \subseteq E$.
(i) Si A est compacte, alors A est une partie fermée bornée de E.
(ii) Si E est compact et A est fermée, alors A est compacte.

Proposition 9. Un produit d'espaces métriques compacts est compact pour la distance produit.

Application 10. Soit (E,d) un espace métrique compact. Soit (u_n) une suite de E telle que $d(u_n,u_{n-1}) \longrightarrow 0$. Alors l'ensemble Γ des valeurs d'adhérence de (u_n) est connexe. **[I-P]** p. 116

Corollaire 11 (Lemme de la grenouille)**.** Soient $f : [0,1] \to [0,1]$ continue et (x_n) une suite de $[0,1]$ telle que

$$\begin{cases} x_0 \in [0,1] \\ x_{n+1} = f(x_n) \end{cases}$$

Alors (x_n) converge si et seulement si $\lim_{n\to+\infty} x_{n+1} - x_n = 0$.

3. Caractérisation dans un espace vectoriel normé de dimension finie

[DEV]

Théorème 12. En dimension finie, toutes les normes sont équivalentes. **[LI]** p. 15

Corollaire 13. Les parties compactes d'un espace vectoriel normé de dimension finie sont les parties fermées bornées.

Corollaire 14.
(i) Tout espace vectoriel de dimension finie est complet.
(ii) Tout espace vectoriel de dimension finie dans un espace vectoriel normé est fermé dans cet espace.
(iii) Si E est un espace vectoriel normé, alors toute application linéaire $T : E \to F$ (où F désigne un espace vectoriel normé arbitraire) est continue.

Application 15. L'exponentielle d'une matrice est un polynôme en la matrice. **[C-G]** p. 407

Théorème 16 (Riesz)**.** La boule unité fermée d'un espace vectoriel normé est compacte si et seulement s'il est dimension finie. **[LI]** p. 17

II - Utilisation en analyse

1. Continuité et compacité

Proposition 17. Soient (E, d_E), (F, d_F) deux espaces métriques et $f : E \to F$ une application continue. Si E est compact, alors $f(E)$ est compact. **[DAN]** p. 55

Corollaire 18. Toute application définie et continue sur un espace métrique compact à valeurs dans un espace métrique est bornée.

Proposition 19. Sous les hypothèses et notations de la Théorème 17, en supposant de plus f injective, alors f réalise un homéomorphisme entre E et $f(E)$.

Théorème 20 (des bornes)**.** Toute fonction réelle continue sur un espace métrique compact est bornée et atteint ses bornes.

Corollaire 21 (Théorème des valeurs intermédiaires)**.** L'image d'un segment $[a, b]$ de $\mathbb{R}$ par une fonction réelle continue est un segment $[c, d]$ de $\mathbb{R}$.

Application 22 (Théorème de Rolle)**.** Soit f une fonction réelle continue sur un intervalle $[a, b]$, dérivable sur $]a, b[$ et telle que $f(a) = f(b)$. Alors, **[GOU20]** p. 73

$$\exists c \in]a, b[\text{ tel que } f'(c) = 0$$

Application 23 (Point fixe dans un compact)**.** Soit (E, d) un espace métrique compact et $f : E \to E$ telle que **[ROU]** p. 171

$$\forall x, y \in E,\ x \neq y \implies d(f(x), f(y)) < d(x, y)$$

alors f admet un unique point fixe et pour tout $x_0 \in E$, la suite des itérés

$$x_{n+1} = f(x_n)$$

converge vers ce point fixe.

Exemple 24. sin admet un unique point fixe sur $[0, 1]$.

Application 25 (Théorème de d'Alembert-Gauss)**.** Tout polynôme non constant de $\mathbb{C}$ admet une racine dans $\mathbb{C}$. **[DAN]** p. 58

Théorème 26 (Heine)**.** Une application continue à valeurs dans un espace métrique définie sur un espace métrique compact est uniformément continue.

Théorème 27 (Théorèmes de Dini)**.** [GOU20] p. 238

(i) Soit (f_n) une suite *croissante* de fonctions réelles *continues* définies sur un segment I de $\mathbb{R}$. Si (f_n) converge simplement vers une fonction *continue* sur I, alors la convergence est uniforme.

(ii) Soit (f_n) une suite de *fonctions croissantes* réelles *continues* définies sur un segment I de $\mathbb{R}$. Si (f_n) converge simplement vers une fonction *continue* sur I, alors la convergence est uniforme.

2. Approximation de fonctions

[DEV]

Théorème 28 (Weierstrass)**.** p. 304 Toute fonction continue $f : [a,b] \to \mathbb{R}$ (avec $a, b \in \mathbb{R}$ tels que $a \leq b$) est limite uniforme de fonctions polynômiales sur $[a,b]$.

On a une version plus générale de ce théorème.

Théorème 29 (Stone-Weierstrass)**.** [LI] p. 46 Soit K un espace compact et $\mathscr{A}$ une sous-algèbre de l'algèbre de Banach réelle $\mathscr{C}(K,\mathbb{R})$. On suppose de plus que :

(i) $\mathscr{A}$ sépare les points de K (ie. $\forall x \in K, \exists f \in A$ telle que $f(x) \neq f(y)$).

(ii) $\mathscr{A}$ contient les constantes.

Alors $\mathscr{A}$ est dense dans $\mathscr{C}(K,\mathbb{R})$.

Remarque 30. Il existe aussi une version "complexe" de ce théorème, où il faut supposer de plus que $\mathscr{A}$ est stable par conjugaison.

Exemple 31. La suite de polynômes réels (r_n) définie par récurrence par

$$r_0 = 0 \text{ et } \forall n \in \mathbb{N}, r_{n+1} : t \mapsto r_n(t) + \frac{1}{2}(t - r_n(t)^2)$$

converge vers $\sqrt{.}$ sur $[0,1]$.

3. Étude d'équations différentielles

Théorème 32 (Arzelà-Peano)**.** Soit F une fonction continue sur un ouvert U de $\mathbb{R}\times\mathbb{R}^n$ à valeurs dans $\mathbb{R}^n$. On considère l'équation différentielle

$$y' = F(t,y)$$

Pour tout couple (y_0,t_0) de U, le problème de Cauchy admet une solution y définie sur un intervalle ouvert contenant t_0.

[GOU20] p. 375

Exemple 33. L'équation différentielle

$$y' = \begin{cases} 0 & \text{si } y<0 \\ \sqrt{y} & \text{si } y\geq 0 \end{cases}$$

admet des solutions.

Théorème 34 (Lemme de sortie de tout compact)**.** Soient $]a,b[$ un intervalle ouvert de $\mathbb{R}$, O un ouvert de $\mathbb{R}^n$ et $F:]a,b[\times O\to\mathbb{R}^n$ une fonction continue et localement lipschitzienne en la seconde variable. Soit $\varphi:]\alpha,\beta[\to\mathbb{R}^n$ une solution maximale de $y'=F(t,y)$.

Alors, si $\beta<b$ (resp. si $a<\alpha$), pour tout compact $K\subseteq O$, il existe un voisinage V de β (resp. de α) dans $]\alpha,\beta[$ tel que $\varphi(t)\notin K$ pour tout $t\in V$.

p. 400

4. Recherche d'extrema

Proposition 35. Le maximum de

$$f:\begin{array}{ccc}\mathbb{R}^n\times\cdots\times\mathbb{R}^n & \to & \mathbb{R} \\ (v_1,\dots,v_n) & \mapsto & \det(v_1,\dots,v_n)\end{array}$$

est atteint sur le cercle unité de $\mathbb{R}^n$.

[ROU] p. 409

Corollaire 36 (Inégalité de Hadamard)**.**

$$\forall v_1,\dots,v_n\in\mathbb{R}^n,\ |\det(v_1,\dots,v_n)|\leq\|v_1\|\dots\|v_n\|$$

où $\|.\|$ désigne la norme associée au produit scalaire usuel sur $\mathbb{R}^n$. On a égalité si et seulement si un des v_i est nul.

Remarque 37. Géométriquement, cette inégalité exprime que les parallélépipèdes de volume maximum sont rectangles.

5. Convexité et compacité

Théorème 38 (Hahn-Banach géométrique)**.** Soit E un espace vectoriel normé. Soient C et K deux parties non vides de E disjointes et telles que C soit convexe et fermée, et K soit convexe et compacte.Alors, il existe une forme linéaire continue $\varphi in E'$ telle que :

$$\sup_{x\in C} \mathrm{Re}(\varphi(x)) < \inf_{x\in K} \mathrm{Re}(\varphi(x))$$

[LI] p. 159

Corollaire 39 (Théorème de Minkowski)**.** Toute partie convexe et fermée d'un espace vectoriel normé réel est égale àl'intersection des demi-espaces fermés qui le contiennent.

Corollaire 40. Soit H un espace de Hilbert sur $\mathbb{R}$ et soit D une partie de H. Alors l'enveloppe convexe fermée de D est égale à l'intersection des demi-espaces de la forme

$$\{y \in H \mid f(y) \leq \alpha\}$$

qui contiennent D, où $f \in H'$ et $\alpha \in \mathbb{R}$.

[BMP] p. 133

III - Utilisation en algèbre

Proposition 41. (i) $\mathrm{SO}_n(\mathbb{R})$ est compact (et connexe).
(ii) $\mathcal{O}_n(\mathbb{R})$ est compact (non-connexe).

[C-G] p. 62

Application 42 (Décomposition polaire)**.** L'application

$$\mu : \begin{array}{ccc} \mathcal{O}_n(\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R}) & \to & \mathrm{GL}_n(\mathbb{R}) \\ (O,S) & \mapsto & OS \end{array}$$

est un homéomorphisme.

p. 376

Corollaire 43. Tout sous-groupe compact de $\mathrm{GL}_n(\mathbb{R})$ qui contient $\mathcal{O}_n(\mathbb{R})$ est $\mathcal{O}_n(\mathbb{R})$.

Corollaire 44. $\mathrm{GL}_n(\mathbb{R})^+$ est connexe.

p. 401

204 Connexité. Exemples d'applications.

I - Diverses approches de la connexité

Soit (E,d) un espace métrique.

1. Une approche topologique

Proposition 1. Les assertions suivantes sont équivalentes. [GOU20] p. 38

(i) Il n'existe pas de partition de E en deux ouverts disjoints non vides.

(ii) Il n'existe pas de partition de E en deux fermés disjoints non vides.

(iii) Les seules parties ouvertes de E sont $\emptyset$ et E.

Définition 2. Un espace métrique vérifiant l'une des assertions de Théorème 1 est dit **connexe**.

Remarque 3. Remarquons qu'il s'agit-là d'une définition *topologique* : tous les résultats de cette sous-section sont donc valables dans le cadre plus général d'un espace topologique.

Proposition 4. Soit $A \subseteq E$. Les assertions suivantes sont équivalentes.

(i) A est connexe.

(ii) Si $A \subseteq O_1 \cap O_2$ avec O_1, O_2 ouverts de E tels que $A \cap O_1 \cap O_2 = \emptyset$, alors

$$(A \cap O_1 = \emptyset \text{ et } A \subseteq O_2) \text{ ou } (A \cap O_2 = \emptyset \text{ et } A \subseteq O_1)$$

(iii) Si $A \subseteq F_1 \cap F_2$ avec F_1, F_2 fermés de E tels que $A \cap F_1 \cap F_2 = \emptyset$, alors

$$(A \cap F_1 = \emptyset \text{ et } A \subseteq F_2) \text{ ou } (A \cap F_2 = \emptyset \text{ et } A \subseteq F_1)$$

Exemple 5. $\mathbb{Q}$ n'est pas un connexe de $\mathbb{R}$.

Proposition 6. Une partie ouverte et fermée d'un espace connexe est vide ou égale à l'espace entier. p. 350

Proposition 7. L'image d'un connexe par une application continue est connexe. p. 39

p. 44

Application 8. Soit $f : \mathbb{U} \to \mathbb{R}$ continue. Alors il existe deux points diamétralement opposés de $\mathbb{U}$ qui ont la même image par f.

Corollaire 9. E est connexe si et seulement si toute application continue de E dans $\{0,1\}$ est constante. p. 39

Proposition 10. Soit $(C_i)_{i\in I}$ une famille de parties connexes de E. On suppose que

$$\exists i_0 \in I \text{ tel que } \forall i \in I,\ C_{i_0} \cap C_i \neq \emptyset$$

Alors, $\bigcup_{i\in I} C_i$ est connexe.

Contre-exemple 11. $\{0\}$ et $\{1\}$ sont des connexes de $\mathbb{R}$, mais pas $\{0\} \cup \{1\} = \{0,1\}$.

Proposition 12. Un produit fini d'espaces métriques est connexe si et seulement si ces espaces métriques sont tous connexes.

[DEV]

Application 13. Soit (E,d) un espace métrique compact. Soit (u_n) une suite de E telle que $d(u_n, u_{n-1}) \longrightarrow 0$. Alors l'ensemble Γ des valeurs d'adhérence de (u_n) est connexe. **[I-P]** p. 116

Corollaire 14 (Lemme de la grenouille)**.** Soient $f : [0,1] \to [0,1]$ continue et (x_n) une suite de $[0,1]$ telle que

$$\begin{cases} x_0 \in [0,1] \\ x_{n+1} = f(x_n) \end{cases}$$

Alors (x_n) converge si et seulement si $\lim_{n\to+\infty} x_{n+1} - x_n = 0$.

2. Une approche géométrique

Définition 15. On appelle **chemin** de E tout application $\gamma : [0,1] \to E$ continue. L'image $\gamma^* = \gamma([0,1])$ du chemin s'appelle un **arc**, $\gamma(0)$ **l'origine** de l'arc et $\gamma(1)$ son **extrémité**. **[GOU20]** p. 42

Définition 16. E est dit **connexe par arcs** si pour tout $(a,b) \in E^2$, il existe un arc inclus dans E d'origine a et d'extrémité b.

Remarque 17. Il s'agit là encore d'une définition topologique.

Théorème 18. Un espace connexe par arcs est connexe.

Contre-exemple 19. L'ensemble

$$\Gamma = \left(\bigcup_{x\in\mathbb{Q}} (\{x\}\times\mathbb{R}^+)\right) \cup \left(\bigcup_{x\in\mathbb{R}\setminus\mathbb{Q}} (\{x\}\times\mathbb{R}_*^-)\right)$$

est un connexe de $\mathbb{R}^2$ non connexe par arcs.

Proposition 20. La réciproque est vraie dans un ouvert d'un espace vectoriel normé.

Application 21. $\mathbb{R}$ et $\mathbb{R}^2$ ne sont pas homéomorphes.

3. Une approche algébrique

Définition 22. On définit la relation $\mathscr{R}$ suivante sur E :

$$x\mathscr{R}y \iff \exists C \subseteq E \text{ connexe tel que } x,y \in E$$

Proposition 23. (i) $\mathscr{R}$ est une relation d'équivalence sur E.

(ii) Si $x \in E$, sa classe d'équivalence est la réunion des connexes contenant x.

Définition 24. Une classe d'équivalence pour la relation $\mathscr{R}$ est une **composante connexe** de E.

Remarque 25. E est la réunion disjointe de ses composantes connexes. E est donc connexe s'il n'admet qu'une seule composante connexe.

Exemple 26. On se place dans le cadre où E est un espace vectoriel euclidien. Alors, $\mathscr{O}(E)$ est non-connexe. Ses composantes connexes sont $\mathrm{SO}(E)$ et $\{u \in \mathscr{O}(E) \mid \det(u) = -1\}$. **[ROM21]** p. 724

Proposition 27. Les composantes connexes de E sont des fermés de E. Si elles sont en nombre fini, ce sont également des ouverts de E. **[GOU20]** p. 41

II - Exemples d'applications en analyse

1. En analyse réelle

Théorème 28. Les connexes de $\mathbb{R}$ sont les intervalles. p. 41

Théorème 29 (Des valeurs intermédiaires)**.** Soient I un intervalle de $\mathbb{R}$ et $f : I \to \mathbb{R}$ continue sur I. Alors $f(I)$ est un intervalle.

Remarque 30. Une autre manière d'écrire ce résultat est que si $f(a) \leq f(b)$ (resp. $f(a) \geq f(b)$) avec $a < b$, alors pour tout $\gamma \in [f(a), f(b)]$ (resp. pour tout $\gamma \in [f(b), f(a)]$), il existe $c \in [a, b]$ tel que $f(c) = \gamma$.

Corollaire 31 (Théorème de Darboux)**.** Soient I un intervalle de $\mathbb{R}$ et $f : I \to \mathbb{R}$ dérivable sur I. Alors $f'(I)$ est un intervalle. p. 47

2. En calcul différentiel

Proposition 32. Soit U un ouvert connexe d'un espace vectoriel normé E. Soit $f : U \to F$ où F est un espace vectoriel normé. Si f est différentiable telle que $\forall x \in U$, $\mathrm{d}f_x = 0$, alors f est constante sur U. p. 328

Exemple 33. Soit f une fonction holomorphe sur un ouvert connexe Ω de $\mathbb{C}$ telle que la suite $(f^{(n)})$ converge uniformément sur tout compact de Ω. On note g la limite de la suite $(f^{(n)})$. Alors, il existe $C \in \mathbb{C}$ tel que $g = C\exp$. **[BMP]** p. 80

Proposition 34. Soit U un ouvert connexe d'un espace vectoriel normé E. Soit $f : U \to E$. Si f est de classe $\mathscr{C}^1$ telle que $\forall x \in U$, $\mathrm{d}f_x$ est une isométrie, alors f est une isométrie affine. **[GOU20]** p. 349

3. En analyse complexe

Soit $\Omega \subseteq \mathbb{C}$ un ouvert. On suppose Ω connexe. Soit $f : \Omega \to \mathbb{C}$. **[BMP]** p. 53

Théorème 35 (Zéros isolés)**.** Si f est une fonction analytique sur Ω et si f n'est pas identiquement nulle, alors l'ensemble des zéros de f n'admet pas de point d'accumulation dans Ω.

Corollaire 36. L'ensemble des zéros d'une fonction analytique non nulle sur Ω est au plus dénombrable.

Remarque 37 (Prolongement analytique). Reformulé de manière équivalente au Théorème 35, si deux fonctions analytiques coïncident sur un sous-ensemble de Ω qui possède un point d'accumulation dans Ω, alors elles sont égales sur Ω.

Exemple 38. Il existe une unique fonction g holomorphe sur $\mathbb{C}$ telle que

$$\forall n \in \mathbb{N}^*, g\left(\frac{1}{n}\right) = \frac{1}{n}$$

et c'est la fonction identité.

p. 77

Contre-exemple 39. Il existe au moins deux fonctions g holomorphes sur $\Omega = \{z \in \mathbb{C} \mid \mathrm{Re}(z) > 0\}$ telles que

$$\forall n \in \mathbb{N}^*, g\left(\frac{1}{n}\right) = 0$$

Application 40 (Transformée de Fourier d'une Gaussienne)**.** On a

$$\forall x \in \mathbb{R}, \int_{\mathbb{R}} e^{-t^2} e^{-itx} \, \mathrm{d}t = \sqrt{\pi} e^{-\frac{x^2}{4}}$$

p. 83

Théorème 41 (Principe du maximum)**.** On suppose Ω borné et f holomorphe sur Ω et continue sur $\overline{\Omega}$. On note M le maximum de f sur la frontière de Ω. Alors,

(i) Pour tout $z \in \Omega$, $|f(z)| \leq M$.

(ii) S'il existe $z_0 \in \Omega$ tel que $|f(z)| = M$, alors f est constant sur Ω.

p. 72

Application 42. Soit (f_n) une suite de fonctions holomorphes sur Ω et continues sur $\overline{\Omega}$. Si (f_n) converge uniformément sur la frontière de Ω, alors (f_n) converge uniformément sur Ω et la limite est holomorphe.

p. 80

Application 43. On suppose que $D(0,1) \subseteq \Omega$ et f holomorphe sur Ω. On suppose de plus que $f(0) = 1$ et $|f(z)| \geq 2$ sur le cercle unité. Alors f s'annule sur le cercle unité.

III - Exemple d'application en algèbre

Proposition 44. $\mathrm{GL}_n(\mathbb{R})$ n'est pas connexe. Ses composantes connexes sont $\mathrm{GL}_n(\mathbb{R})^+$ et $\mathrm{GL}_n(\mathbb{R})^-$. **[BMP]** p. 213

Application 45. $\exp : \mathcal{M}_n(\mathbb{R}) \to \mathrm{GL}_n(\mathbb{R})$ n'est pas surjective.

Proposition 46. $\mathrm{GL}_n(\mathbb{C})$ est connexe par arcs. **[ROM21]** p. 770

Lemme 47. (i) Soit $A \in \mathcal{M}_n(\mathbb{C})$. Alors $\exp(A) \in \mathrm{GL}_n(\mathbb{C})$.
(ii) $\exp$ est différentiable en 0 et $\mathrm{d}\exp_0 = \mathrm{id}_{\mathcal{M}_n(\mathbb{C})}$.
(iii) Soit $M \in \mathrm{GL}_n(\mathbb{C})$. Alors $M^{-1} \in \mathbb{C}[M]$. **[I-P]** p. 396

[DEV] **Théorème 48.** $\exp : \mathcal{M}_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$ est surjective.

Application 49. $\exp(\mathcal{M}_n(\mathbb{R})) = \mathrm{GL}_n(\mathbb{R})^2$, où $\mathrm{GL}_n(\mathbb{R})^2$ désigne les carrés de $\mathrm{GL}_n(\mathbb{R})$.

205 Espaces complets. Exemples et applications.

I - Complétude

1. Complétude dans un espace métrique

Soit (E,d) un espace métrique.

[GOU20] p. 20

Définition 1. On dit qu'une suite (x_n) d'éléments de E est **de Cauchy** si

$$\forall \epsilon > 0, \exists N \in \mathbb{N} \text{ tel que } \forall p > q \geq N, d(u_p, u_q) < \epsilon$$

Proposition 2. (i) Une suite convergente est de Cauchy.
(ii) Une suite de Cauchy est bornée.
(iii) Une suite de Cauchy qui possède une valeur d'adhérence ℓ converge vers ℓ.

Contre-exemple 3. La série $\sum \frac{1}{n}$ est une suite de Cauchy de $\mathbb{Q}$ non convergente dans $\mathbb{Q}$.

[HAU] p. 312

Remarque 4. La notion de suite de Cauchy n'est pas topologique : elle ne peut pas être définie à partir des ouverts de E. Cependant, si une suite est de Cauchy pour une certaine distance, alors elle l'est pour toute autre distance équivalente.

[GOU20] p. 20

Définition 5. E est **complet** si toute suite de Cauchy de E converge dans E.

Exemple 6. $\forall n \in \mathbb{N}^*$, $\mathbb{R}^n$ est complet mais $\mathbb{Q}$ ne l'est pas.

Proposition 7. (i) Toute partie complète d'un espace métrique est fermée.
(ii) Toute partie fermée d'un espace complet est complète.

Proposition 8. Soient $E_1, \dots, E_n$ des espaces métriques. Alors $E_1 \times \cdots \times E_n$ est complet si et seulement si $\forall i \in [\![1,n]\!]$, E_i est complet.

Proposition 9 (Fermés emboîtés)**.** E est complet si et seulement si toute suite décroissante de fermés non-vides de E dont le diamètre converge vers 0 converge vers un singleton.

Proposition 10 (Critère de Cauchy pour les fonctions)**.** Soit (F, d') un espace métrique complet. Soient $f : A \to F$ où $A \subseteq E$ et $a \in \overline{A}$. Alors f admet une limite quand x tend vers a si et seulement si

$$\forall \epsilon > 0, \exists \eta > 0 \text{ tel que } \forall x, y \in A,\ d(a,x) < \eta \text{ et } d(a,y) < \eta \implies d'(f(x), f(y)) < \epsilon$$

Théorème 11 (Complété d'un espace métrique)**.** Il existe un espace métrique complet $\widehat{E}$ et $i : E \to \widehat{E}$ une isométrie telle que $i(E)$ est dense dans $\widehat{E}$. De plus, $\widehat{E}$ est unique à isométrie bijective près. p. 25

Exemple 12. $\mathbb{R}$ est le complété de $\mathbb{Q}$.

2. Complétude dans un espace vectoriel normé

Définition 13. Un espace vectoriel normé complet est un **espace de Banach**. p. 20

Proposition 14. Un espace vectoriel normé E est complet si et seulement si toute série absolument convergence de E est convergente dans E. p. 52

Proposition 15. Un espace vectoriel de dimension finie est complet.

Application 16. L'exponentielle d'une matrice est un polynôme en la matrice. **[C-G]** p. 407

3. Exemples et contre-exemples classiques

Contre-exemple 17. L'espace des fonctions polynômiales définies sur $[-1,1]$ et muni de la norme $\|.\|_\infty$ n'est pas complet. **[DAN]** p. 45

Exemple 18. Soient X un ensemble et E un espace de Banach. Alors, $(\mathscr{B}(X,E), \|.\|_\infty)$ est un espace de Banach. **[GOU20]** p. 21

Exemple 19. Si E est un espace vectoriel normé et F est un espace de Banach, $(\mathscr{L}(E,F), |||.|||)$ est un espace de Banach. p. 8

[LI] p. 7

Définition 20. — Pour $p \in [1,+\infty[$, on note $\mathscr{L}_p(X,\mathscr{A},\mu)$) (où $\mathscr{L}_p$ en l'absence d'ambiguïté) l'espace des applications f mesurables de $(X,\mathscr{A},\mu)$ dans $(\mathbb{R},\mathscr{B}(R))$ telles que

$$\int_X |f(x)|^p \,\mathrm{d}\mu(x) < +\infty$$

on note alors $\|f\|_p = \left(\int_X |f(x)|^p \,\mathrm{d}\mu(x)\right)^{\frac{1}{p}}$.

— On note de même $\mathscr{L}_\infty$ l'espace des applications mesurables de $(X,\mathscr{A},\mu)$ dans $(\mathbb{R},\mathscr{B}(R))$ de sup-essentiel borné. On note alors $\|f\|_\infty$ pour $f \in \mathscr{L}_\infty$.

Remarque 21. En reprenant les notations précédentes, on a $\forall f \in \mathscr{L}_p$, $\|f\|_p = 0 \iff f = 0$ pp..

Théorème 22 (Inégalité de Minkowski)**.**

$$\forall f,g \in \mathscr{L}_p,\ \|f+g\|_p \leq \|f\|_p + \|g\|_p$$

Théorème 23. On définit pour tout $p \in [1,+\infty]$,

$$L_p = \mathscr{L}_p / V$$

où $V = \{v \in \mathscr{L}_p \mid v = 0 \text{ pp.}\}$. Muni de $\|.\|_p$, L_p est un espace vectoriel normé.

Théorème 24 (Riesz-Fischer)**.** Pour tout $p \in [1,+\infty]$, L_p est complet pour la norme $\|.\|_p$.

II - Espaces de Hilbert

1. Généralités

Définition 25. Un espace vectoriel H sur le corps $\mathbb{K}$ est un **espace de Hilbert** s'il est muni d'un produit scalaire $\langle .,. \rangle$ et est complet pour la norme associée $\|.\| = \sqrt{\langle .,. \rangle}$.

p. 31

Exemple 26. Tout espace euclidien ou hermitien est un espace de Hilbert.

Exemple 27. $L_2(\mu)$ muni de $\langle .,. \rangle : (f,g) \mapsto \int f\overline{g}\,\mathrm{d}\mu$ est un espace de Hilbert.

Pour toute la suite, on fixe H un espace de Hilbert de norme $\|.\|$ et on note $\langle .,. \rangle$ le produit scalaire associé.

Lemme 28 (Identité du parallélogramme)**.**

$$\forall x, y \in H,\ \|x+y\|^2 + \|x-y\|^2 = 2(\|x\|^2\|y\|^2)$$

et cette identité caractérise les normes issues d'un produit scalaire.

[DEV]

Théorème 29 (Projection sur un convexe fermé)**.** Soit $C \subseteq H$ un convexe fermé non-vide. Alors :

$$\forall x \in H, \exists! y \in C \text{ tel que } d(x,C) = \inf_{z\in C} \|x-z\| = d(x,y)$$

On peut donc noter $y = P_C(x)$, le **projeté orthogonal de** x **sur** C. Il s'agit de l'unique point de C vérifiant

$$\forall z \in C, \langle x - P_C(x), z - P_C(x)\rangle \leq 0$$

Théorème 30. Si F est un sous espace vectoriel fermé dans H, alors P_F est une application linéaire continue. De plus, pour tout $x \in H$, $P_F(x)$ est l'unique point $y \in F$ tel que $x - y \in F^\perp$.

Théorème 31. Si F est un sous espace vectoriel fermé dans H, alors

$$H = F \oplus F^\perp$$

et P_F est la projection sur F parallèlement à $F^\perp$: c'est la **projection orthogonale** sur F.

Corollaire 32. Soit F un sous-espace vectoriel de H. Alors,

$$\overline{F} = H \iff F^\perp = 0$$

Théorème 33 (de représentation de Riesz)**.**

$$\forall \varphi \in H', \exists! y \in H, \text{ tel que } \forall x \in H, \varphi(x) = \langle x, y\rangle$$

et de plus, $|||\varphi||| = \|y\|$.

Corollaire 34.

$$\forall T \in H', \exists! U \in H' \text{ tel que } \forall x, y \in H, \langle T(x), y\rangle = \langle x, U(y)\rangle$$

On note alors $U = T^*$: c'est **l'adjoint** de T. On a alors $|||T||| = |||T^*|||$.

p. 65

Exemple 35 (Opérateur de Voltera)**.** On définit T sur $H = L_2([0,1])$ par :

$$T : \begin{array}{ccc} H & \to & H \\ f & \mapsto & x \mapsto \int_0^x f(t)\,\mathrm{d}t \end{array}$$

T est une application linéaire continue et son adjoint T^* est défini par :

$$T^* : g \mapsto \left(x \mapsto \int_x^1 g(t)\,\mathrm{d}t\right)$$

[DEV]

Application 36 (Dual de L_p)**.** Soit $(X, \mathscr{A}, \mu)$ un espace mesuré de mesure finie. On note $\forall p \in]1,2[$,

$$\varphi : \begin{array}{ccc} L_q & \to (L_p)' & \\ g & \mapsto \left(\varphi_g : f \mapsto \int_X fg\,\mathrm{d}\mu\right) & \text{où } \dfrac{1}{p} + \dfrac{1}{q} = 1 \end{array}$$

est une isométrie linéaire surjective. C'est donc un isomorphisme isométrique.

[Z-Q] p. 222

2. Bases hilbertiennes

Définition 37. On dit que $(e_n) \in H^{\mathbb{N}}$ est une **base hilbertienne** de H si

- (e_n) est orthonormale.
- (e_n) est totale.

[LI] p. 43

Exemple 38. $(t \mapsto e^{2\pi i n t})_{n\in\mathbb{Z}}$ est une base hilbertienne de $L_2([0,1])$.

Théorème 39. Soit $(e_n)_{n\in\mathbb{N}}$ une base hilbertienne de H. Alors :

$$\forall x \in H,\ x = \sum_{n=0}^{+\infty} \langle x, e_n\rangle e_n$$

On a de plus, pour tout $x, y \in H$, les formules de Parseval :

- $\|x\|^2 = \sum_{n=0}^{+\infty} |\langle x, e_n\rangle|^2$.
- $\langle x, y\rangle = \sum_{n=0}^{+\infty} \langle x, e_n\rangle \overline{\langle y, e_n\rangle}$.

Application 40.

$$\sum_{n=1}^{+\infty} \frac{1}{n^4} = \frac{\pi^4}{90}$$

[GOU20] p. 272

III - Applications

1. Point fixe

Théorème 41 (Point fixe de Banach)**.** Soient (E,d) un espace métrique complet et $f : E \to E$ une application contractant (ie. $\exists k \in]0,1[$ tel que $\forall x,y \in E,\ d(f(x),f(y)) \leq k d(x,y)$). Alors,

$$\exists! x \in E \text{ tel que } f(x) = x$$

De plus la suite des itérés définie par $x_0 \in E$ et $\forall n \in \mathbb{N}, x_{n+1} = f(x_n)$ converge vers x.

p. 21

Application 42 (Théorème de Cauchy-Lipschitz local)**.** Soit E un espace de Banach sur $\mathbb{R}$ ou $\mathbb{C}$. Soient I un intervalle de $\mathbb{R}$ et Ω un ouvert de E. Soit $F : I \times \Omega \to E$ une fonction continue et localement lipschitzienne en la seconde variable. Alors, pour tout $(t_0,y_0) \in I \times \Omega$, le problème de Cauchy

$$\begin{cases} y' = F(t,y) \\ y(t_0) = y_0 \end{cases} \qquad (C)$$

admet une unique solution maximale.

p. 374

2. Prolongement

Théorème 43 (Prolongement des applications uniformément continues)**.** Soient (E,d_E) et (F,d_F) des espaces métriques. On suppose F complet. Soient $A \subseteq E$ dense et $f : A \to F$ une application uniformément continue. Alors, il existe une unique application $\widehat{f} : E \to F$ uniformément continue et telle que $\widehat{f}_{|A} = f$.

[DAN] p. 47

Corollaire 44. Soient (E,d_E) et (F,d_F) des espaces métriques. On suppose F complet. Soient $A \subseteq E$ dense et $f : A \to F$ une application k-lipschitzienne. Alors, il existe une unique application $\widehat{f} : E \to F$ k-lipschitzienne et telle que $\widehat{f}_{|A} = f$.

Exemple 45. Une application dérivable sur un intervalle $]a,b[$ et de dérivée bornée est prolongeable par une application lipschitzienne sur $[a,b]$.

Application 46 (Théorème de Hahn-Banach analytique)**.** Soient H un espace de Hilbert et F un sous-espace vectoriel de H. Soit $f \in F'$. Alors, il existe $\widehat{f} \in H'$ telle que $\widehat{f}_{|F} = f$ et $|||\widehat{f}|||_H = |||f|||_F$.

[BMP] p. 106

[LI] p. 94

Application 47 (Transformation de Fourier-Plancherel)**.** La transformation de Fourier $\mathscr{F}$ définie sur $L_1(\mathbb{R}) \cap L_2(\mathbb{R})$ se prolonge de manière unique en un isomorphisme d'espaces de Hilbert de $L_2(\mathbb{R})$ sur lui-même.

3. Théorème de Baire

Théorème 48 (Baire)**.** On suppose E complet. Alors toute intersection d'ouvert denses est encore dense dans E.

[LI] p. 111

Application 49. Un espace vectoriel normé à base dénombrable n'est pas complet.

[GOU20] p. 419

Application 50 (Théorème de Banach-Steinhaus)**.** Soient $(E, \|.\|_E)$ et $(F, \|.\|_F)$ deux espaces de Banach et $(T_i)_{i\in I}$ des applications linéaires continues telles que

$$\forall x \in E, \sup_{i\in I} \|T_i(x)\|_F < +\infty$$

alors,

$$\sup_{i\in I} |||T_i||| < +\infty$$

[LI] p. 112

Application 51 (Théorème du graphe fermé)**.** Soient E et F deux espaces de Banach et $T \in L(E,F)$. Si le graphe de T :

$$\{(x, T(x)) \mid x \in E\} \subseteq E \times F$$

est fermé dans $E \times F$, alors T est continue.

Application 52 (Théorème de l'application ouverte)**.** Soient E et F deux espaces de Banach et $T \in \mathscr{L}(E,F)$ surjective. Alors,

$$\exists c > 0, T(B_E(0,1)) \supseteq B_F(0,c)$$

Corollaire 53 (Théorème des isomorphismes de Banach)**.** Soient E et F deux espaces de Banach et $T \in \mathscr{L}(E,F)$ bijective. Alors T^{-1} est continue.

Corollaire 54. On suppose que E est de Banach. Soient E_1 et E_2 deux supplémentaires algébriques fermés dans E. Alors les projections associées sur E_1 et E_2 sont continues.

206 Exemples d'utilisation de la notion de dimension finie en analyse.

I - Espaces vectoriels normés

1. Complétude

Soit (E,d) un espace métrique.

[DAN] p. 52

Définition 1. On dit que E est complet si toute suite de Cauchy de E est convergente dans E.

Exemple 2.
— $(\mathbb{R},|.|)$ est complet.
— $(\mathbb{R}^p,|.|)$ est complet pour tout $p\in\mathbb{N}^*$.

Proposition 3. On suppose que E est un espace métrique complet. Soit $A\subseteq E$. Alors (A,d) est complet si et seulement si A est une partie fermée de E.

Proposition 4. On suppose que E est un espace vectoriel sur $\mathbb{R}$ de dimension finie $n\geq 1$ muni de la norme infinie $\|.\|_\infty$. Alors E est un espace vectoriel normé complet.

Contre-exemple 5. L'espace des fonctions polynômiales définies sur $[-1,1]$ et muni de la norme $\|.\|_\infty$ n'est pas complet.

Application 6 (Théorème du point fixe de Banach)**.** Soient (E,d) un espace métrique complet et $f:E\to E$ une application contractant (ie. $\exists k\in]0,1[$ tel que $\forall x,y\in E,\ d(f(x),f(y))\leq d(x,y)$). Alors,

$$\exists! x\in E \text{ tel que } f(x)=x$$

De plus la suite des itérés définie par $x_0\in E$ et $\forall n\in\mathbb{N}, x_{n+1}=f(x_n)$ converge vers x.

Application 7 (Théorème de prolongement des applications uniformément continues)**.** Soient (E,d_E) et (F,d_F) des espaces métriques. On suppose F complet. Soient $A\subseteq E$ dense et $f:A\to F$ une application uniformément continue. Alors, il existe une unique application $\widehat{f}:E\to F$ uniformément continue et telle que $\widehat{f}_{|A}=f$.

2. Compacité

Soit (E,d) un espace métrique.

[DAN] p. 51

Définition 8. Un espace métrique est **compact** s'il vérifie la propriété de Bolzano-Weierstrass :

De toute suite de l'espace on peut extraire une sous-suite convergente dans cet espace.

Exemple 9. Tout segment $[a,b]$ de $\mathbb{R}$ est compact, mais $\mathbb{R}$ n'est pas compact.

Proposition 10. (i) Un espace métrique compact est complet.
(ii) Un espace métrique compact est borné.

Proposition 11. Soit $A \subseteq E$.
(i) Si A est compacte, alors A est une partie fermée bornée de E.
(ii) Si E est compact et A est fermée, alors A est compacte.

Proposition 12. Un produit d'espaces métriques compacts est compact pour la distance produit.

Proposition 13. On suppose que E est un espace vectoriel de dimension finie $n \geq 1$ muni de la norme infinie $\|.\|_\infty$. Les compacts de cet espace vectoriel normé sont les parties fermées et bornées.

Application 14. Un intervalle de $\mathbb{R}$ est compact si et seulement si c'est un segment.

3. Équivalence des normes

Soit E un espace vectoriel.

[LI] p. 15

Définition 15. On dit que deux normes $\|.\|_1$ et $\|.\|_2$ sur E sont équivalentes si

$$\exists \alpha, \beta > 0 \text{ tels que } \forall x \in E,\ \alpha\|x\|_2 \leq \|x\|_1 \leq \beta\|x\|_2$$

Remarque 16. Deux normes équivalentes sur E définissent la même topologie sur E.

[DEV]

Théorème 17. En dimension finie, toutes les normes sont équivalentes.

Le corollaire suivant justifie l'étude de la compacité dans la Section 2.

Corollaire 18. Les parties compactes d'un espace vectoriel normé de dimension finie sont les parties fermées bornées.

Et le corollaire suivant justifie l'étude de la complétude dans la Section 1.

Corollaire 19.
(i) Tout espace vectoriel de dimension finie est complet.
(ii) Tout espace vectoriel de dimension finie dans un espace vectoriel normé est fermé dans cet espace.
(iii) Si E est un espace vectoriel normé, alors toute application linéaire $T : E \to F$ (où F désigne un espace vectoriel normé arbitraire) est continue.

Application 20 (Théorème de d'Alembert-Gauss)**.** Tout polynôme non constant de $\mathbb{C}$ admet une racine dans $\mathbb{C}$. **[DAN]** p. 58

Application 21. L'exponentielle d'une matrice est un polynôme en la matrice. **[C-G]** p. 407

Théorème 22 (Riesz)**.** La boule unité fermée d'un espace vectoriel normé est compacte si et seulement s'il est dimension finie. **[LI]** p. 17

4. Applications linéaires

Soient $(E, \|.\|_E)$ et $(F, \|.\|_F)$ deux espaces vectoriels normés sur $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. **[GOU20]** p. 48

Notation 23. On note $L(E,F)$ l'ensemble des applications linéaires de E dans F et $\mathscr{L}(E,F)$ l'ensemble des applications linéaires continues de E dans F. Si $E = F$, on note $L(E,F) = L(E)$ et $\mathscr{L}(E,F) = \mathscr{L}(E)$.

Théorème 24. Soit $f \in L(E,F)$. Les assertions suivantes sont équivalentes.
(i) $f \in \mathscr{L}(E,F)$.
(ii) f est continue en 0.
(iii) f est bornée sur $\overline{B}(0,1) \subseteq E$.
(iv) f est bornée sur $S(0,1) \subseteq E$.
(v) Il existe $M \geq 0$ tel que $\|f(x)\|_F \leq M\|x\|_E$.
(vi) f est lipschitzienne.
(vii) f est uniformément continue sur E.

Proposition 25. Toute application linéaire d'un espace vectoriel normé de dimension finie dans un espace vectoriel normé quelconque est continue.

Contre-exemple 26. La dérivation sur $\mathbb{K}[X]$, $P \mapsto P'$ n'est pas continue.

II - Espaces de Hilbert

1. Espaces de Hilbert et dimension finie

Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

[LI] p. 31

Définition 27. Un espace vectoriel H sur le corps $\mathbb{K}$ est un **espace de Hilbert** s'il est muni d'un produit scalaire $\langle .,. \rangle$ et est complet pour la norme associée $\|.\| = \sqrt{\langle .,. \rangle}$.

Exemple 28. Tout espace préhilbertien (ie. muni d'un produit scalaire) de dimension finie est un espace de Hilbert.

Théorème 29 (Projection sur un convexe fermé)**.** Soit $C \subseteq H$ un convexe fermé non-vide. Alors :

$$\forall x \in H, \exists! y \in C \text{ tel que } d(x,C) = \inf_{z \in C} \|x - z\| = d(x,y)$$

On peut donc noter $y = P_C(x)$, le **projeté orthogonal de** x **sur** C. Il s'agit de l'unique point de C vérifiant

$$\forall z \in C, \langle x - P_C(x), z - P_C(x) \rangle \leq 0$$

Théorème 30. Si F est un sous espace vectoriel fermé dans H (par exemple, si F est de dimension finie), alors P_F est une application linéaire continue. De plus, pour tout $x \in H$, $P_F(x)$ est l'unique point $y \in F$ tel que $x - y \in F^\perp$.

Théorème 31. Si F est un sous espace vectoriel fermé dans H (par exemple, si F est de dimension finie), alors

$$H = F \oplus F^\perp$$

et P_F est la projection sur F parallèlement à $F^\perp$: c'est la **projection orthogonale** sur F.

[BMP] p. 93

Remarque 32. En reprenant les notations précédentes, en supposant F de dimension finie et en notant $(e_1, \dots, e_n)$ une base orthonormée de F, alors

$$\forall x \in H, p_F(x) = \sum_{i=1}^{n} \langle x, e_i \rangle e_i$$

2. Séries de Fourier

Notation 33. — Pour tout $p \in [1,+\infty]$, on note $L_p^{2\pi}$ l'espace des fonctions $f : \mathbb{R} \to \mathbb{C}$, 2π-périodiques et mesurables, telles que $\|f\|_p < +\infty$.

— Pour tout $n \in \mathbb{Z}$, on note e_n la fonction 2π-périodique définie pour tout $t \in \mathbb{R}$ par $e_n(t) = e^{int}$.

[Z-Q] p. 73

Remarque 34.

$$1 \leq p < q \leq +\infty \implies L_q^{2\pi} \subseteq L_p^{2\pi} \text{ et } \|.\|_p \leq \|.\|_q$$

Proposition 35. $L_2^{2\pi}$ est un espace de Hilbert pour le produit scalaire

$$\langle .,. \rangle : (f,g) \mapsto \frac{1}{2\pi} \int_0^{2\pi} f(t)\overline{g(t)}\,\mathrm{d}t$$

Théorème 36. La famille $(e_n)_{n\in\mathbb{Z}}$ est une base hilbertienne (totale et orthonormée) de $L_2^{2\pi}$.

[BMP] p. 123

Corollaire 37. Soit $n \geq 1$. On note

$$\mathscr{P}_n = \mathrm{Vect}(e_k)_{k\in[\![1,n]\!]}$$

le sous-espace vectoriel des polynômes trigonométriques de degré n. Alors :

(i) $L_2^{2\pi} = \mathscr{P}_n \oplus \mathscr{P}_n^{\perp}$.

(ii) $P_{\mathscr{P}_n}(f) = S_n(f)$ où $S_n(f)$ est la somme partielle d'ordre n de la série de Fourier de f.

(iii) $\inf_{g\in\mathscr{P}_n} \|f-g\|^2 = \|f - S_n(f)\|^2 = \frac{1}{2\pi}\int_0^{2\pi} |f(t)|^2\,\mathrm{d}t - \sum_{k=-n}^{n} |c_k(f)|^2$ où $c_k(f)$ est le k-ième coefficient de Fourier.

[GOU21] p. 270

Application 38 (Inégalité de Beissel)**.**

$$\sum_{k=-\infty}^{+\infty} |c_k(f)|^2 \leq \frac{1}{2\pi}\int_0^{2\pi} |f(t)|^2\,\mathrm{d}t$$

Remarque 39. Cette inégalité est en fait une égalité : c'est l'égalité de Parseval.

Exemple 40. On considère $f : x \mapsto 1 - \frac{x^2}{\pi^2}$ sur $[-\pi,\pi]$. Alors,

$$\frac{\pi^4}{90} = \|f\|_2 = \sum_{n=0}^{+\infty} \frac{1}{n^4}$$

III - Calcul différentiel

1. Différentielle et dérivées partielles

Soient $(E, \|.\|_E)$ et $(F, \|.\|_F)$ deux espaces vectoriels normés sur $\mathbb{R}$. Soient $U \subseteq E$ ouvert et $f : U \to F$ une application de U dans F. [GOU20] p. 323

Définition 41. f est dite **différentiable** en un point a de U s'il existe $\ell_a \in \mathscr{L}(E,F)$ telle que

$$f(a+h) = f(a) + \ell_a(h) + o(\|h\|_E) \text{ quand } h \longrightarrow 0$$

Si ℓ_a existe, alors elle est unique et on la note $\mathrm{d}f_a$: c'est la **différentielle** de f en a.

Remarque 42.
— En dimension quelconque $\mathrm{d}f_a$ dépend a priori des normes $\|.\|_E$ et $\|.\|_F$. Cependant, en dimension finie, l'équivalence des normes implique que l'existence et la valeur de $\mathrm{d}f_a$ ne dépend pas des normes choisies.
— La définition demande à ℓ_a d'être continue. En dimension finie, le problème ne se pose donc pas.

Exemple 43. Si f est linéaire et continue, alors $\mathrm{d}f_a = f$ pour tout $a \in E$.

On se place maintenant dans le cas où $E = \mathbb{R}^n$.

Définition 44. Soit $a \in U$.

— Soit $v \in E$. Si la fonction de la variable réelle $\varphi : t \mapsto f(a+tv)$ est dérivable en 0, on dit que f est **dérivable en a selon le vecteur v**. On note alors

$$f'_v(a) = \varphi'(0)$$

— Soit $(e_1, \dots, e_n)$ la base canonique de $\mathbb{R}^n$ et soit $i \in [\![1, n]\!]$. On dit que f admet une **i-ième dérivée partielle en a** si f est dérivable en a selon le vecteur e_i. On note alors

$$\frac{\partial f}{\partial x_i}(a) = f'_{e_i}(a)$$

Proposition 45. Une fonction différentiable en un point est dérivable selon tout vecteur en ce point.

Contre-exemple 46. La fonction

$$\begin{array}{ccc} \mathbb{R}^2 & \to & \mathbb{R} \\ (x,y) & \mapsto & \begin{cases} \frac{y^2}{x} & \text{si } x \neq 0 \\ y & \text{sinon} \end{cases} \end{array}$$

est dérivable selon tout vecteur au point $(0,0)$ mais n'est pas continue en $(0,0)$.

Théorème 47. Si toutes les dérivées partielles de f existent et si elles sont continues en un point a de U, alors f est différentiable en a et on a

$$\mathrm{d}f_a = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(a) e_i^*$$

où $(e_i^*)_{i\in[\![1,n]\!]}$ est la base duale de la base canonique $(e_i)_{i\in[\![1,n]\!]}$ de $\mathbb{R}^n$.

Application 48. Soit $a \in U$. Si $F = \mathbb{R}^m$, la matrice de $\mathrm{d}f_a$ dans les bases canoniques de $\mathbb{R}^n$ et $\mathbb{R}^m$ est

$$\left(\frac{\partial f_i}{\partial x_j}(a)\right)_{\substack{i\in[\![1,n]\!] \\ j\in[\![1,m]\!]}}$$

(où l'on a noté $f = (f_1, \dots, f_m)$)) : c'est la **matrice jacobienne** de f en a.

2. Équations différentielles linéaires

p. 373

Définition 49. Soient $n \in \mathbb{N}^*$, E un espace de Banach et $\Omega \subseteq \mathbb{R} \times E^n$ un ouvert. Soit $F : \Omega \times \mathbb{R}^n \to E$ une fonction.

— On appelle **équation différentielle** une équation de la forme

$$y^{(n)} = F(t, y, y', \dots, y^{(n-1)}) \qquad (*)$$

(ie. une équation portant sur les dérivées d'une fonction.)

— Toute application $\varphi : I \to E$ (où I est un intervalle de $\mathbb{R}$) n fois dérivable vérifiant :

(i) $\forall t \in I, (t, \varphi(t), \dots, \varphi^{(n-1)}(t)) \in \Omega$;

(ii) $\forall t \in I, F(t, \varphi(t), \dots, \varphi^{(n-1)}(t)) = \varphi^{(n)}(t)$;

est une **solution** de $(*)$. On note $\mathcal{S}_*$ l'ensemble des solutions de $(*)$.

— Une solution $\varphi : I \to E$ de $(*)$ est dite **maximale** s'il n'existe pas d'autre solution $\psi : J \to E$ (où J est un intervalle de $\mathbb{R}$) de $(*)$ telle que $I \subseteq J$, $I \neq J$ et $\psi = \varphi$ sir I.

— On appelle **problème de Cauchy** de $(*)$ en $(t_0, x_0, \dots, x_{n-1})$ la recherche d'une solution

$\varphi : I \to E$ de $(*)$ vérifiant

$$\forall t_0 \in I, \varphi(t_0) = x_0, \dots, \varphi^{(n-1)}(t_0) = x_{n-1}$$

Définition 50. Toute équation différentielle sur $\mathbb{K}^n$ d'ordre $p \geq 1$ du type

$$Y^{(p)} = A_{p-1}(t)Y^{(p-1)} + \cdots + A_0(t)Y + B(t) \qquad (L)$$

(où $A_{p-1}, \dots, A_0$ sont des fonctions continues d'un intervalle I de $\mathbb{R}$ non réduit à un point dans $\mathcal{M}_n(\mathbb{K})$ et $B : I \to \mathbb{K}^n$ est une fonction continue) est appelée **équation différentielle linéaire** d'ordre p.

Si de plus $B = 0$, alors (L) est qualifiée d'**homogène**.

p. 377

[DEV]

Théorème 51 (Cauchy-Lipschitz linéaire)**.** Soient $A : I \to \mathcal{M}_n(\mathbb{K})$ et $B : I \to \mathbb{K}^d$ deux fonctions continues. Alors $\forall t_0 \in I$, le problème de Cauchy

$$\begin{cases} Y' = A(t)Y + B(t) \\ Y(t_0) = y_0 \end{cases}$$

admet une unique solution définie sur I tout entier.

[DAN] p. 520

Exemple 52. Considérons l'équation $y' - y = 0$. Comme la fonction nulle est solution maximale, il s'agit de l'unique solution qui s'annule sur $\mathbb{R}$.

[ROM19-1] p. 402

208 Espaces vectoriels normés, applications linéaires continues. Exemples.

Dans toute la suite, $\mathbb{K}$ désignera le corps $\mathbb{R}$ ou $\mathbb{C}$ et E un espace vectoriel sur $\mathbb{K}$.

I - Généralités

1. Normes sur un espace vectoriel

Définition 1. Une **norme** sur E est une application $\|.\| : E \to \mathbb{R}^+$ telle que :
(i) $\|x\| = 0 \iff x = 0$ (séparabilité).
(ii) $\forall \lambda \in \mathbb{K}, \forall x \in E, \|\lambda x\| = |\lambda|\|x\|$ (homogénéité).
(iii) $\forall x, y \in E, \|x+y\| \leq \|x\| + \|y\|$ (inégalité triangulaire).

[GOU20] p. 7

Exemple 2.
— $x \mapsto |x|$ est une norme sur $\mathbb{R}$, $z \mapsto |z|$ est une norme sur $\mathbb{C}$.
— $\forall \alpha \geq 1, \|.\|_\alpha : (x_1, \dots, x_n) \mapsto \left(\sum_{i=1}^n |x_i|^\alpha\right)^{\frac{1}{\alpha}}$ est une norme sur $\mathbb{R}^n$.

Définition 3. E est dit **normé** s'il est muni d'une norme $\|.\|$.

p. 47

Dans toute la suite, E désignera un espace vectoriel normé muni d'une norme $\|.\|$.

Définition 4. Deux normes $\|.\|_1$ et $\|.\|_2$ sur E sont dites **équivalentes** si

$$\exists a, b > 0 \text{ tels que } \forall x \in E,\ a\|x\|_1 \leq \|x\|_2 \leq b\|x\|_1$$

Remarque 5. Deux normes équivalentes définissent des distances équivalentes. Sur un plan topologique et lorsqu'on travaille avec des suites de Cauchy, il est indifférent de prendre l'une ou l'autre de ces normes.

2. Quelques exemples

Exemple 6. Comme mentionné précédemment, $\mathbb{R}^n$ et $\mathbb{C}^n$ sont des espaces vectoriels normés (munis de $\|.\|_\alpha$ définie à l'Théorème 2).

Exemple 7. L'ensemble $\mathscr{B}(X, E)$ des applications bornées d'un ensemble X dans E est un espace vectoriel normé muni de la norme $\|.\|_\infty : f \mapsto \sup_{x \in X} |f(x)|$.

p. 8

p. 53

Exemple 8. — $\ell_1(\mathbb{R}) = \{(u_n) \in \mathbb{R}^n \mid \sum_{n=0}^{+\infty} |u_n| < +\infty\}$ est un espace vectoriel normé muni de la norme $\|(u_n)\|_1 = \sum_{n=0}^{+\infty} |u_n|$.

— $\ell_\infty(\mathbb{R}) = \{(u_n) \in \mathbb{R}^n \mid (u_n) \text{ est bornée}\}$ est un espace vectoriel normé muni de la norme $\|(u_n)\|_\infty = \sup_{n\in\mathbb{N}} |u_n|$.

3. Applications linéaires continues

Soit $(F, \|.\|_F)$ un espace vectoriel normé sur $\mathbb{K}$. $\|.\|_E$ désigne la norme sur E.

p. 48

Notation 9. On note $L(E,F)$ l'ensemble des applications linéaires de E dans F et $\mathscr{L}(E,F)$ l'ensemble des applications linéaires continues de E dans F. Si $E = F$, on note $L(E,F) = L(E)$ et $\mathscr{L}(E,F) = \mathscr{L}(E)$.

Théorème 10. Soit $f \in L(E,F)$. Les assertions suivantes sont équivalentes.

(i) $f \in \mathscr{L}(E,F)$.

(ii) f est continue en 0.

(iii) f est bornée sur $\overline{B}(0,1) \subseteq E$.

(iv) f est bornée sur $S(0,1) \subseteq E$.

(v) Il existe $M \geq 0$ tel que $\|f(x)\|_F \leq M\|x\|_E$.

(vi) f est lipschitzienne.

(vii) f est uniformément continue sur E.

Corollaire 11. L'application $|||.||| : f \mapsto \sup_{\|x\|_E=1} \|f(x)\|_F = \sup_{x\neq 0} \frac{\|f(x)\|_F}{\|x\|_E}$ est correctement définie sur $\mathscr{L}(E,F)$ et définit une norme sur cet espace.

Remarque 12. Le réel $|||f|||$ du corollaire précédent est le plus petit réel positif M tel que $\|f(x)\|_F \leq M\|x\|_E$ pour tout $x \in E$. En particulier,

$$\forall x \in E,\ \|f(x)\|_F \leq |||f|||\,\|x\|_E$$

Proposition 13. Soient $(G, \|.\|_G)$ un espace vectoriel normé, $f \in \mathscr{L}(E,F)$ et $g \in \mathscr{L}(F,G)$. Alors, $|||g \circ f||| \leq |||g|||\,|||f|||$.

Proposition 14. Si $f \in \mathscr{L}(E,F)$ est inversible, $|||f|||^{-1} \leq |||f^{-1}|||$.

Proposition 15. Une forme linéaire sur E (ie. un élément de $L(E,\mathbb{K}) = E^*$) est continue (ie. est un élément de $\mathscr{L}(E,\mathbb{K}) = E'$) si et seulement si son noyau est fermé.

Exemple 16. L'application [LI] p. 19

$$\delta_0 : \begin{array}{ccc} \mathscr{C}([0,1],\mathbb{K}) & \to & \mathbb{K} \\ f & \mapsto & f(0) \end{array}$$

est continue pour $\|.\|_\infty$ mais pas pour $\|.\|_1$ (où $\|.\|_1 = \int_{[0,1]} |.| \mathrm{d}\mu$ et $\|.\|_\infty = \sup_{[0,1]}$).

II - Étude en dimension finie

On se place ici dans le cas où E est de dimension finie.

Théorème 17. Dans un espace vectoriel normé de dimension finie, toutes les normes sont équivalentes. [DEV]

Corollaire 18. Toute application linéaire d'un espace vectoriel normé de dimension finie dans un espace vectoriel normé (quelconque) est continue.

Corollaire 19. Tout sous-espace vectoriel d'un espace vectoriel normé de dimension finie est fermé.

Corollaire 20. Les parties compactes d'un espace vectoriel normé de dimension finie sont les parties fermées et bornées.

Contre-exemple 21. Munir $\mathbb{R}[X]$ de la norme $\|.\|_\infty \mapsto \sum_i a_i X^i \mapsto \sup_i |a_i|$ rend l'opérateur de dérivation $P \mapsto P'$ non continu.

Théorème 22 (Riesz)**.** La boule unité fermée d'un espace vectoriel normé est compacte si et seulement s'il est dimension finie. p. 56

III - Complétude

1. Espaces de Banach

Définition 23. Un espace vectoriel normé complet (ie. dans lequel toute suite de Cauchy converge) est un **espace de Banach**.

[LI] p. 20

Exemple 24. Tout espace vectoriel normé de dimension finie est complet.

p. 50

Exemple 25. Soit F un espace de Banach. Alors $\mathscr{L}(E,F)$ est un espace de Banach.

Exemple 26. Soient X un ensemble. On suppose que E un espace de Banach. Alors $\mathscr{B}(X,E)$ est un espace de Banach.

p. 21

Exemple 27. Pour tout compact K de $\mathbb{R}$, $(\mathscr{C}(K,\mathbb{K}),\|.\|_\infty)$ est complet. Mais pas $(\mathscr{C}(K,\mathbb{K}),\|.\|_1)$.

p. 10

Théorème 28 (Riesz-Fischer)**.** Pour tout $p \in [1,+\infty]$, L_p est complet pour la norme $\|.\|_p$.

Proposition 29. E est de Banach si et seulement si toute série de E absolument convergente est convergente.

[GOU20] p. 52

Théorème 30 (Baire)**.** On suppose E complet. Alors toute intersection d'ouvert denses est encore dense dans E.

[LI] p. 111

Application 31. Un espace vectoriel normé à base dénombrable n'est pas complet.

[GOU20] p. 419

Application 32 (Théorème de Banach-Steinhaus)**.** Soient $(E,\|.\|_E)$ et $(F,\|.\|_F)$ deux espaces de Banach et $(T_i)_{i\in I}$ des applications linéaires continues telles que

$$\forall x \in E,\ \sup_{i\in I} \|T_i(x)\|_F < +\infty$$

alors,

$$\sup_{i\in I} |||T_i||| < +\infty$$

[LI] p. 112

Application 33 (Théorème du graphe fermé)**.** Soient E et F deux espaces de Banach et $T \in L(E,F)$. Si le graphe de T :

$$\{(x,T(x)) \mid x \in E\} \subseteq E \times F$$

est fermé dans $E \times F$, alors T est continue.

Application 34 (Théorème de l'application ouverte)**.** Soient E et F deux espaces de Banach et $T \in \mathscr{L}(E,F)$ surjective. Alors,

$$\exists c > 0,\ T(B_E(0,1)) \supseteq B_F(0,c)$$

Corollaire 35 (Théorème des isomorphismes de Banach)**.** Soient E et F deux espaces de Banach et $T \in \mathscr{L}(E,F)$ bijective. Alors T^{-1} est continue.

Corollaire 36. On suppose que E est de Banach. Soient E_1 et E_2 deux supplémentaires algébriques fermés dans E. Alors les projections associées sur E_1 et E_2 sont continues.

2. Espaces de Hilbert

a. Généralités

Définition 37. Un espace vectoriel H sur le corps $\mathbb{K}$ est un **espace de Hilbert** s'il est muni d'un produit scalaire $\langle .,. \rangle$ et est complet pour la norme associée $\|.\| = \sqrt{\langle .,. \rangle}$.

[LI] p. 31

Exemple 38. Tout espace euclidien ou hermitien est un espace de Hilbert.

Exemple 39. $L_2(\mu)$ muni de $\langle .,. \rangle : (f,g) \mapsto \int f\overline{g}\,\mathrm{d}\mu$ est un espace de Hilbert.

Pour toute la suite, on fixe H un espace de Hilbert de norme $\|.\|$ et on note $\langle .,. \rangle$ le produit scalaire associé.

Lemme 40 (Identité du parallélogramme)**.**

$$\forall x,y \in H,\ \|x+y\|^2 + \|x-y\|^2 = 2(\|x\|^2\|y\|^2)$$

et cette identité caractérise les normes issues d'un produit scalaire.

[DEV]

Théorème 41 (Projection sur un convexe fermé)**.** Soit $C \subseteq H$ un convexe fermé non-vide. Alors :

$$\forall x \in H, \exists! y \in C \text{ tel que } d(x,C) = \inf_{z\in C} \|x - z\| = d(x,y)$$

On peut donc noter $y = P_C(x)$, le **projeté orthogonal de** x **sur** C. Il s'agit de l'unique point de C vérifiant

$$\forall z \in C, \langle x - P_C(x), z - P_C(x)\rangle \leq 0$$

Théorème 42. Si F est un sous espace vectoriel fermé dans H, alors P_F est une application linéaire continue. De plus, pour tout $x \in H$, $P_F(x)$ est l'unique point $y \in F$ tel que $x - y \in F^\perp$.

Corollaire 43. Soit F un sous-espace vectoriel de H. Alors,

$$\overline{F} = H \iff F^\perp = 0$$

Théorème 44 (de représentation de Riesz)**.**

$$\forall \varphi \in H', \exists! y \in H, \text{ tel que } \forall x \in H, \varphi(x) = \langle x, y\rangle$$

et de plus, $|||\varphi||| = \|y\|$.

Corollaire 45.

$$\forall T \in H', \exists! U \in H' \text{ tel que } \forall x, y \in H, \langle T(x), y\rangle = \langle x, U(y)\rangle$$

On note alors $U = T^*$: c'est **l'adjoint** de T. On a alors $|||T||| = |||T^*|||$.

Exemple 46 (Opérateur de Voltera)**.** On définit T sur $H = L_2([0,1])$ par : p. 65

$$T : \begin{array}{ccc} H & \to & H \\ f & \mapsto & x \mapsto \int_0^x f(t)\,\mathrm{d}t \end{array}$$

T est une application linéaire continue et son adjoint T^* est défini par :

$$T^* : g \mapsto \left(x \mapsto \int_x^1 g(t)\,\mathrm{d}t\right)$$

Application 47. L'application [Z-Q] p. 222

$$\varphi : \begin{array}{ccc} L_q & \to & (L_p)' \\ g & \mapsto & \left(\varphi_g : f \mapsto \int_X fg\,\mathrm{d}\mu\right) \end{array} \qquad \text{où } \frac{1}{p} + \frac{1}{q} = 1$$

est une isométrie linéaire surjective. C'est donc un isomorphisme isométrique.

b. Bases hilbertiennes

Définition 48. On dit que $(e_n) \in H^{\mathbb{N}}$ est une **base hilbertienne** de H si
- (e_n) est orthonormale.
- (e_n) est totale.

[LI] p. 43

Exemple 49. $(t \mapsto e^{2\pi i n t})_{n\in\mathbb{Z}}$ est une base hilbertienne de $L_2([0,1])$.

Théorème 50. Soit $(e_n)_{n\in\mathbb{N}}$ une base hilbertienne de H. Alors :

$$\forall x \in H,\ x = \sum_{n=0}^{+\infty} \langle x, e_n\rangle e_n$$

On a de plus, pour tout $x, y \in H$, les formules de Parseval :
- $\|x\|^2 = \sum_{n=0}^{+\infty} |\langle x, e_n\rangle|^2$.
- $\langle x, y\rangle = \sum_{n=0}^{+\infty} \langle x, e_n\rangle\overline{\langle y, e_n\rangle}$.

Application 51. On considère $f : x \mapsto 1 - \frac{x^2}{\pi^2}$ sur $[-\pi, \pi]$. Alors,

$$\frac{\pi^4}{90} = \|f\|_2 = \sum_{n=0}^{+\infty} \frac{1}{n^4}$$

[GOU20] p. 272

Annexes

[LI] p. 32

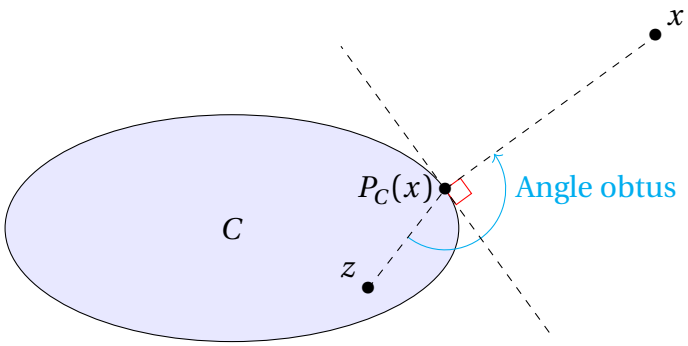


FIGURE I.19 – Illustration du théorème de projection sur un convexe fermé.

209 Approximation d'une fonction par des fonctions régulières. Exemples d'applications.

Dans toute la suite, $\mathbb{K}$ désignera le corps $\mathbb{R}$ ou $\mathbb{C}$.

I - Approximation par des polynômes

1. Approximation locale

Théorème 1 (Formule de Taylor-Lagrange)**.** Soit f une fonction réelle de classe $\mathscr{C}^n$ sur un intervalle $[a,b]$ telle que $f^{(n+1)}$ existe sur un intervalle $]a,b[$. Alors,

$$\exists c \in]a,b[\text{ tel que } f(b) = \underbrace{\sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(b-a)^k}_{=T_n(b)} + \frac{f^{(n+1)}(c)}{(n+1)!}(b-a)^{n+1}$$

[GOU20] p. 75

Application 2.
— $\forall x \in \mathbb{R}^+,\ x - \frac{x^2}{2} \leq \ln(1+x) \leq x - \frac{x^2}{2} + \frac{x^3}{3}$.
— $\forall x \in \mathbb{R}^+,\ x - \frac{x^3}{6} \leq \sin(x) \leq x - \frac{x^3}{6} + \frac{x^5}{120}$.
— $\forall x \in \mathbb{R},\ 1 - \frac{x^2}{2} \leq \cos(x) \leq 1 - \frac{x^2}{2} + \frac{x^4}{24}$.

Proposition 3. En reprenant les notations du Théorème 1, on a

$$\| \exp - T_n \|_\infty \longrightarrow 0$$

sur $[a,b]$.

2. Approximation sur un compact

Théorème 4 (Théorèmes de Dini)**.**
(i) Soit (f_n) une suite *croissante* de fonctions réelles *continues* définies sur un segment I de $\mathbb{R}$. Si (f_n) converge simplement vers une fonction *continue* sur I, alors la convergence est uniforme.
(ii) Soit (f_n) une suite de *fonctions croissantes* réelles *continues* définies sur un segment I de $\mathbb{R}$. Si (f_n) converge simplement vers une fonction *continue* sur I, alors la convergence est uniforme.

p. 238

p. 242

Théorème 5 (Bernstein)**.** Soit $f : [0,1] \to \mathbb{C}$ continue. On note

$$B_n(f) : x \mapsto \sum_{k=0}^{n} f\left(\frac{k}{n}\right)\binom{n}{k} x^k (1-x)^{n-k}$$

Alors,

$$\|B_n(f) - f\|_\infty \longrightarrow_{n\to+\infty} 0$$

[DEV]

Corollaire 6 (Weierstrass)**.** Toute fonction continue $f : [a,b] \to \mathbb{R}$ (avec $a, b \in \mathbb{R}$ tels que $a \leq b$) est limite uniforme de fonctions polynômiales sur $[a,b]$.

p. 304

On a une version plus générale de ce théorème.

Théorème 7 (Stone-Weierstrass)**.** Soit K un espace compact et $\mathscr{A}$ une sous-algèbre de l'algèbre de Banach réelle $\mathscr{C}(K,\mathbb{R})$. On suppose de plus que :

(i) $\mathscr{A}$ sépare les points de K (ie. $\forall x \in K, \exists f \in A$ telle que $f(x) \neq f(y)$).

(ii) $\mathscr{A}$ contient les constantes.

Alors $\mathscr{A}$ est dense dans $\mathscr{C}(K,\mathbb{R})$.

[LI] p. 46

Remarque 8. Il existe aussi une version "complexe" de ce théorème, où il faut supposer de plus que $\mathscr{A}$ est stable par conjugaison.

Exemple 9. La suite de polynômes réels (r_n) définie par récurrence par

$$r_0 = 0 \text{ et } \forall n \in \mathbb{N}, r_{n+1} : t \mapsto r_n(t) + \frac{1}{2}(t - r_n(t)^2)$$

converge vers $\sqrt{.}$ sur $[0,1]$.

3. Interpolation

Soit f une fonction réelle continue sur un intervalle $[a,b]$. On se donne $n+1$ points $x_0, \dots, x_n \in [a,b]$ distincts deux-à-deux.

[DEM] p. 21

Définition 10. Pour $i \in [\![0,n]\!]$, on définit le i-ième **polynôme de Lagrange** associé à $x_1, \dots, x_n$ par

$$\ell_i : x \mapsto \prod_{\substack{j=0 \\ j\neq i}}^{n} \frac{x - x_j}{x_i - x_j}$$

Théorème 11. Il existe une unique fonction polynômiale p_n de degré n telle que $\forall i \in [\![0,n]\!]$, $p_n(x_i) = f(x_i)$:

$$p_n = \sum_{i=0}^{n} f(x_i)\ell_i$$

Théorème 12. On note $\pi_{n+1} : x \mapsto \prod_{j=0}^{n}(x-x_j)$ et on suppose f $n+1$ fois dérivable $[a,b]$. Alors, pour tout $x \in [a,b]$, il existe un réel $\xi_x \in]\min(x,x_i), \max(x,x_i)[$ tel que

$$f(x) - p_n(x) = \frac{\pi_{n+1}(x)}{(n+1)!} f^{(n+1)}(\xi_x)$$

Corollaire 13.

$$\|f - p_n\|_\infty \leq \frac{1}{(n+1)!}\|\pi_{n+1}\|_\infty \|f^{(n+1)}\|_\infty$$

Application 14 (Calculs approchés d'intégrales)**.** On note $I(f) = \int_a^b f(t)\,\mathrm{d}t$. L'objectif est d'approximer $I(f)$ par une expression $P(f)$ et de majorer l'erreur d'approximation $E(f) = |I(f) - P(f)|$. **[DAN]** p. 506

(i) Méthode des rectangles. On suppose f continue. Avec $P(f) = (b-a)f(a)$, on a $E(f) \leq \frac{(b-a)^2}{2}\|f'\|_\infty$.

(ii) Méthode du point milieu. On suppose f de classe $\mathscr{C}^2$. Avec $P(f) = (b-a)f\left(\frac{a+b}{2}\right)$, on a $E(f) \leq \frac{(b-a)^3}{24}\|f''\|_\infty$.

(iii) Méthode des trapèzes. On suppose f de classe $\mathscr{C}^2$. Avec $P(f) = \frac{b-a}{2}(f(a)+f(b))$, on a $E(f) \leq \frac{(b-a)^3}{12}\|f''\|_\infty$.

(iv) Méthode de Simpson. On suppose f de classe $\mathscr{C}^4$. Avec $P(f) = \frac{b-a}{6}\left(f(a)+f(b)+4f\left(\frac{a+b}{2}\right)\right)$, on a $E(f) \leq \frac{(b-a)^3}{2880}\|f^{(4)}\|_\infty$.

II - Approximation dans les espaces de Lebesgue

1. Convolution

Définition 15. Soient f et g deux fonctions de $\mathbb{R}^d$ dans $\mathbb{R}$. On dit que **la convolée** (ou **le produit de convolution**) de f et g en $x \in \mathbb{R}$ **existe** si la fonction **[AMR08]** p. 75

$$\begin{array}{ccc} \mathbb{R} & \to & \mathbb{C} \\ t & \mapsto & f(x-t)g(t) \end{array}$$

est intégrable sur $\mathbb{R}^d$ pour la mesure de Lebesgue. On pose alors :

$$(f*g)(x) = \int_{\mathbb{R}^d} f(x-t)g(t)\,\mathrm{d}t$$

Proposition 16. Dans $L_1(\mathbb{R}^d)$, le produit de convolution est commutatif, bilinéaire et associatif.

Théorème 17. Soient $p,q>0$ et $f\in L_p(\mathbb{R}^d)$ et $g\in L_q(\mathbb{R}^d)$.

(i) Si $p,q\in[1,+\infty]$ tels que $\frac{1}{p}+\frac{1}{q}=1$, alors $(f*g)(x)$ existe pour tout $x\in\mathbb{R}^d$ et est uniformément continue. On a, $\|f*g\|_\infty \le \|f\|_p\|g\|_q$ et, si $p\neq 1,+\infty$, $f*g\in\mathscr{C}_0(\mathbb{R})$.

(ii) Si $p=1$ et $q=+\infty$, alors $(f*g)(x)$ existe pour tout $x\in\mathbb{R}^d$ et $f*g\in\mathscr{C}_b(\mathbb{R})$.

(iii) Si $p=1$ et $q\in[1,+\infty[$, alors $(f*g)(x)$ existe pp. en $x\in\mathbb{R}^d$ et $f*g\in L_q(\mathbb{R})$ telle que $\|f*g\|_q\le\|f\|_1\|g\|_q$.

(iv) Si $p=1$ et $q=1$, alors $(f*g)(x)$ existe pp. en $x\in\mathbb{R}^d$ et $f*g\in L_1(\mathbb{R})$ telle que $\|f*g\|_1\le\|f\|_1\|g\|_1$.

Exemple 18. Soient $a<b\in\mathbb{R}_*^+$. Alors $\mathbb{1}_{[-a,a]}*\mathbb{1}_{[-b,b]}$ existe pour tout $x\in\mathbb{R}$ et

$$\left(\mathbb{1}_{[-a,a]}*\mathbb{1}_{[-b,b]}\right)(x) = \begin{cases} 2a & \text{si } 0\le|x|\le b-a \\ b+a-|x| & \text{si } b-a\le|x|\le b+a \\ 0 & \text{sinon} \end{cases}$$

Proposition 19. $L_1(\mathbb{R}^d)$ est une algèbre de Banach pour le produit de convolution. p. 85

Remarque 20. Cette algèbre n'a pas d'élément neutre. Afin de pallier à ce manque, nous allons voir la notion d'approximation de l'identité dans la sous-section suivante.

2. Densité

Définition 21. On appelle **approximation de l'identité** toute suite (ρ_n) de fonctions mesurables de $L_1(\mathbb{R}^d)$ telles que [B-P] p. 306

(i) $\forall n\in\mathbb{N}$, $\int_{\mathbb{R}^d}\rho_n\,\mathrm{d}\lambda_d = 1$.

(ii) $\sup_{n\ge1}\|\rho_n\|<+\infty$.

(iii) $\forall\epsilon>0$, $\lim_{n\to+\infty}\int_{\mathbb{R}\setminus B(0,\epsilon)}\rho_n(x)\,\mathrm{d}x=0$.

Remarque 22. Dans la définition précédente, (ii) implique (i) lorsque les fonctions ρ_n sont positives. Plutôt que des suites, on pourra considérer les familles indexées par $\mathbb{R}_*^+$.

Exemple 23. — Noyau de Laplace sur $\mathbb{R}$:

$$\forall t > 0,\ \rho_t(x) = \frac{1}{2t} e^{-\frac{|x|}{t}}$$

— Noyau de Cauchy sur $\mathbb{R}$:

$$\forall t > 0,\ \rho_t(x) = \frac{t}{\pi(t^2 + x^2)}$$

— Noyau de Gauss sur $\mathbb{R}$:

$$\forall t > 0,\ \rho_t(x) = \frac{1}{\sqrt{2\pi}t} e^{-\frac{|x|^2}{2t^2}}$$

Théorème 24. Soit (ρ_n) une approximation de l'identité. Soient $p \in [1, +\infty[$ et $f \in L_p(\mathbb{R}^d)$, alors : p. 307

$$\forall n \geq 1,\ f * \rho_n \in L_p(\mathbb{R}^d) \quad \text{et} \quad \|f * \rho_n - f\|_p \longrightarrow 0$$

Théorème 25. Soient (ρ_n) une approximation de l'identité et $f \in L_\infty(\mathbb{R}^d)$. Alors :

— Si f est continue en $x_0 \in \mathbb{R}^d$, alors $(f * \rho_n)(x_0) \longrightarrow_{n\to+\infty} f(x_0)$.

— Si f est uniformément continue sur $\mathbb{R}^d$, alors $\|f * \rho_n - f\|_\infty \longrightarrow_{n\to+\infty} 0$.

— Si f est continue sur un compact K, alors $\sup_{x\in K} |(f * \rho_n)(x) - f(x)| \longrightarrow_{n\to+\infty} 0$.

Définition 26. On qualifie de **régularisante** toute suite (α_n) d'approximations de l'identité telle que $\forall n \in \mathbb{N},\ \alpha_n \in \mathscr{C}_K^\infty(\mathbb{R}^d)$.

Exemple 27. Soit $\alpha \in \mathscr{C}_K^\infty(\mathbb{R}^d)$ une densité de probabilité. Alors la suite (α_n) définie pour tout $n \in \mathbb{N}$ par $\alpha_n : x \mapsto n\alpha(nx)$ est régularisante. p. 274

Application 28. (i) $\mathscr{C}_K^\infty(\mathbb{R}^d)$ est dense dans $\mathscr{C}_K(\mathbb{R}^d)$ pour $\|.\|_\infty$. **[AMR08]** p. 96

(ii) $\mathscr{C}_K^\infty(\mathbb{R}^d)$ est dense dans $L_p(\mathbb{R}^d)$ pour $\|.\|_p$ avec $p \in [1, +\infty[$.

III - Approximations de fonctions périodiques

1. Séries de Fourier

Notation 29. — Pour tout $p \in [1,+\infty]$, on note $L_p^{2\pi}$ l'espace des fonctions $f : \mathbb{R} \to \mathbb{C}$, 2π-périodiques et mesurables, telles que $\|f\|_p < +\infty$.

— Pour tout $n \in \mathbb{Z}$, on note e_n la fonction 2π-périodique définie pour tout $t \in \mathbb{R}$ par $e_n(t) = e^{int}$.

[Z-Q] p. 73

Proposition 30. $L_2^{2\pi}$ est un espace de Hilbert pour le produit scalaire

$$\langle .,. \rangle : (f,g) \mapsto \frac{1}{2\pi} \int_0^{2\pi} f(t)\overline{g(t)}\,\mathrm{d}t$$

Définition 31. Soit $f \in L_1^{2\pi}$. On appelle :

— **Coefficients de Fourier complexes**, les complexes définis par

$$\forall n \in \mathbb{Z},\ c_n(f) = \frac{1}{2\pi} \int_0^{2\pi} f(t)e^{-int}\,\mathrm{d}t = \langle f, e_n \rangle$$

— **Coefficients de Fourier réels**, les complexes définis par

$$\forall n \in \mathbb{N},\ a_n(f) = \frac{1}{\pi} \int_0^{2\pi} f(t)\cos(nt)\,\mathrm{d}t \text{ et } \forall n \in \mathbb{N}^*,\ b_n(f) = \frac{1}{\pi} \int_0^{2\pi} f(t)\sin(nt)\,\mathrm{d}t$$

[GOU20] p. 268

2. Approximation hilbertienne

Théorème 32. Soit H un espace de Hilbert et $(\epsilon_n)_{n\in I}$ une famille orthonormée dénombrable de H. Les propriétés suivantes sont équivalentes :

(i) La famille orthonormée $(\epsilon_n)_{n\in I}$ est une base hilbertienne de H.

(ii) $\forall x \in H,\ x = \sum_{n=0}^{+\infty} \langle x, \epsilon_n \rangle \epsilon_n$.

(iii) $\forall x \in H,\ \|x\|_2 = \sum_{n=0}^{+\infty} |\langle x, \epsilon_n \rangle|^2$.

p. 109

Remarque 33. L'égalité du Théorème 1 Théorème 32 est appelée **égalité de Parseval**.

Théorème 34. La famille $(e_n)_{n\in\mathbb{Z}}$ est une base hilbertienne de $L_2^{2\pi}$.

p. 123

Corollaire 35.

$$\forall f \in L^{2\pi}_2,\ f = \sum_{n=-\infty}^{+\infty} c_n(f) e_n$$

Exemple 36. On considère $f : x \mapsto 1 - \frac{x^2}{\pi^2}$ sur $[-\pi, \pi]$. Alors, [GOU20] p. 272

$$\frac{\pi^4}{90} = \|f\|_2 = \sum_{n=0}^{+\infty} \frac{1}{n^4}$$

Remarque 37. L'égalité du Point (iii) est valable dans $L^{2\pi}_2$, elle signifie donc que [BMP] p. 124

$$\left\| \sum_{n=-N}^{N} c_n(f) e_n - f \right\|_2 \longrightarrow_{N \to +\infty} 0$$

3. Approximation au sens de Cesàro

Définition 38. Soit $f \in L^{2\pi}_1$. On appelle **série de Fourier** associée à f la série $(S_N(f))$ définie par [GOU20] p. 269

$$\forall N \in \mathbb{N},\ S_N(f) = \sum_{n=-N}^{N} c_n(f) e_n \overset{(*)}{=} \frac{a_0(f)}{2} + \sum_{n=1}^{N} (a_n(f)\cos(nx) + b_n(f)\sin(nx))$$

Remarque 39. L'égalité $(*)$ de la définition précédente est justifiée car,

$$\forall n \in \mathbb{N}^*,\ \forall x \in \mathbb{R},\ c_n(f)e^{inx} + c_{-n}(f)e^{-inx} = a_n(f)\cos(nx) + b_n(f)\sin(nx)$$

Définition 40. Pour tout $N \in \mathbb{N}$, la fonction $D_N = \sum_{n=-N}^{N} e_N$ est appelée **noyau de Dirichlet** d'ordre N. [AMR08] p. 184

Proposition 41. Soit $N \in \mathbb{N}$.

(i) D_N est une fonction paire, 2π-périodique, et de norme 1.

(ii)

$$\forall x \in \mathbb{R} \setminus 2\pi\mathbb{Z},\ D_N(x) = \frac{\sin\left(\left(N + \frac{1}{2}\right)x\right)}{\sin\left(\frac{x}{2}\right)}$$

(iii) Pour tout $f \in L^{2\pi}_1$, $S_N(f) = f * D_N$.

Définition 42. Pour tout $N \in \mathbb{N}$, la fonction $K_N = \frac{1}{N}\sum_{j=0}^{N-1} D_j$ est appelé **noyau de Fejér** d'ordre N.

Notation 43. Pour tout $N \in \mathbb{N}^*$, on note $\sigma_N = \frac{1}{N}\sum_{k=0}^{N-1} S_n(f)$ la somme de Cesàro d'ordre N de la série de Fourier d'une fonction $f \in L_1^{2\pi}$.

Proposition 44. Soient $N \in \mathbb{N}^*$ et $f \in L_1^{2\pi}$.

(i) K_N est une fonction positive et de norme 1.

(ii)
$$\forall x \in \mathbb{R} \setminus 2\pi\mathbb{Z},\ K_N(x) = \frac{1}{N}\left(\frac{\sin\left(\frac{Nx}{2}\right)}{\sin\left(\frac{x}{2}\right)}\right)^2$$

(iii) $K_N = \sum_{n=-N}^{N}\left(1 - \frac{|n|}{N}\right)e_n$.

(iv) $\sigma_N(f) = f * K_N$.

[DEV]

Théorème 45 (Fejér)**.** Soit $f : \mathbb{R} \to \mathbb{C}$ une fonction 2π-périodique. p. 190

(i) Si f est continue, alors $\|\sigma_N(f)\|_\infty \leq \|f\|_\infty$ et $(\sigma_N(f))$ converge uniformément vers f.

(ii) Si $f \in L_p^{2\pi}$ pour $p \in [1, +\infty[$, alors $\|\sigma_N(f)\|_p \leq \|f\|_p$ et $(\sigma_N(f))$ converge vers f pour $\|.\|_p$.

Corollaire 46. L'espace des polynômes trigonométriques $\{\sum_{n=-N}^{N} c_n e_n \mid (c_n) \in \mathbb{C}^{\mathbb{N}}, N \in \mathbb{N}\}$ est dense dans l'espace des fonction continues 2π-périodiques pour $\|.\|_\infty$ et est dense dans $L_p^{2\pi}$ pour $\|.\|_p$ avec $p \in [1, +\infty[$.

213 Espaces de Hilbert. Exemples d'applications.

I - Généralités

1. Espaces préhilbertiens

[LI] p. 27

Définition 1. Soit H un espace vectoriel réel (resp. complexe). On appelle **produit scalaire** sur H une forme bilinéaire $\langle .,. \rangle$ telle que :

(i) $\forall y \in H$, $x \mapsto \langle x, y \rangle$ est une forme linéaire.

(ii) $\forall x \in H$, $\langle x, x \rangle \geq 0$ avec égalité si et seulement si $x = 0$.

(iii) $\forall x, y \in H$, $\langle x, y \rangle = \langle y, x \rangle$ (resp. $\langle x, y \rangle = \overline{\langle y, x \rangle}$).

Remarque 2. Dans le cas complexe, on a donc

$$\forall x, y \in H, \forall \lambda \in \mathbb{C}, \langle x, \lambda y \rangle = \overline{\lambda} \langle x, y \rangle$$

Définition 3. En reprenant les notations de la définition, si H est muni d'un produit scalaire, on dit que H est un espace **préhilbertien**.

Exemple 4. — $\mathbb{C}^n$ muni de

$$\langle .,. \rangle : ((x_i)_{i \in [\![1,n]\!]}, (y_i)_{i \in [\![1,n]\!]}) \mapsto \sum_{i=1}^{n} x_i \overline{y_i}$$

est un espace préhilbertien.

— Plus généralement, on peut définit d'autres produits scalaires sur $\mathbb{R}^n$ ou $\mathbb{C}^n$ en se donnant un poids $\omega = (\omega_1, \ldots, \omega_n)$ où $\forall i \in [\![1, n]\!]$, $\omega > 0$. Il suffit de munir l'espace produit du produit scalaire suivant :

$$\langle .,. \rangle_\omega : ((x_i)_{i \in [\![1,n]\!]}, (y_i)_{i \in [\![1,n]\!]}) \mapsto \sum_{i=1}^{n} \omega_i x_i \overline{y_i}$$

Dans toute la suite, on considérera un espace préhilbertien $(H, \langle .,. \rangle)$ sur le corps $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Notation 5. Puisque $\langle .,. \rangle \geq 0$, on peut poser

$$\|.\| = \sqrt{\langle .,. \rangle}$$

Proposition 6 (Identités de polarisation)**.** Soient $x, y \in H$.

(i) $\|x + y\|^2 = \|x\|^2 + 2\langle x, y \rangle + \|y\|^2$ (si $\mathbb{K} = \mathbb{R}$).

(ii) $\|x+y\|^2 = \|x\|^2 + 2\,\mathrm{Re}(\langle x,y\rangle) + \|y\|^2$ (si $\mathbb{K}=\mathbb{C}$).

Théorème 7 (Inégalité de Cauchy-Schwarz)**.**

$$\forall x,y \in H,\ |\langle x,y\rangle| \leq \|x\|\|y\|$$

avec égalité si et seulement si x et y sont colinéaires.

Corollaire 8. $\|.\|$ définit une norme sur H, ce qui fait de $(H,\|.\|)$ un espace vectoriel normé.

Proposition 9 (Identité du parallélogramme)**.** p. 62

$$\forall x,y \in H,\ \|x+y\|^2 + \|x-y\|^2 = 2(\|x\|^2\|y\|^2)$$

et cette identité caractérise les normes issues d'un produit scalaire.

2. Orthogonalité

Définition 10. On dit que deux vecteurs x et y de H sont orthogonaux si p. 31

$$\langle x,y\rangle = 0$$

et on le note $x \perp y$.

Exemple 11. Dans $\mathbb{R}^2$ muni de son produit scalaire usuel, on a $(-1,1) \perp (1,1)$.

Remarque 12 (Théorème de Pythagore). Si $\mathbb{K}=\mathbb{R}$, par la Théorème 6,

$$\forall x,y \in H,\ x \perp y \iff \|x+y\|^2 = \|x\|^2 + \|y\|^2$$

Définition 13. L'orthogonal d'une partie $A \subseteq H$ est l'ensemble

$$A^\perp = \{y \in H \mid \forall x \in A,\ x \perp y\}$$

Proposition 14. Soit $A \subseteq H$. **[BMP]** p. 99

(i) $A^\perp$ est un sous-espace vectoriel fermé de H.

(ii) $A^\perp = (\mathrm{Vect}(A))^\perp$.

(iii) $A^\perp = (\overline{A})^\perp$.

3. Espaces de Hilbert

Définition 15. Si $(H, \|.\|)$ est complet, on dit que H est un **espace de Hilbert**. p. 91

On suppose dans la suite que $(H, \|.\|)$ est un espace de Hilbert.

Exemple 16. — Tout espace euclidien ou hermitien est un espace de Hilbert.

— L'ensemble des suites de nombres complexes de carré sommables

$$\ell_2(\mathbb{N}) = \{(x_n) \in \mathbb{C}^2 \mid \sum_{n=0}^{+\infty} |x_n|^2 < +\infty\}$$

muni du produit scalaire hermitien

$$\langle .,. \rangle : ((x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}}) \mapsto \sum_{n=0}^{+\infty} x_n \overline{y_n}$$

est un espace de Hilbert.

II - Le théorème de projection sur un convexe fermé et ses conséquences

1. Théorème de projection

[DEV]

Théorème 17 (Projection sur un convexe fermé)**.** Soit $C \subseteq H$ un convexe fermé non-vide. Alors : [LI] p. 32

$$\forall x \in H, \exists! y \in C \text{ tel que } d(x,C) = \inf_{z\in C} \|x - z\| = d(x,y)$$

On peut donc noter $y = P_C(x)$, le **projeté orthogonal de** x **sur** C. Il s'agit de l'unique point de C vérifiant

$$\forall z \in C, \langle x - P_C(x), z - P_C(x) \rangle \leq 0 \qquad (*)$$

Remarque 18. En dimension finie, dans un espace euclidien ou hermitien, on peut projeter sur tous les fermés. On perd cependant l'unicité et la caractérisation angulaire. [BMP] p. 96

Proposition 19. Soit $C \subseteq H$ un convexe fermé non-vide. L'application P_C est lipschitzienne de rapport 1 et est, en particulier, continue.

2. Décomposition en somme directe orthogonale

Théorème 20 (Projection sur un sous-espace fermé)**.** Soit F un sous-espace vectoriel fermé de H.

(i) Si $x \in H$, le projeté $P_F(x)$ de x sur F est l'unique élément $p \in H$ qui vérifie

$$p \in F \text{ et } x - p \in F^\perp$$

(ii) $P_F : H \to F$ est linéaire, continue, surjective.

(iii) $H = F \oplus F^\perp$ et P_F est le projecteur sur F associé à cette décomposition.

(iv) Soient $x, x_1, x_2 \in H$. On a :

$$x = x_1 + x_2 \text{ avec } x_1 \in F, x_2 \in F^\perp \iff x_1 = P_F(x) \text{ et } x_2 = P_{F^\perp}(x)$$

Contre-exemple 21. On considère le sous-espace vectoriel de $\ell_2(\mathbb{N})$ constitué des suites nulles à partir d'un certain rang. Alors $F^\perp = \{0\}$, et ainsi $H \neq F \oplus F^\perp$.

Corollaire 22. Soit F un sous-espace vectoriel de H. Alors,

$$F^{\perp\perp} = \overline{F}$$

Corollaire 23. Soit F un sous-espace vectoriel de H. Alors,

$$\overline{F} = H \iff F^\perp = 0$$

3. Dualité dans un espace de Hilbert

Théorème 24 (de représentation de Riesz)**.** L'application

$$\Phi : \begin{array}{ccc} H & \to & H' \\ y & \mapsto & (x \mapsto \langle x, y \rangle) \end{array}$$

est une isométrie linéaire bijective de H sur son dual topologique H'.

Remarque 25. Cela signifie que :

$$\forall \varphi \in H', \exists! y \in H, \text{ tel que } \forall x \in H, \varphi(x) = \langle x, y \rangle$$

et de plus, $|||\varphi||| = \|y\|$.

Application 26 (Existence de l'adjoint)**.** Soit $u \in \mathscr{L}(H)$. Il existe un unique $v \in \mathscr{L}(H)$ tel que :

$$\forall x, y \in H, \langle u(x), y\rangle = \langle x, v(y)\rangle$$

On dit que v est **l'adjoint** de u et on note généralement $v = u^*$.

[DEV]

Application 27 (Dual de L_p)**.** Soit $(X, \mathscr{A}, \mu)$ un espace mesuré de mesure finie. On note $\forall p \in]1,2[$, $L_p = L_p(X, \mathscr{A}, \mu)$. L'application

$$\varphi : \begin{array}{ll} L_q & \to (L_p)' \\ g & \mapsto \left(\varphi_g : f \mapsto \int_X fg \,\mathrm{d}\mu\right) \end{array} \qquad \text{où } \frac{1}{p} + \frac{1}{q} = 1$$

est une isométrie linéaire surjective. C'est donc un isomorphisme isométrique.

[Z-Q] p. 222

III - Bases hilbertiennes

Définition 28. On dit qu'une famille $(e_i)_{i\in I}$ d'éléments de H est **orthonormée** de H si :

$$\forall i, j \in I, \langle e_i, e_j\rangle = \delta_{i,j}$$

[LI] p. 41

Exemple 29. Dans $\ell_2(\mathbb{N})$, la famille $(u_n)_{n\in\mathbb{N}}$ définie par

$$\forall n \in \mathbb{N},\ u_n = (0, \dots, 0, \underbrace{1}_{n\text{-ième position}}, 0 \dots)$$

est orthonormée.

Proposition 30. Toute famille orthonormée est libre.

Proposition 31 (Inégalité de Bessel)**.** Soient $x \in H$ et $(e_i)_{i\in I}$ une famille orthonormée de H. Alors,

$$\sum_{i\in I} |\langle x, e_i\rangle| \leq \|x\|$$

Définition 32. On dit qu'une famille $(e_i)_{i\in I}$ d'éléments de H est une **base** de H si elle est orthonormée et totale (ie. $\mathrm{Vect}(e_i)_{i\in I}$ est dense dans H).

Théorème 33. (i) Tout espace de Hilbert admet une base hilbertienne.

(ii) Tout espace de Hilbert séparable (ie. admettant une partie dénombrable dense) admet une base hilbertienne dénombrable.

[BMP] p. 108

Exemple 34. $\mathbb{K}^n$ est séparable pour tout entier n et L_p aussi pour tout $p \in [1,+\infty[$. On a donc existence d'une base hilbertienne dénombrable pour ces espaces.

Théorème 35. Soit H un espace de Hilbert séparable et $(e_n)_{n\in I}$ une famille orthonormée dénombrable de H. Les propriétés suivantes sont équivalentes :

(i) La famille orthonormée $(e_n)_{n\in I}$ est une base hilbertienne de H.

(ii) $\forall x \in H,\ x = \sum_{n=0}^{+\infty} \langle x, e_n\rangle e_n$.

(iii) $\forall x \in H,\ \|x\|_2 = \sum_{n=0}^{+\infty} |\langle x, e_n\rangle|^2$.

(iv) L'application

$$\Delta : \begin{array}{ccc} H & \to & \ell_2(\mathbb{N}) \\ x & \mapsto & (\langle x, e_n\rangle)_{n\in\mathbb{N}} \end{array}$$

est une isométrie linéaire bijective.

Remarque 36. L'égalité du Théorème 35 Point (iii) est appelée **égalité de Parseval**.

Corollaire 37. Tous les espaces de Hilbert séparables sont isométriquement isomorphes à $\ell_2(\mathbb{N})$.

[LI] p. 45

IV - L'espace L_2

1. Aspect hilbertien

Soit $(X, \mathscr{A}, \mu)$ un espace mesuré.

[BMP] p. 92

Notation 38. On note $L_p = L_p(X, \mathscr{A}, \mu)$ pour tout $p \in [1,+\infty]$.

Définition 39. On considère la forme bilinéaire suivante sur L_2 :

$$\langle .,. \rangle : (f,g) \mapsto \int_X f\overline{g}\,\mathrm{d}\mu$$

C'est un produit scalaire hermitien, ce qui confère à $(L_2, \langle .,. \rangle)$ une structure d'espace préhilbertien.

Remarque 40. La norme associée au produit scalaire précédent est la norme $\|.\|_2$ de L_2.

Théorème 41 (Riesz-Fischer)**.** Pour tout $p \in [1,+\infty]$, L_p est complet pour la norme $\|.\|_p$.

[LI] p. 10

p. 31

Corollaire 42. L_2 est un espace de Hilbert.

2. Polynômes orthogonaux

Soit I un intervalle de $\mathbb{R}$. On pose $\forall n \in \mathbb{N}$, $g_n : x \mapsto x^n$.

[BMP] p. 110

Définition 43. On appelle **fonction poids** une fonction $\rho : I \to \mathbb{R}$ mesurable, positive et telle que $\forall n \in \mathbb{N}, \rho g_n \in L_1(I)$.

Soit $\rho : I \to \mathbb{R}$ une fonction poids.

Notation 44. On note $L_2(I,\rho)$ l'espace des fonctions de carré intégrable pour la mesure de densité ρ par rapport à la mesure de Lebesgue.

Proposition 45. Muni de

$$\langle .,. \rangle : (f,g) \mapsto \int_I f(x)\overline{g(x)}\rho(x)\,\mathrm{d}x$$

$L_2(I,\rho)$ est un espace de Hilbert.

Théorème 46. Il existe une unique famille (P_n) de polynômes unitaires orthogonaux deux-à-deux telle que $\deg(P_n) = n$ pour tout entier n. C'est la famille de **polynômes orthogonaux** associée à ρ sur I.

Exemple 47 (Polynômes de Hermite)**.** Si $\forall x \in I$, $\rho(x) = e^{-x^2}$, alors

$$\forall n \in \mathbb{N},\ \forall x \in I,\ P_n(x) = \frac{(-1)^n}{2^n} e^{x^2} \frac{\partial}{\partial x^n}\left(e^{-x^2}\right)$$

Lemme 48. On suppose que $\forall n \in \mathbb{N}$, $g_n \in L_1(I,\rho)$ et on considère (P_n) la famille des polynômes orthogonaux associée à ρ sur I. Alors $\forall n \in \mathbb{N}$, $g_n \in L_2(I,\rho)$. En particulier, l'algorithme de Gram-Schmidt a bien du sens et (P_n) est bien définie.

p. 140

Application 49. On considère (P_n) la famille des polynômes orthogonaux associée à ρ sur I et on suppose qu'il existe $a > 0$ tel que

$$\int_I e^{a|x|}\rho(x)\,\mathrm{d}x < +\infty$$

alors (P_n) est une base hilbertienne de $L_2(I,\rho)$ pour la norme $\|.\|_2$.

Contre-exemple 50. On considère, sur $I = \mathbb{R}_*^+$, la fonction poids $\rho : x \mapsto x^{-\ln(x)}$. Alors, la famille des g_n n'est pas totale. La famille des polynômes orthogonaux associée à ce poids particulier n'est donc pas totale non plus : ce n'est pas une base hilbertienne.

3. Séries de Fourier

Notation 51. — Pour tout $p \in [1, +\infty]$, on note $L_p^{2\pi}$ l'espace des fonctions $f : \mathbb{R} \to \mathbb{C}$, 2π-périodiques et mesurables, telles que $\|f\|_p < +\infty$.

— Pour tout $n \in \mathbb{Z}$, on note e_n la fonction 2π-périodique définie pour tout $t \in \mathbb{R}$ par $e_n(t) = e^{int}$.

[Z-Q] p. 73

Proposition 52. $L_2^{2\pi}$ est un espace de Hilbert pour le produit scalaire

$$\langle .,. \rangle : (f,g) \mapsto \frac{1}{2\pi} \int_0^{2\pi} f(t)\overline{g(t)}\,\mathrm{d}t$$

Théorème 53. La famille $(e_n)_{n\in\mathbb{Z}}$ est une base hilbertienne de $L_2^{2\pi}$.

[BMP] p. 123

Corollaire 54.

$$\forall f \in L_2^{2\pi}, f = \sum_{n=-\infty}^{+\infty} \langle f, e_n \rangle e_n$$

Exemple 55. On considère $f : x \mapsto 1 - \frac{x^2}{\pi^2}$ sur $[-\pi, \pi]$. Alors,

$$\frac{\pi^4}{90} = \|f\|_2 = \sum_{n=0}^{+\infty} \frac{1}{n^4}$$

[GOU20] p. 272

Remarque 56. L'égalité du Théorème 54 est valable dans $L_2^{2\pi}$, elle signifie donc que

$$\left\| \sum_{n=-N}^{N} \langle f, e_n \rangle e_n - f \right\|_2 \longrightarrow_{N\to+\infty} 0$$

[BMP] p. 124

Annexes

[LI] p. 32

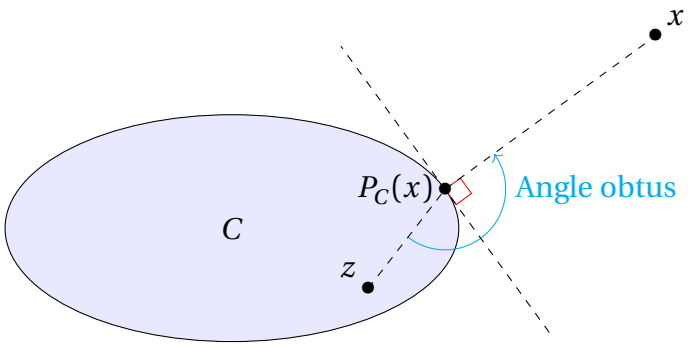


FIGURE I.20 – Illustration du théorème de projection sur un convexe fermé.

214 Théorème d'inversion locale, théorème des fonctions implicites. Illustrations en analyse et en géométrie.

Soient E et F deux espaces de Banach et $U \subseteq E$ un ouvert.

I - Théorème d'inversion locale

1. Difféomorphisme

Pour une fonction réelle $f : \mathbb{R} \to \mathbb{R}$ de classe $\mathscr{C}^1$, on sait que si $f'(x) \neq 0$ pour tout $x \in \mathbb{R}$, alors f admet un inverse global f^{-1} qui vérifie [GOU20] p. 341

$$\forall x \in \mathbb{R},\ f'(f(x)) = \frac{1}{f'(x)}$$

L'objectif ici va être de généraliser ce résultat.

Définition 1. Soit $f : U \to F$. On dit que f est un **difféomorphisme** de classe $\mathscr{C}^k$ de U sur $V = f(U)$ si f et f^{-1} sont bijectives et de classe $\mathscr{C}^k$ respectivement sur U et V. [ROU] p. 54

Proposition 2. On se place dans le cas où $E = \mathbb{R}^n$ et $F = \mathbb{R}^p$. Soit $f : U \to F$ un difféomorphisme. Alors :

(i) Pour tout $x \in U$, en posant $y = f(x)$,

$$\mathrm{d}(f^{-1})_y \circ \mathrm{d}f_x = \mathrm{id}$$

(ii) $n = p$.

Exemple 3. $x \mapsto x^3$ est un homéomorphisme de $\mathbb{R}$ sur $\mathbb{R}$, de classe $\mathscr{C}^1$, mais n'est pas un difféomorphisme.

2. Énoncé

Théorème 4 (Inversion locale)**.** Soit $f : U \to F$ de classe $\mathscr{C}^1$. On suppose qu'il existe $a \in U$ tel que $\mathrm{d}f_a$ est inversible. [GOU20] p. 341

Alors, il existe V voisinage de a et W voisinage de $f(a)$ tels que $f_{|V}$ soit un difféomorphisme de classe $\mathscr{C}^1$ de V sur W.

Remarque 5. Si $E = F = \mathbb{R}^n$, $\mathrm{d}f_a$ est inversible si et seulement si le jacobien de f en a, $\det \mathrm{Jac}(f)_a$, est non nul.

Corollaire 6. Soit $f : U \to \mathbb{R}^q$ de classe $\mathscr{C}^1$. On suppose que pour tout $a \in U$, $\mathrm{d}f_a$ est inversible. Alors f est une application ouverte.

Exemple 7. L'application de $\mathbb{R}^2$ dans $\mathbb{R}^2$ définie par $(x,y) \mapsto (x^2 - y^2, xy)$ est un difféomorphisme de classe $\mathscr{C}^\infty$ en tout point de $\mathbb{R}^2 \setminus (0,0)$.

p. 347

Application 8. Soit $\varphi : U \to \mathbb{R}^n$ un difféomorphisme de classe $\mathscr{C}^1$. Alors, $V = \varphi(U)$ est mesurable et tout fonction f appartient à L_1 si et seulement si $|\det \mathrm{Jac}(\varphi)_a| f \circ \varphi$ appartient à L_1. Dans ce cas,

$$\int_V f(x)\,\mathrm{d}x = \int_U |\det \mathrm{Jac}(\varphi)_a| f(\varphi(y))\,\mathrm{d}y$$

[BMP] p. 9

Exemple 9. En passant en coordonnées polaires,

$$\int_{\mathbb{R}} e^{-x^2}\,\mathrm{d}x = \sqrt{\pi}$$

[GOU20] p. 355

Application 10. Soient $A \in \mathscr{M}_n(\mathbb{R})$ et k un entier. Alors, si A est suffisamment proche de l'identité I_n, A est une racine k-ième (ie. $\exists B \in \mathscr{M}_n(\mathbb{R})$ telle que $B^k = A$).

[BMP] p. 9

3. Généralisation

Théorème 11 (Inversion globale)**.** Soit $f : U \to F$ de classe $\mathscr{C}^1$. Alors, f est un difféomorphisme de classe $\mathscr{C}^1$ de U sur $V = f(U)$ si et seulement si f est injective sur U et $\mathrm{d}f_a$ est un isomorphisme pour tout $a \in U$.

p. 13

Exemple 12. L'application de l'Théorème 7 n'est pas un difféomorphisme global.

[GOU20] p. 347

Remarque 13. Il existe une version holomorphe de ce théorème :

Soient U un ouvert connexe de $\mathbb{C}$ et $f : U \to \mathbb{C}$ holomorphe sur U. On suppose f injective sur U. Alors, $V = f(U)$ est un ouvert (connexe) de $\mathbb{C}$ et f est un difféomorphisme holomorphe de classe $\mathscr{C}^1$ de U sur V.

Remarquons que seule l'injectivité de f suffit.

[ROU] p. 191

p. 231

Théorème 14 (du rang constant)**.** On se place dans le cas où $E = \mathbb{R}^n$ et $F = \mathbb{R}^p$. Soit $f : U \to \mathbb{R}^p$ de classe $\mathscr{C}^1$. On suppose que le rang de $\mathrm{d}f_x$ est constant égal à $r \leq n$ pour tout $x \in U$. Soit $a \in U$. Alors, il existe V voisinage de a, W voisinage de $f(a)$ et deux difféomorphismes $\phi : V \to V$ et $\psi : W \to W$ tels que

$$\phi \circ f \circ \psi = \pi_r$$

où π_r désigne la projection de $\mathbb{R}^n$ sur $\mathbb{R}^r$: $\pi_r : (x_1, \dots, x_n) \mapsto (x_1, \dots, x_{r-1}, x_r, 0, \dots, 0)$.

II - Théorème des fonctions implicites

1. Énoncé

Définition 15. Soient $E_1, \dots, E_n, F$ des espaces de Banach, $\Omega \subseteq E$ un ouvert où $E = E_1 \times \cdots \times E_n$ et $a = (a_1, \dots, a_n) \in E$. Soit $f : \Omega \to F$. Alors, pour tout $i \in [\![1, n]\!]$, $f_i : x \mapsto f(a_1, \dots, a_{i-1}, x, a_{i+1}, \dots, a_n)$ est définie sur un voisinage de a_i dans E_i. Si elle est différentiable en a_i, on dit que f admet une **différentielle partielle** d'indice i en a, et on note celle-ci $\partial_i f_a$.

[GOU20] p. 344

Remarque 16. En reprenant les notations précédentes :

— Si pour tout $i \in [\![1, n]\!]$, $E_i = \mathbb{R}$ et $F = E = \mathbb{R}^n$, alors $\partial_i f_a = h \frac{\partial f}{\partial x_i}(a)$.

— Si f est différentiable en a, alors pour tout $i \in [\![1, n]\!]$, $\partial_i f_a$ existe et

$$\forall h = (h_1, \dots, h_n) \in E, \mathrm{d}f_a(h) = \sum_{i=1}^{n} \partial_i f_a(h_i)$$

Théorème 17 (des fonctions implicites)**.** Soient E, F, G trois espaces de Banach. Soient $U \times V \subseteq E \times F$ où U et V sont des ouvertes. Soit $f : U \times V \to G$ de classe $\mathscr{C}^1$. On suppose qu'il existe $(a, b) \in U \times V$ tel que $f(a, b) = 0$ et $\partial_2 f_{(a,b)} : F \to G$ est un isomorphisme. Alors, il existe :

— Un voisinage ouvert U_0 de a dans U.

— Un voisinage ouvert W de $f(a, b)$.

— Un voisinage ouvert Ω de (a, b) dans $U \times V$.

— Une fonction $\varphi : U_0 \times W \to V$ de classe $\mathscr{C}^1$.

Vérifiant :

$$\forall x \in U_0, \forall z \in W, \exists! y \in V \text{ tel que } f(x, y) = z \text{ avec } (x, y) \in \Omega \text{ et } y = \varphi(x, z)$$

En particulier,

$$\forall (x, z) \in U_0 \times W, f(x, \varphi(x, z)) = z$$

Remarque 18. Avec les notations précédentes, si $E = F = \mathbb{R}$, on peut choisir n'importe quelle variable pour obtenir

$$y = \varphi(x) \text{ si } \frac{\partial f}{\partial y}(a,b) \neq 0 \text{ ou } x = \varphi(y) \text{ si } \frac{\partial f}{\partial y}(a,b) \neq 0$$

[BMP] p. 11

Remarque 19. La signification de ce théorème est que la surface définie implicitement par l'équation $f(x,y) = 0$ peut, au moins localement, être vue comme le graphe d'une fonction φ.

[ROU] p. 193

Proposition 20. Avec les notations précédentes, la différentielle de la fonction implicite φ est donnée par :

$$\mathrm{d}\varphi_x = -(\partial_2 f_{(x,\varphi(x))})^{-1} \circ (\partial_1 f_{(x,\varphi(x))})$$

2. Exemples

Exemple 21. Pour l'équation $x^2 + y^2 - 1 = 0$, on a $\partial_2 f_{(x,y)} = 2y$. On exclue les points où $y = 0$. En prenant $(0,1)$ et $(0,-1)$ pour points de départ, on a deux fonctions implicites qui correspondent aux demi-cercles supérieur et inférieur :

— $y = \varphi_1(x) = \sqrt{1-x^2}$.

— $y = \varphi_2(x) = -\sqrt{1-x^2}$.

De plus, en dérivant par rapport à x : $2x + 2yy' = 0$ et, $y' = \varphi_1'(x) = \frac{-x}{y}$.

Exemple 22 (Folium de Descartes)**.** Soit $C = \{(x,y) \in \mathbb{R}^2 \mid x^3 + y^3 - 3xy = 0\}$. En tout point $(a,b) \in \mathbb{R}^2 \setminus \{(0,0), (2^{\frac{2}{3}}, 2^{\frac{1}{3}})\}$, C peut être vu comme le graphe d'une fonction φ telle que

$$\varphi'(a) = \frac{a^2 - b}{a - b^2}$$

p. 237

Exemple 23. Soit $f : (x,y) \mapsto \sin(y) + xy^4 + x^2$. Alors, il existe U, V deux voisinages ouverts de 0 dans $\mathbb{R}$, $y = \varphi(x) \in V$ est l'unique solution de $f(x,y) = 0$. De plus, on a un développement limité de φ :

$$\varphi(x) = -x^2 - \frac{x^6}{6} - x^9 - \frac{x^{10}}{40} + o(x^{11})$$

[GOU20] p. 348

III - Applications

1. Homéomorphismes

Lemme 24. Soit $A_0 \in \mathcal{S}_n(\mathbb{R})$ inversible. Alors il existe un voisinage V de A_0 dans $\mathcal{S}_n(\mathbb{R})$ et une application $\psi : V \to \mathrm{GL}_n(\mathbb{R})$ de classe $\mathcal{C}^1$ telle que

$$\forall A \in V,\ A = {}^t\psi(A) A_0 \psi(A)$$

[ROU] p. 209

[DEV]

Lemme 25 (Morse)**.** Soit $f : U \to \mathbb{R}$ une fonction de classe $\mathcal{C}^3$ (où U désigne un ouvert de $\mathbb{R}^n$ contenant l'origine). On suppose :

- $\mathrm{d}f_0 = 0$.
- La matrice symétrique $\mathrm{Hess}(f)_0$ est inversible.
- La signature de $\mathrm{Hess}(f)_0$ est $(p, n-p)$.

Alors il existe un difféomorphisme $\phi = (\phi_1, \dots, \phi_n)$ de classe $\mathcal{C}^1$ entre deux voisinage de l'origine de $\mathbb{R}^n$ $V \subseteq U$ et W tel que $\varphi(0) = 0$ et

$$\forall x \in U,\ f(x) - f(0) = \sum_{k=1}^{p} \phi_k^2(x) - \sum_{k=p+1}^{n} \phi_k^2(x)$$

p. 354

Exemple 26. On considère $f : (x, y) \mapsto x^2 - y^2 + \frac{y^4}{4}$. La courbe d'équation

$$f(x, y) = 0$$

est (au changement près du nom des coordonnées) une projection de l'intersection d'un cylindre et d'une sphère tangents. On a

$$f = u^2 - v^2$$

avec $u : (x, y) \mapsto x$ et $v : (x, y) \mapsto y\sqrt{1 - \frac{y^2}{4}}$.

p. 334

Application 27. Soit S la surface d'équation $z = f(x, y)$ où f est de classe $\mathcal{C}^3$ au voisinage de l'origine. On suppose la forme quadratique $\mathrm{d}^2 f_0$ non dégénérée. Alors, en notant P le plan tangent à S en 0 :

(i) Si $\mathrm{d}^2 f_0$ est de signature $(2, 0)$, alors S est au-dessus de P au voisinage de 0.

(ii) Si $\mathrm{d}^2 f_0$ est de signature $(0, 2)$, alors S est en-dessous de P au voisinage de 0.

(iii) Si $\mathrm{d}^2 f_0$ est de signature $(1, 1)$, alors S traverse P selon une courbe admettant un point double en $(0, f(0))$.

p. 341

[BMP] p. 15

Application 28. Soit $f : \mathbb{R}^n \to \mathbb{R}$ de classe $\mathscr{C}^3$ telle que $\mathrm{d}f_0 = 0$ et $\mathrm{d}^2 f_0$ est définie positive. Alors 0 est un minimum local (strict) de f.

2. Optimisation

Théorème 29 (Extrema liés)**.** Soit U un ouvert de $\mathbb{R}^n$ et soient $f, g_1, \dots, g_r : U \to \mathbb{R}$ des fonctions de classe $\mathscr{C}^1$. On note $\Gamma = \{x \in U \mid g_1(x) = \cdots = g_r(x) = 0\}$. Si $f_{|\Gamma}$ admet un extremum relatif en $a \in \Gamma$ et si les formes linéaires $\mathrm{d}(g_1)_a, \dots, \mathrm{d}(g_r)_a$ sont linéairement indépendantes, alors il existe des uniques $\lambda_1, \dots, \lambda_r$ tels que

$$\mathrm{d}f_a = \lambda_1 \mathrm{d}(g_1)_a + \cdots + \lambda_r \mathrm{d}(g_r)_a$$

[GOU20] p. 337

Définition 30. Les $\lambda_1, \dots, \lambda_r$ du théorème précédent sont appelés appelés **multiplicateurs de Lagrange**.

Remarque 31. La relation finale du Théorème 29 équivaut à

$$\bigcap_{i=1}^{n} \mathrm{Ker}(\mathrm{d}(g_i)_a) \subseteq \mathrm{Ker}(\mathrm{d}f_a)$$

et elle exprime que $\mathrm{d}f_a$ est nulle sur l'espace tangent à Γ en a (ie. ∇f_a est orthogonal à l'espace tangent à Γ en a).

[BMP] p. 21

Contre-exemple 32. On pose $g : (x, y) \mapsto x^3 - y^2$ et on considère $f : (x, y) \mapsto x + y^2$. On cherche à minimiser f sous la contrainte $g(x, y) = 0$.

Alors, le minimum (global) de f sous cette contrainte est atteint en $(0, 0)$, la différentielle de g en $(0, 0)$ est nulle et la relation finale du Théorème 29 n'est pas vraie.

Application 33 (Théorème spectral)**.** Tout endomorphisme symétrique d'un espace euclidien se diagonalise dans une base orthonormée.

Application 34.

$$\mathrm{SO}_n(\mathbb{R}) = \left\{ M \in \mathscr{M}_n(\mathbb{R}) \mid \|M\|^2 = \inf_{P \in \mathrm{SL}_n(\mathbb{R})} \|P\|^2 \right\}$$

où $\|.\| : M \mapsto \sqrt{\mathrm{trace}({}^t MM)}$ (ie. $\mathrm{SO}_n(\mathbb{R})$ est l'ensemble des matrices de $\mathrm{SL}_n(\mathbb{R})$ qui minimisent la norme euclidienne canonique de $\mathscr{M}_n(\mathbb{R})$).

p. 35

[GOU20] p. 339

Application 35 (Inégalité arithmético-géométrique)**.**

$$\forall (x_1,\dots,x_n)\in(\mathbb{R}^+)^n,\ \left(\prod_{i=1}^n x_i\right)^{\frac{1}{n}} \leq \frac{1}{n}\sum_{i=1}^n x_i$$

Application 36 (Inégalité d'Hadamard)**.** [ROU] p. 409

$$\forall (x_1,\dots,x_n)\in\mathbb{R}^n,\ \det(x_1,\dots,x_n)\leq \|x_1\|\dots\|x_n\|$$

avec égalité si et seulement si $(x_1,\dots,x_n)$ est une base orthogonale de $\mathbb{R}^n$.

3. Régularité des racines d'un polynôme

Proposition 37. Soient $P_0\in\mathbb{R}_n[X]$ et $x_0\in\mathbb{R}$ une racine simple de P_0. Alors, il existe φ une application $\mathscr{C}^\infty$ définie sur un voisinage U de P_0 dans $\mathbb{R}_n[X]$ à valeurs dans un voisinage V de x_0 telle que [BMP] p. 11

$$\forall P\in U,\forall x\in V,\ x=\varphi(P)\iff P(x)=0$$

Application 38. Soit $\mathscr{S}_{rs}$ l'ensemble des polynômes de $\mathbb{R}_n[X]$ scindés à racines simples. Alors, $\mathscr{S}_{rs}$ est un ouvert de $\mathbb{R}_n[X]$.

4. Surjectivité de l'exponentielle matricielle

Lemme 39. [I-P] p. 396

(i) Soit $A\in\mathscr{M}_n(\mathbb{C})$. Alors $\exp(A)\in \mathrm{GL}_n(\mathbb{C})$.

(ii) exp est différentiable en 0 et $\mathrm{d}\exp_0=\mathrm{id}_{\mathscr{M}_n(\mathbb{C})}$.

(iii) Soit $M\in\mathrm{GL}_n(\mathbb{C})$. Alors $M^{-1}\in\mathbb{C}[M]$.

[DEV]

Théorème 40. $\exp:\mathscr{M}_n(\mathbb{C})\to\mathrm{GL}_n(\mathbb{C})$ est surjective.

Application 41. $\exp(\mathscr{M}_n(\mathbb{R}))=\mathrm{GL}_n(\mathbb{R})^2$, où $\mathrm{GL}_n(\mathbb{R})^2$ désigne les carrés de $\mathrm{GL}_n(\mathbb{R})$.

Annexes

[BMP]
p. 10

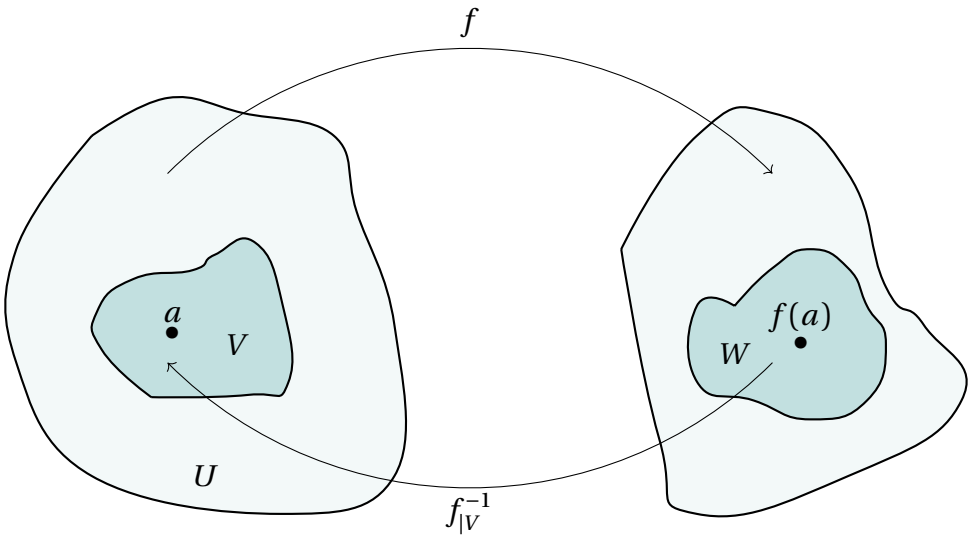


FIGURE I.21 – Inversion locale.

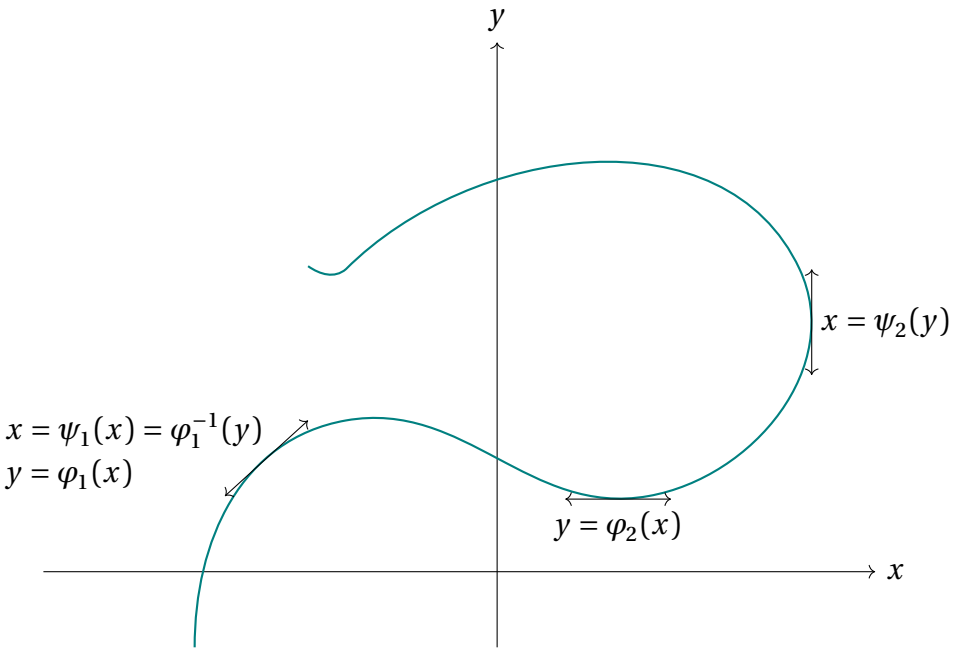


FIGURE I.22 – Fonctions implicites.

215 Applications différentiables définies sur un ouvert de $\mathbb{R}^n$. Exemples et applications.

Sauf mention contraire, nous travaillerons sur l'espace vectoriel normé $\mathbb{R}^n$ pour $n \geq 1$. Soient F un espace vectoriel normé sur $\mathbb{R}$ et $U \subseteq \mathbb{R}^n$ un ouvert.

I - Généralisation de la notion de dérivée

1. Différentielle

[GOU20] p. 323

Définition 1. Soit $(E, \|.\|)$ un espace vectoriel normé sur $\mathbb{R}$. Soient $U \subseteq E$ ouvert et $f : U \to F$ une application de U dans F. f est dite **différentiable** en un point a de U s'il existe $\ell_a \in \mathscr{L}(E,F)$ telle que

$$f(a+h) = f(a) + \ell_a(h) + o(\|h\|) \text{ quand } h \longrightarrow 0$$

Si ℓ_a existe, alors elle est unique et on la note $\mathrm{d}f_a$: c'est la **différentielle** de f en a.

Remarque 2.
- En dimension quelconque $\mathrm{d}f_a$ dépend a priori des normes choisies sur E et F. Cependant, en dimension finie, l'équivalence des normes implique que l'existence et la valeur de $\mathrm{d}f_a$ ne dépend pas des normes choisies.
- La définition demande à ℓ_a d'être continue. En dimension finie, le problème ne se pose donc pas.
- Une fonction réelle est différentiable en a si et seulement si elle est dérivable en a. Dans ce cas, on a $\mathrm{d}f_a : h \mapsto f'(a)h$.

Exemple 3. Si f est linéaire et continue, alors $\mathrm{d}f_a = f$ pour tout $a \in E$.

Proposition 4. Une fonction différentiable en un point et continue en ce point.

Proposition 5. Soit $V \subseteq F$ un ouvert. Soit $f : U \to F$ différentiable en un point a de U.

(i) $\forall \lambda \in \mathbb{R}$, λf est différentiable en a, et $\mathrm{d}(\lambda f)_a = \lambda \mathrm{d}f_a$.

(ii) Si $g : U \to F$ est différentiable en a, alors $f+g$ l'est aussi, et $\mathrm{d}(f+g)_a = \mathrm{d}f_a + \mathrm{d}g_a$.

(iii) Soit $g : V \to G$. On suppose $f(U) \subseteq V$ et g différentiable en $f(a)$. Alors $g \circ f$ est différentiable en a et, $\mathrm{d}(f \circ g)_a = \mathrm{d}g_{f(a)} \circ \mathrm{d}f_a$.

2. Dérivée selon un vecteur

Définition 6. Soit $a \in U$. p. 324

— Soit $v \in \mathbb{R}^n$. Si la fonction de la variable réelle $\varphi : t \mapsto f(a+tv)$ est dérivable en 0, on dit que f est **dérivable en a selon le vecteur v**. On note alors

$$f'_v(a) = \varphi'(0)$$

— Soit $(e_1, \dots, e_n)$ la base canonique de $\mathbb{R}^n$ et soit $i \in [\![1, n]\!]$. On dit que f admet une **i-ième dérivée partielle en a** si f est dérivable en a selon le vecteur e_i. On note alors

$$\frac{\partial f}{\partial x_i}(a) = f'_{e_i}(a)$$

Remarque 7. Soient $i \in [\![1, n]\!]$ et $a = (a_1, \dots, a_n) \in \mathbb{R}^n$. La dérivée partielle $\frac{\partial f}{\partial x_i}(a)$ est aussi la dérivée de l'application partielle $t \mapsto f(a_1, \dots, a_{i-1}, a_i + t, a_{i+1}, \dots, a_n)$ en $t = 0$.

Proposition 8. Une fonction différentiable en un point est dérivable selon tout vecteur en ce point.

Contre-exemple 9. La fonction p. 329

$$\begin{array}{ccc} \mathbb{R}^2 & \to & \mathbb{R} \\ (x,y) & \mapsto & \begin{cases} \frac{y^2}{x} & \text{si } x \neq 0 \\ y & \text{sinon} \end{cases} \end{array}$$

est dérivable selon tout vecteur au point $(0,0)$ mais n'est pas continue en $(0,0)$.

Théorème 10. Si toutes les dérivées partielles de f existent et si elles sont continues en un point a de U, alors f est différentiable en a et on a p. 325

$$\mathrm{d}f_a = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(a) e_i^*$$

où $(e_i^*)_{i \in [\![1,n]\!]}$ est la base duale de la base canonique $(e_i)_{i \in [\![1,n]\!]}$ de $\mathbb{R}^n$.

Contre-exemple 11. La fonction

$$f : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ (x,y) & \mapsto & \begin{cases} x^2 \sin\left(\frac{1}{x}\right) & \text{si } x \neq 0 \\ 0 & \text{sinon} \end{cases} \end{array}$$

est différentiable en 0, mais f' n'est pas continue en 0.

Corollaire 12. Soit $f : U \to \mathbb{R}^m$ différentiable en un point $a \in \mathbb{R}^n$. On note par f_i la i-ième coordonnée de f $\forall i \in [\![1,m]\!]$. Alors la matrice de l'application linéaire $\mathrm{d}f_a$ dans les bases canoniques de $\mathbb{R}^n$ et $\mathbb{R}^m$ est

$$\mathrm{Jac}(f)_a = \left(\frac{\partial f_i}{\partial x_j}\right)_{\substack{i\in[\![1,m]\!] \\ j\in[\![1,n]\!]}}$$

p. 327

Définition 13. Soit $f : U \to \mathbb{R}^m$ différentiable en un point $a \in \mathbb{R}^n$. La matrice $\mathrm{Jac}(f)_a$ est la **jacobienne** de f en a. Son déterminant est le **jacobien** de f en a.

Exemple 14. Soit $f : (r,\theta) \mapsto (r\cos(\theta), r\sin(\theta))$, alors $\det(\mathrm{Jac}(f)_{(r,\theta)}) = r$.

p. 354

Théorème 15 (Inégalité des accroissements finis)**.** Soit $f : U \to F$ continue sur un segment $[a,b] \subseteq U$ et différentiable sur $]a,b[$. On suppose qu'il existe $M > 0$ tel que $|||\mathrm{d}f_c||| \leq M$ pour tout $c \in]a,b[$. Alors,

$$\|f(b) - f(a)\| \leq M\|b-a\| \qquad (*)$$

p. 327

Corollaire 16. En reprenant les notations du théorème précédent :

(i) Si U est convexe, si f est différentiable sur U et si $|||\mathrm{d}f_c||| \leq M$ pour tout $c \in U$, alors l'inégalité $(*)$ précédente est vraie pour tout $a, b \in U$.

(ii) Si U est un ouvert connexe et $\mathrm{d}f_c = 0$ pour tout $c \in U$, alors f est constante.

3. Différentielle itérée

Définition 17. Soit $f : U \to F$. Sous réserve d'existence, on peut définir par récurrence sur p une dérivée partielle d'ordre p par la relation

$$\frac{\partial^p}{\partial x_{i_p} \dots \partial x_{i_1}} f = \frac{\partial}{\partial x_{i_p}} \left(\frac{\partial^{p-1}}{\partial x_{i_{p-1}} \dots \partial x_{i_1}} f \right)$$

f est alors dite de classe $\mathscr{C}^p$ si toutes ses dérivées partielles jusqu'à l'ordre p existent et sont

continues sur U.

Exemple 18. La fonction

$$x \mapsto \begin{cases} e^{-\frac{1}{x}} \text{ si } x > 0 \\ 0 \text{ sinon} \end{cases}$$

est $\mathscr{C}^\infty$.

p. 79

Théorème 19 (Schwarz)**.** On se place dans la cas $n = 2$. Soit $f : U \to \mathbb{R}$ qui admet des dérivées partielles sur U, continues en $a \in U$. Alors :

$$\frac{\partial^2 f}{\partial x \partial y}(a) = \frac{\partial^2 f}{\partial y \partial x}(a)$$

p. 326

Corollaire 20. Soit $f : U \to \mathbb{R}^m$ de classe $\mathscr{C}^p$. Alors les dérivées partielles jusqu'à l'ordre p ne dépendant pas de l'ordre de dérivation.

Notation 21. Soient $f : U \to \mathbb{R}^m$ de classe $\mathscr{C}^k$ sur U et $n \in [\![1, k]\!]$. Par analogie avec

$$\forall (a_1, \dots, a_m) \in \mathbb{R}^m, (a_1 + \cdots + a_m)^n = \sum_{i_1 + \cdots + i_m = n} \frac{n!}{i_1! \dots i_m!} a_1^{i_1} \dots a_m^{i_m}$$

on note

$$\left(\sum_{i=1}^m h_i \frac{\partial f}{\partial x_i}(a) \right)^{(n)} = \sum_{i_1 + \cdots + i_m = n} \frac{n!}{i_1! \dots i_m!} h_1^{i_1} \dots h_m^{i_m} \frac{\partial^n}{\partial x_1^{i_1} \dots \partial x_m^{i_m}} f(a)$$

Théorème 22 (Formule de Taylor-Lagrange)**.** Soient $f : U \to \mathbb{R}$ de classe $\mathscr{C}^p$ sur U, $x \in \mathbb{R}^n$, $h = (h_1, \dots, h_n) \in \mathbb{R}^n$ tels que $[x, x + h] \subseteq U$. Alors, $\exists \theta \in]0, 1[$ tel que

$$f(x + h) = \sum_{j=0}^{p-1} \frac{1}{i!} \left(\sum_{i=1}^n h_i \frac{\partial f}{\partial x_i}(x) \right)^{(j)} + \frac{1}{p!} \left(\sum_{i=1}^n h_i \frac{\partial f}{\partial x_i}(x + \theta h) \right)^{(p)}$$

Exemple 23. Pour $f : \mathbb{R}^2 \to \mathbb{R}$ de classe $\mathscr{C}^2$, pour $(h, k) \in \mathbb{R}^2$, il existe $\theta \in]0, 1[$ tel que

$$\begin{aligned} f(h,k) = f(0,0) &+ h \frac{\partial f}{\partial x}(0,0) + k \frac{\partial f}{\partial y}(0,0) \\ &+ \frac{1}{2} \left(h^2 \frac{\partial^2 f}{\partial^2 x} f(\theta h, \theta k) + hk \frac{\partial^2 f}{\partial x \partial y} f(\theta h, \theta k) + k^2 \frac{\partial^2 f}{\partial^2 y} f(\theta h, \theta k) \right) \\ &+ o(\|(h,k)\|^2) \end{aligned}$$

Théorème 24 (Formule de Taylor avec reste intégral)**.** Soient $f : U \to \mathbb{R}^p$ de classe $\mathscr{C}^k$ sur U, $x \in \mathbb{R}^n$, $h = (h_1, \dots, h_n) \in \mathbb{R}^n$ tels que $[x, x+h] \subseteq U$. Alors,

$$f(x+h) = \sum_{j=0}^{k-1} \frac{1}{i!} \left(\sum_{i=1}^{n} h_i \frac{\partial f}{\partial x_i}(x) \right)^{(j)} + \int_0^1 \frac{(1-t)^{k-1}}{(k-1)!} \left(\sum_{i=1}^{n} h_i \frac{\partial f}{\partial x_i}(x+th) \right)^{(k)} \mathrm{d}t$$

Théorème 25 (Formule de Taylor-Young)**.** Soient $f : U \to \mathbb{R}^p$ de classe $\mathscr{C}^k$ sur U, $x \in \mathbb{R}^n$, $h = (h_1, \dots, h_n) \in \mathbb{R}^n$ tels que $[x, x+h] \subseteq U$. Alors,

$$f(x+h) = \sum_{j=0}^{k} \frac{1}{i!} \left(\sum_{i=1}^{n} h_i \frac{\partial f}{\partial x_i}(x) \right)^{(j)} + o(\|h\|^k)$$

Application 26 (Lemme d'Hadamard)**.** Soit $f : \mathbb{R}^n \to \mathbb{R}$ de classe $\mathscr{C}^\infty$. On suppose f différentiable en 0 avec $\mathrm{d}f_0 = 0$ et $f(0) = 0$. Alors,

$$f(x_1, \dots, x_n) = \sum_{i,j=1}^{n} x_i x_j h_{i,j}(x_1, \dots, x_n)$$

où $\forall i, j \in [\![1, n]\!]$, $h_{i,j} : \mathbb{R}^n \to \mathbb{R}$ est $\mathscr{C}^\infty$.

II - Théorèmes fondamentaux

1. Inversion locale

Définition 27. Soit $f : U \to F$. On dit que f est un **difféomorphisme** de classe $\mathscr{C}^k$ de U sur $V = f(U)$ si f et f^{-1} sont bijectives et de classe $\mathscr{C}^k$ respectivement sur U et V.

[ROU] p. 54

Exemple 28. $x \mapsto x^3$ est un homéomorphisme de $\mathbb{R}$ sur $\mathbb{R}$, de classe $\mathscr{C}^1$, mais n'est pas un difféomorphisme.

Théorème 29 (Inversion locale)**.** Soit $f : U \to F$ de classe $\mathscr{C}^1$. On suppose qu'il existe $a \in U$ tel que $\mathrm{d}f_a$ est inversible.

Alors, il existe V voisinage de a et W voisinage de $f(a)$ tels que $f_{|V}$ soit un difféomorphisme de classe $\mathscr{C}^1$ de V sur W.

[GOU20] p. 341

Remarque 30. Si $F = \mathbb{R}^n$, $\mathrm{d}f_a$ est inversible si et seulement si le jacobien de f en a, $\det \mathrm{Jac}(f)_a$, est non nul.

Corollaire 31. Soit $f : U \to \mathbb{R}^q$ de classe $\mathscr{C}^1$. On suppose que pour tout $a \in U$, $\mathrm{d}f_a$ est inversible. Alors f est une application ouverte.

Exemple 32. L'application de $\mathbb{R}^2$ dans $\mathbb{R}^2$ définie par $(x,y) \mapsto (x^2-y^2, xy)$ est un difféomorphisme de classe $\mathscr{C}^\infty$ en tout point de $\mathbb{R}^2 \setminus (0,0)$. p. 347

Application 33. Soit $\varphi : U \to \mathbb{R}^n$ un difféomorphisme de classe $\mathscr{C}^1$. Alors, $V = \varphi(U)$ est mesurable et tout fonction f appartient à L_1 si et seulement si $|\det \mathrm{Jac}(\varphi)_a| f \circ \varphi$ appartient à L_1. Dans ce cas,

$$\int_V f(x)\,\mathrm{d}x = \int_U |\det \mathrm{Jac}(\varphi)_a| f(\varphi(y))\,\mathrm{d}y$$

[BMP] p. 9

Exemple 34. En passant en coordonnées polaires,

$$\int_{\mathbb{R}} e^{-x^2}\,\mathrm{d}x = \sqrt{\pi}$$

[GOU20] p. 355

Application 35. Soient $A \in \mathscr{M}_n(\mathbb{R})$ et k un entier. Alors, si A est suffisamment proche de l'identité I_n, A est une racine k-ième (ie. $\exists B \in \mathscr{M}_n(\mathbb{R})$ telle que $B^k = A$).

[BMP] p. 9

Lemme 36. (i) Soit $A \in \mathscr{M}_n(\mathbb{C})$. Alors $\exp(A) \in \mathrm{GL}_n(\mathbb{C})$.

(ii) exp est différentiable en 0 et $\mathrm{d}\exp_0 = \mathrm{id}_{\mathscr{M}_n(\mathbb{C})}$.

(iii) Soit $M \in \mathrm{GL}_n(\mathbb{C})$. Alors $M^{-1} \in \mathbb{C}[M]$.

[I-P] p. 396

[DEV] **Théorème 37.** $\exp : \mathscr{M}_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$ est surjective.

Application 38. $\exp(\mathscr{M}_n(\mathbb{R})) = \mathrm{GL}_n(\mathbb{R})^2$, où $\mathrm{GL}_n(\mathbb{R})^2$ désigne les carrés de $\mathrm{GL}_n(\mathbb{R})$.

2. Fonctions implicites

Définition 39. Soient $E_1, \dots, E_n, F$ des espaces de Banach, $\Omega \subseteq E$ un ouvert où $E = E_1 \times \cdots \times E_n$ et $a = (a_1, \dots, a_n) \in E$. Soit $f : \Omega \to F$. Alors, pour tout $i \in [\![1, n]\!]$, $f_i : x \mapsto f(a_1, \dots, a_{i-1}, x, a_{i+1}, \dots, a_n)$ est définie sur un voisinage de a_i dans E_i. Si elle est différentiable en a_i, on dit que f admet une **différentielle partielle** d'indice i en a, et on note celle-ci $\partial_i f_a$.

[GOU20] p. 344

Remarque 40. En reprenant les notations précédentes :

— Si pour tout $i \in [\![1,n]\!]$, $E_i = \mathbb{R}$ et $F = E = \mathbb{R}^n$, alors $\partial_i f_a = h\frac{\partial f}{\partial x_i}(a)$.

— Si f est différentiable en a, alors pour tout $i \in [\![1,n]\!]$, $\partial_i f_a$ existe et

$$\forall h = (h_1, \dots, h_n) \in E,\ \mathrm{d}f_a(h) = \sum_{i=1}^{n} \partial_i f_a(h_i)$$

Théorème 41 (des fonctions implicites)**.** Soient $U \times V \subseteq \mathbb{R}^n \times \mathbb{R}^m$ où U et V sont des ouvertes. Soit $f : U \times V \to F$ de classe $\mathscr{C}^1$. On suppose qu'il existe $(a,b) \in U \times V$ tel que $f(a,b) = 0$ et $\partial_2 f_{(a,b)} : \mathbb{R}^m \to F$ est un isomorphisme. Alors, il existe :

— Un voisinage ouvert U_0 de a dans U.

— Un voisinage ouvert W de $f(a,b)$.

— Un voisinage ouvert Ω de (a,b) dans $U \times V$.

— Une fonction $\varphi : U_0 \times W \to V$ de classe $\mathscr{C}^1$.

Vérifiant :

$$\forall x \in U_0,\ \forall z \in W,\ \exists! y \in V \text{ tel que } f(x,y) = z \text{ avec } (x,y) \in \Omega \text{ et } y = \varphi(x,z)$$

En particulier,

$$\forall (x,z) \in U_0 \times W,\ f(x, \varphi(x,z)) = z$$

Remarque 42. Avec les notations précédentes, si $E = F = \mathbb{R}$, on peut choisir n'importe quelle variable pour obtenir

$$y = \varphi(x) \text{ si } \frac{\partial f}{\partial y}(a,b) \neq 0 \text{ ou } x = \varphi(y) \text{ si } \frac{\partial f}{\partial y}(a,b) \neq 0$$

[BMP] p. 11

Remarque 43. La signification de ce théorème est que la surface définie implicitement par l'équation $f(x,y) = 0$ peut, au moins localement, être vue comme le graphe d'une fonction φ.

[ROU] p. 193

Proposition 44. Avec les notations précédentes, la différentielle de la fonction implicite φ est donnée par :

$$\mathrm{d}\varphi_x = -(\partial_2 f_{(x,\varphi(x))})^{-1} \circ (\partial_1 f_{(x,\varphi(x))})$$

Exemple 45. Pour l'équation $x^2 + y^2 - 1 = 0$, on a $\partial_2 f_{(x,y)} = 2y$. On exclue les points où $y = 0$. En prenant $(0,1)$ et $(0,-1)$ pour points de départ, on a deux fonctions implicites qui correspondent aux demi-cercles supérieur et inférieur :

— $y = \varphi_1(x) = \sqrt{1-x^2}$.

— $y = \varphi_2(x) = -\sqrt{1-x^2}$.

De plus, en dérivant par rapport à x : $2x + 2yy' = 0$ et, $y' = \varphi_1'(x) = \frac{-x}{y}$.

III - Application aux fonctions à valeurs dans $\mathbb{R}$

1. Gradient, hessienne

Soit $f : U \to \mathbb{R}$ une application différentiable en un point a de U.

[GOU20] p. 324

Définition 46. $\mathrm{d}f_a$ est une forme linéaire, et le théorème de représentation de Riesz donne l'existence d'un unique vecteur v de $\mathbb{R}^n$ tel que

$$\forall h \in \mathbb{R}^n,\ \mathrm{d}f_a(h) = \langle v, h\rangle$$

Le vecteur v s'appelle **gradient** de f, et est noté ∇f_a.

Proposition 47. $\frac{\partial f}{\partial x_i}$ existe pour tout $i \in [\![1, n]\!]$ et,

$$\nabla f_a = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(a) e_i$$

où $(e_1, \dots, e_n)$ est la base canonique de $\mathbb{R}^n$.

On suppose pour la suite f de classe $\mathscr{C}^2$.

p. 336

Définition 48. La matrice **hessienne** de f en a, notée $\mathrm{Hess}(f)_a$, est définie par

$$\mathrm{Hess}(f)_a = \left(\frac{\partial^2 f}{\partial x_i \partial x_j}\right)_{i,j \in [\![1,n]\!]}$$

Remarque 49. Pour f de classe $\mathscr{C}^2$, $\mathrm{Hess}(f)_a$ est symétrique.

Théorème 50. On suppose $\mathrm{d}f_a = 0$ (a est un **point critique** de f). Alors :

(i) Si f admet un minimum (resp. maximum) relatif en a, $\mathrm{Hess}(f)_a$ est positive (resp. négative).

(ii) Si $\mathrm{Hess}(f)_a$ définit une forme quadratique définie positive (resp. définie négative), f admet un minimum (resp. maximum) relatif en a.

Exemple 51. On suppose $\mathrm{d}f_a = 0$. On pose $(r,s,t) = \left(\frac{\partial^2}{\partial x_i \partial x_j} f\right)_{i+j=2}$. Alors :

(i) Si $rt - s^2 > 0$ et $r > 0$ (resp. $r < 0$), f admet une minimum (resp. maximum) relatif en a.

(ii) Si $rt - s^2 < 0$, f n'a pas d'extremum en a.

(iii) Si $rt - s^2 = 0$, on ne peut rien conclure.

Exemple 52. La fonction $(x,y) \mapsto x^4 + y^2 - 2(x-y)^2$ a trois points critiques qui sont des minimum locaux : $(0,0)$, $(\sqrt{2}, -\sqrt{2})$ et $(-\sqrt{2}, \sqrt{2})$.

Contre-exemple 53. $x \mapsto x^3$ a sa hessienne positive en 0, mais n'a pas d'extremum en 0.

2. Homéomorphismes

Lemme 54. Soit $A_0 \in \mathcal{S}_n(\mathbb{R})$ inversible. Alors il existe un voisinage V de A_0 dans $\mathcal{S}_n(\mathbb{R})$ et une application $\psi : V \to \mathrm{GL}_n(\mathbb{R})$ de classe $\mathcal{C}^1$ telle que

$$\forall A \in V,\ A = {}^t\psi(A) A_0 \psi(A)$$

[ROU] p. 209

[DEV]

Lemme 55 (Morse)**.** Soit $f : U \to \mathbb{R}$ une fonction de classe $\mathcal{C}^3$ (où U désigne un ouvert de $\mathbb{R}^n$ contenant l'origine). On suppose :

— $\mathrm{d}f_0 = 0$.

— La matrice symétrique $\mathrm{H}(f)_0$ est inversible.

— La signature de $\mathrm{H}(f)_0$ est $(p, n-p)$.

Alors il existe un difféomorphisme $\phi = (\phi_1, \dots, \phi_n)$ de classe $\mathcal{C}^1$ entre deux voisinage de l'origine de $\mathbb{R}^n$ $V \subseteq U$ et W tel que $\varphi(0) = 0$ et

$$\forall x \in U,\ f(x) - f(0) = \sum_{k=1}^{p} \phi_k^2(x) - \sum_{k=p+1}^{n} \phi_k^2(x)$$

p. 354

Exemple 56. On considère $f : (x,y) \mapsto x^2 - y^2 + \frac{y^4}{4}$. La courbe d'équation

$$f(x,y) = 0$$

est (au changement près du nom des coordonnées) une projection de l'intersection d'un cylindre et d'une sphère tangents. On a

$$f = u^2 - v^2$$

p. 334

avec $u : (x,y) \mapsto x$ et $v : (x,y) \mapsto y\sqrt{1-\frac{y^2}{4}}$.

3. Optimisation

Théorème 57 (Extrema liés)**.** Soit U un ouvert de $\mathbb{R}^n$ et soient $f, g_1, \dots, g_r : U \to \mathbb{R}$ des fonctions de classe $\mathscr{C}^1$. On note $\Gamma = \{x \in U \mid g_1(x) = \cdots = g_r(x) = 0\}$. Si $f_{|\Gamma}$ admet un extremum relatif en $a \in \Gamma$ et si les formes linéaires $\mathrm{d}(g_1)_a, \dots, \mathrm{d}(g_r)_a$ sont linéairement indépendantes, alors il existe des uniques $\lambda_1, \dots, \lambda_r$ tels que

$$\mathrm{d}f_a = \lambda_1 \mathrm{d}(g_1)_a + \cdots + \lambda_r \mathrm{d}(g_r)_a$$

[GOU20] p. 337

Définition 58. Les $\lambda_1, \dots, \lambda_r$ du théorème précédent sont appelés appelés **multiplicateurs de Lagrange**.

Remarque 59. La relation finale du Théorème 57 équivaut à

$$\bigcap_{i=1}^{n} \mathrm{Ker}(\mathrm{d}(g_i)_a) \subseteq \mathrm{Ker}(\mathrm{d}f_a)$$

et elle exprime que $\mathrm{d}f_a$ est nulle sur l'espace tangent à Γ en a (ie. ∇f_a est orthogonal à l'espace tangent à Γ en a).

[BMP] p. 21

Contre-exemple 60. On pose $g : (x,y) \mapsto x^3 - y^2$ et on considère $f : (x,y) \mapsto x + y^2$. On cherche à minimiser f sous la contrainte $g(x,y) = 0$.

Alors, le minimum (global) de f sous cette contrainte est atteint en $(0,0)$, la différentielle de g en $(0,0)$ est nulle et la relation finale du Théorème 57 n'est pas vraie.

Application 61 (Théorème spectral)**.** Tout endomorphisme symétrique d'un espace euclidien se diagonalise dans une base orthonormée.

Application 62.

$$\mathrm{SO}_n(\mathbb{R}) = \left\{ M \in \mathscr{M}_n(\mathbb{R}) \mid \|M\|^2 = \inf_{P \in \mathrm{SL}_n(\mathbb{R})} \|P\|^2 \right\}$$

où $\|.\| : M \mapsto \sqrt{\mathrm{trace}({}^tMM)}$ (ie. $\mathrm{SO}_n(\mathbb{R})$ est l'ensemble des matrices de $\mathrm{SL}_n(\mathbb{R})$ qui minimisent la norme euclidienne canonique de $\mathscr{M}_n(\mathbb{R})$).

p. 35

[GOU20] p. 339

Application 63 (Inégalité arithmético-géométrique)**.**

$$\forall (x_1,\dots,x_n)\in(\mathbb{R}^+)^n,\ \left(\prod_{i=1}^n x_i\right)^{\frac{1}{n}} \leq \frac{1}{n}\sum_{i=1}^n x_i$$

Application 64 (Inégalité d'Hadamard)**.**

[ROU] p. 409

$$\forall (x_1,\dots,x_n)\in\mathbb{R}^n,\ \det(x_1,\dots,x_n)\leq \|x_1\|\dots\|x_n\|$$

avec égalité si et seulement si $(x_1,\dots,x_n)$ est une base orthogonale de $\mathbb{R}^n$.

Annexes

[BMP]
p. 10

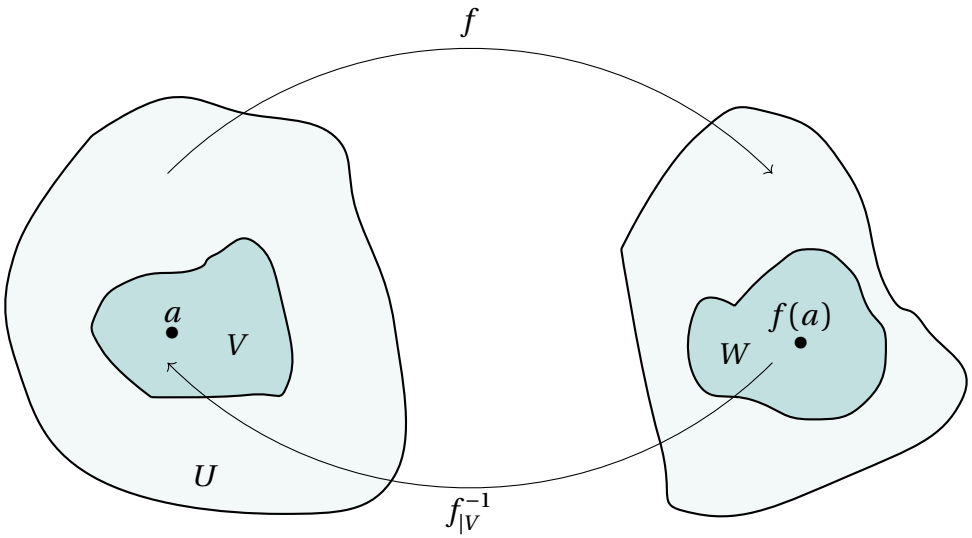


FIGURE I.23 – Inversion locale.

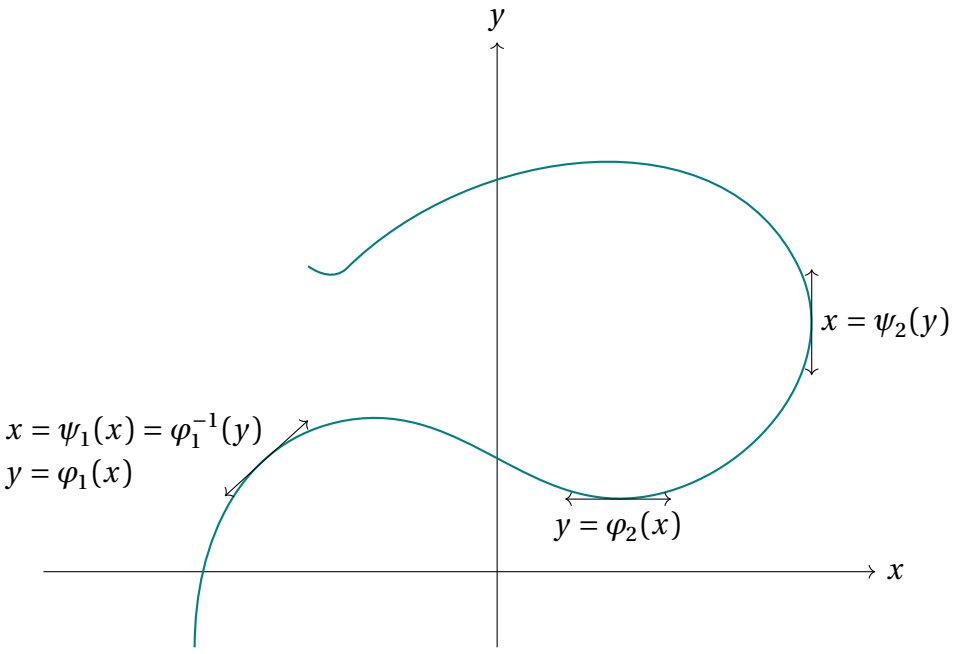


FIGURE I.24 – Fonctions implicites.

218 Formules de Taylor. Exemples et applications.

I - Énoncés des formules de Taylor

1. En dimension 1

Dans cette partie, I désigne un segment $[a,b]$ de $\mathbb{R}$ non réduit à un point et E un espace de Banach sur $\mathbb{R}$. Soit $f : I \to E$ une application.Dans un premier temps, supposons $E = \mathbb{R}$. [GOU20] p. 73

Théorème 1 (Rolle)**.** On suppose f continue sur $[a,b]$, dérivable sur $]a,b[$ et telle que $f(a) = f(b)$. Alors,

$$\exists c \in]a,b[\text{ tel que } f'(c) = 0$$

Théorème 2 (Formule de Taylor-Lagrange)**.** On suppose f de classe $\mathscr{C}^n$ sur $[a,b]$ telle que $f^{(n+1)}$ existe sur $]a,b[$. Alors,

$$\exists c \in]a,b[\text{ tel que } f(b) = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(b-a)^k + \frac{f^{(n+1)}(c)}{(n+1)!}(b-a)^{n+1}$$

Application 3.
- $\forall x \in \mathbb{R}^+, x - \frac{x^2}{2} \leq \ln(1+x) \leq x - \frac{x^2}{2} + \frac{x^3}{3}$.
- $\forall x \in \mathbb{R}^+, x - \frac{x^3}{6} \leq \sin(x) \leq x - \frac{x^3}{6} + \frac{x^5}{120}$.
- $\forall x \in \mathbb{R}, 1 - \frac{x^2}{2} \leq \cos(x) \leq 1 - \frac{x^2}{2} + \frac{x^4}{24}$.

On ne suppose plus $E = \mathbb{R}$. Le Théorème 1 n'est plus forcément vrai, mais on a tout de même le résultat suivant.

Théorème 4 (Inégalité des accroissements finis)**.** Soit $g : I \to \mathbb{R}$. On suppose f et g continues sur $[a,b]$ et dérivables sur $]a,b[$. Si pour tout $t \in]a,b[$ on a $\|f'(t)\| \leq g'(t)$. Alors,

$$\|f(b) - f(a)\| \leq (g(b) - g(a))$$

Corollaire 5 (Inégalité de Taylor-Lagrange)**.** On suppose f de classe $\mathscr{C}^n$ sur $[a,b]$ telle que $f^{(n+1)}$ existe sur $]a,b[$. On suppose qu'il existe $M > 0$ tel que $\forall t \in]a,b[$, $\|f^{(n+1)}(t)\| \leq M$. Alors,

$$\left\| f(b) - f(a) - \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(b-a)^k \right\| \leq M \frac{(b-a)^{n+1}}{(n+1)!}$$

Théorème 6 (Formule de Taylor-Young)**.** On suppose f de classe $\mathscr{C}^n$ sur I telle que $f^{(n+1)}(x)$

existe pour $x \in I$. Alors, quand $h \longrightarrow 0$, on a

$$f(x+h) = \sum_{k=0}^{n+1} \frac{f^{(k)}(x)}{k!} h^k + o(h^{n+1})$$

Application 7 (Théorème de Darboux)**.** On suppose f dérivable sur I. Alors $f'(I)$ est un intervalle.

p. 80

Théorème 8 (Formule de Taylor avec reste intégral)**.** On suppose f de classe $\mathscr{C}^{n+1}$ sur I. Alors,

$$f(b) = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(b-a)^k + \int_a^b \frac{(b-t)^n}{n!} f^{(n+1)}(t)\,\mathrm{d}t$$

p. 77

2. En dimension supérieure

Soit $U \subseteq \mathbb{R}^n$ un ouvert.

p. 328

Notation 9. Soient $f : U \to \mathbb{R}^m$ de classe $\mathscr{C}^k$ sur U et $n \in [\![1, k]\!]$. Par analogie avec

$$\forall (a_1, \dots, a_m) \in \mathbb{R}^m, (a_1 + \cdots + a_m)^n = \sum_{i_1 + \cdots + i_m = n} \frac{n!}{i_1! \dots i_m!} a_1^{i_1} \dots a_m^{i_m}$$

on note

$$\left(\sum_{i=1}^{m} h_i \frac{\partial f}{\partial x_i}(a)\right)^{(n)} = \sum_{i_1 + \cdots + i_m = n} \frac{n!}{i_1! \dots i_m!} h_1^{i_1} \dots h_m^{i_m} \frac{\partial^n}{\partial x_1^{i_1} \dots \partial x_m^{i_m}} f(a)$$

Théorème 10 (Formule de Taylor-Lagrange)**.** Soient $f : U \to \mathbb{R}$ de classe $\mathscr{C}^p$ sur U, $x \in \mathbb{R}^n$, $h = (h_1, \dots, h_n) \in \mathbb{R}^n$ tels que $[x, x+h] \subseteq U$. Alors, $\exists \theta \in]0,1[$ tel que

$$f(x+h) = \sum_{j=0}^{p-1} \frac{1}{i!} \left(\sum_{i=1}^{n} h_i \frac{\partial f}{\partial x_i}(x)\right)^{(j)} + \frac{1}{p!} \left(\sum_{i=1}^{n} h_i \frac{\partial f}{\partial x_i}(x+\theta h)\right)^{(p)}$$

Exemple 11. Pour $f : \mathbb{R}^2 \to \mathbb{R}$ de classe $\mathscr{C}^2$, pour $(h,k) \in \mathbb{R}^2$, il existe $\theta \in]0,1[$ tel que

$$\begin{aligned} f(h,k) = f(0,0) &+ h\frac{\partial f}{\partial x}(0,0) + k\frac{\partial f}{\partial y}(0,0) \\ &+ \frac{1}{2}\left(h^2 \frac{\partial^2 f}{\partial^2 x} f(\theta h, \theta k) + hk \frac{\partial^2 f}{\partial x \partial y} f(\theta h, \theta k) + k^2 \frac{\partial^2 f}{\partial^2 y} f(\theta h, \theta k)\right) \\ &+ o(\|(h,k)\|^2) \end{aligned}$$

Théorème 12 (Formule de Taylor avec reste intégral)**.** Soient $f : U \to \mathbb{R}^p$ de classe $\mathscr{C}^k$ sur U, $x \in \mathbb{R}^n$, $h = (h_1, \dots, h_n) \in \mathbb{R}^n$ tels que $[x, x+h] \subseteq U$. Alors,

$$f(x+h) = \sum_{j=0}^{k-1} \frac{1}{i!} \left(\sum_{i=1}^{n} h_i \frac{\partial f}{\partial x_i}(x) \right)^{(j)} + \int_0^1 \frac{(1-t)^{k-1}}{(k-1)!} \left(\sum_{i=1}^{n} h_i \frac{\partial f}{\partial x_i}(x+th) \right)^{(k)} \mathrm{d}t$$

Théorème 13 (Formule de Taylor-Young)**.** Soient $f : U \to \mathbb{R}^p$ de classe $\mathscr{C}^k$ sur U, $x \in \mathbb{R}^n$, $h = (h_1, \dots, h_n) \in \mathbb{R}^n$ tels que $[x, x+h] \subseteq U$. Alors,

$$f(x+h) = \sum_{j=0}^{k} \frac{1}{i!} \left(\sum_{i=1}^{n} h_i \frac{\partial f}{\partial x_i}(x) \right)^{(j)} + o(\|h\|^k)$$

Application 14 (Lemme d'Hadamard)**.** Soit $f : \mathbb{R}^n \to \mathbb{R}$ de classe $\mathscr{C}^\infty$. On suppose f différentiable en 0 avec $\mathrm{d}f_0 = 0$ et $f(0) = 0$. Alors,

$$f(x_1, \dots, x_n) = \sum_{i,j=1}^{n} x_i x_j h_{i,j}(x_1, \dots, x_n)$$

où $\forall i, j \in [\![1, n]\!]$, $h_{i,j} : \mathbb{R}^n \to \mathbb{R}$ est $\mathscr{C}^\infty$.

II - Applications en analyse réelle

Dans cette partie, I désigne un intervalle de $\mathbb{R}$ non réduit à un point et E un espace de Banach sur $\mathbb{R}$. Soit $f : I \to E$ une application.

1. Étude asymptotique de fonctions

On suppose $0 \in I$.

p. 89

Définition 15. On dit que f admet un **développement limité** à l'ordre $n \in \mathbb{N}^*$ s'il existe $a_0, \dots, a_n \in E$ tels que, au voisinage de 0,

$$f(x) = \sum_{k=0}^{n} a_k x^k + o(x^n)$$

Remarque 16. On pourrait de même définir les développements limités au voisinage d'un point $a \in \bar{I}$.

Proposition 17. (i) Un développement limité, s'il existe, est unique.

(ii) Si f admet un développement limité en 0 à l'ordre $n \geq 1$, f est dérivable en 0 et sa dérivée en 0 vaut a_1.

(iii) Si f est paire (resp. impaire), les coefficients du développement limité d'indice impair (resp. pair) sont nuls.

(iv) Si f est n fois dérivable en 0, f' admet un développement limité en 0 : $f'(x) = \sum_{k=1}^{n} a_k x^{k-1} + o(x^{n-1})$.

(v) Si f est dérivable sur I et f' admet un développement limité en 0 : $f'(x) = \sum_{k=0}^{n} a_k x^k + o(x^n)$; alors, f admet un développement limité en 0 donné par $f(x) = \sum_{k=0}^{n} \frac{a_k}{(k+1)!} x^{k+1} + o(x^{k+1})$.

(vi) Les règles de somme, produit, quotient et composition obéissent aux mêmes règles que pour les polynômes (sous réserve de bonne définition).

On déduit du Théorème 6 le résultat suivant.

Proposition 18. Si f est n fois dérivable en 0, alors f admet un développement limité à l'ordre n en 0 :

$$f(x) = \sum_{k=0}^{n+1} \frac{f^{(k)}(0)}{k!} x^k + o(x^{n+1})$$

Exemple 19. En 0, on a les développements limités usuels suivants.

— $e^x = \sum_{k=0}^{n} \frac{x^k}{k!} + o(x^n)$.

— $\sin(x) = \sum_{k=0}^{n} (-1)^k \frac{x^{2k+1}}{(2k+1)!} + o(x^{2n+2})$.

— $\cos(x) = \sum_{k=0}^{n} (-1)^k \frac{x^{2k}}{(2k)!} + o(x^{2n+1})$.

— $\sinh(x) = \sum_{k=0}^{n} \frac{x^{2k+1}}{(2k+1)!} + o(x^{2n+2})$.

— $\cosh(x) = \sum_{k=0}^{n} \frac{x^{2k}}{(2k)!} + o(x^{2n+1})$.

— Pour tout $\alpha \in \mathbb{R}$, $(1+x)^\alpha = \sum_{k=0}^{n} \frac{\alpha(\alpha-1)\ldots(\alpha-k+1)}{k!} + o(x^n)$.

Application 20.

$$\lim_{x \to 0} \frac{\tan(x) - x}{\sin(x) - x} = -2$$

Application 21 (Développement asymptotique de la série harmonique)**.** On note $\forall n \in \mathbb{N}^*$, $H_n = \sum_{k=1}^{n} \frac{1}{k}$. Alors, quand n tend vers $+\infty$,

$$H_n = \ln(n) + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + o\left(\frac{1}{n^2}\right)$$

[I-P] p. 380

2. Développements en série entière

Définition 22. Soient $U \subseteq \mathbb{C}$ un ouvert et $f : U \to \mathbb{C}$. On dit que f est **développable en série entière en** $a \in U$ s'il existe $r > 0$ et $(a_n) \in \mathbb{C}^{\mathbb{N}}$ tels que $D(a,r) \subseteq U$ et

$$\forall z \in D(a,r),\ f(z) = \sum_{n=0}^{+\infty} a_n (z-a)^n$$

[BMP] p. 46

Exemple 23. Soit $z_0 \in \mathbb{C}$. Alors,

$$\forall z \in D(0,|z_0|),\ \frac{1}{z-z_0} = -\frac{1}{z_0 \sum_{n=0}^{+\infty}} \left(\frac{z}{z_0}\right)^n$$

[GOU20] p. 251

Nous nous limiterons ici aux fonctions réelles.

Proposition 24. Soit $I \subseteq \mathbb{R}$ un intervalle contenant un voisinage de 0. Une fonction $f : I \to \mathbb{R}$ de classe $\mathscr{C}^\infty$ est développable en série entière si et seulement s'il existe $\alpha > 0$ tel que la suite de fonctions (R_n) définie par

$$R_n(x) = f(x) - \sum_{k=0}^{n} \frac{f^{(k)}(0)}{k!} x^k$$

tende simplement vers 0 sur $]-\alpha,\alpha[$. La série entière $\sum \frac{f^{(n)}(0)}{n!} z^n$ a alors un rayon de convergence supérieur ou égal à α et f est égale à la somme de cette série entière sur $]-\alpha,\alpha[$.

Remarque 25. Dans la pratique, pour montrer que le (R_n) précédent tend simplement vers 0, on peut l'exprimer comme un reste de Taylor (Lagrange ou intégral).

Exemple 26. On a les développements en série entière usuels suivants.

- Pour tout $x \in \mathbb{R}$, $e^x = \sum_{k=0}^{+\infty} \frac{x^k}{k!}$.
- Pour tout $x \in \mathbb{R}$, $\sin(x) = \sum_{k=0}^{+\infty} (-1)^k \frac{x^{2k+1}}{(2k+1)!}$.
- Pour tout $x \in \mathbb{R}$, $\cos(x) = \sum_{k=0}^{+\infty} (-1)^k \frac{x^{2k}}{(2k)!}$.
- Pour tout $x \in \mathbb{R}$, $\sinh(x) = \sum_{k=0}^{+\infty} \frac{x^{2k+1}}{(2k+1)!}$.
- Pour tout $x \in \mathbb{R}$, $\cosh(x) = \sum_{k=0}^{+\infty} \frac{x^{2k}}{(2k)!}$.
- Pour tout $\alpha \in \mathbb{R}$, Pour tout $x \in]-1,1[$, $(1+x)^\alpha = \sum_{k=0}^{+\infty} \frac{\alpha(\alpha-1)\ldots(\alpha-k+1)}{k!}$.

Contre-exemple 27. La fonction

$$f : x \mapsto \begin{cases} e^{-\frac{1}{x}} \text{ si } x > 0 \\ 0 \text{ sinon} \end{cases}$$

est $\mathscr{C}^\infty$, vérifie $f^{(n)}(0) = 0$ pour tout entier n, mais ne coïncide pas avec la somme de $\sum \frac{f^{(n)}(0)}{n!} z^n$ sur $]-\alpha, \alpha[$ pour tout $\alpha > 0$.

Contre-exemple 28. On considère fonction définie sur $\mathbb{R}^+$ par

$$g : x \mapsto \int_0^{+\infty} \frac{e^{-t}}{1+xt} \, \mathrm{d}t$$

Alors g est $\mathscr{C}^\infty$, vérifie $g^{(n)}(0) = 0$ pour tout entier n, et $\sum \frac{g^{(n)}(0)}{n!} z^n$ a un rayon de convergence nul.

Théorème 29 (Bernstein)**.** Soient $a > 0$ et $f :]-a, a[\to \mathbb{R}$ de classe $\mathscr{C}^\infty$. On suppose les dérivées de f positives sur $]-a, a[$. Alors f est développable en série entière sur $]-a, a[$.

[ROM18] p. 302

3. Méthode de Newton

[DEV]

Théorème 30 (Méthode de Newton)**.** Soit $f : [c, d] \to \mathbb{R}$ une fonction de classe $\mathscr{C}^2$ strictement croissante sur $[c, d]$. On considère la fonction

$$\varphi : \begin{array}{ccc} [c,d] & \to & \mathbb{R} \\ x & \mapsto & x - \frac{f(x)}{f'(x)} \end{array}$$

(qui est bien définie car $f' > 0$). Alors :

(i) $\exists! a \in [c, d]$ tel que $f(a) = 0$.

(ii) $\exists \alpha > 0$ tel que $I = [a - \alpha, a + \alpha]$ est stable par φ.

(iii) La suite (x_n) des itérés (définie par récurrence par $x_{n+1} = \varphi(x_n)$ pour tout $n \geq 0$) converge quadratiquement vers a pour tout $x_0 \in I$.

[ROU] p. 152

Corollaire 31. En reprenant les hypothèses et notations du théorème précédent, et en supposant de plus f strictement convexe sur $[c, d]$, le résultat du théorème est vrai sur $I = [a, d]$. De plus :

(i) (x_n) est strictement décroissante (ou constante).

(ii) $x_{n+1} - a \sim \frac{f''(a)}{2f'(a)} (x_n - a)^2$ pour $x_0 > a$.

Exemple 32. — On fixe $y > 0$. En itérant la fonction $F : x \mapsto \frac{1}{2}\left(x + \frac{y}{x}\right)$ pour un nombre de départ compris entre c et d où $0 < c < d$ et $c^2 < 0 < d^2$, on peut obtenir une approximation du nombre $\sqrt{y}$.

— En itérant la fonction $F : x \mapsto \frac{x^2+1}{2x-1}$ pour un nombre de départ supérieur à 2, on peut obtenir une approximation du nombre d'or $\varphi = \frac{1+\sqrt{5}}{2}$.

4. Majoration d'une erreur d'approximation

Soit f une fonction réelle continue sur un intervalle $[a,b]$. On se donne $n+1$ points $x_0, \dots, x_n \in [a,b]$ distincts deux-à-deux. **[DEM]** p. 21

Définition 33. Pour $i \in [\![0,n]\!]$, on définit le i-ième **polynôme de Lagrange** associé à $x_1, \dots, x_n$ par

$$\ell_i : x \mapsto \prod_{\substack{j=0 \\ j\neq i}}^{n} \frac{x - x_j}{x_i - x_j}$$

Théorème 34. Il existe une unique fonction polynômiale p_n de degré n telle que $\forall i \in [\![0,n]\!]$, $p_n(x_i) = f(x_i)$:

$$p_n = \sum_{i=0}^{n} f(x_i)\ell_i$$

Théorème 35. On note $\pi_{n+1} : x \mapsto \prod_{j=0}^{n}(x - x_j)$ et on suppose f $n+1$ fois dérivable $[a,b]$. Alors, pour tout $x \in [a,b]$, il existe un réel $\xi_x \in]\min(x,x_i), \max(x,x_i)[$ tel que

$$f(x) - p_n(x) = \frac{\pi_{n+1}(x)}{(n+1)!} f^{(n+1)}(\xi_x)$$

Corollaire 36.

$$\|f - p_n\|_\infty \leq \frac{1}{(n+1)!} \|\pi_{n+1}\|_\infty \|f^{(n+1)}\|_\infty$$

Application 37 (Calculs approchés d'intégrales)**.** On note $I(f) = \int_a^b f(t)\,\mathrm{d}t$. L'objectif est d'approximer $I(f)$ par une expression $P(f)$ et de majorer l'erreur d'approximation $E(f) = |I(f) - P(f)|$. **[DAN]** p. 506

(i) Méthode des rectangles. On suppose f continue. Avec $P(f) = (b-a)f(a)$, on a $E(f) \leq \frac{(b-a)^2}{2}\|f'\|_\infty$.

(ii) Méthode du point milieu. On suppose f de classe $\mathscr{C}^2$. Avec $P(f) = (b-a)f\left(\frac{a+b}{2}\right)$, on a $E(f) \leq \frac{(b-a)^3}{24}\|f''\|_\infty$.

(iii) Méthode des trapèzes. On suppose f de classe $\mathscr{C}^2$. Avec $P(f) = \frac{b-a}{2}(f(a) + f(b))$, on

a $E(f) \leq \frac{(b-a)^3}{12}\|f''\|_\infty$.

(iv) Méthode de Simpson. On suppose f de classe $\mathscr{C}^4$. Avec $P(f) = \frac{b-a}{6}\left(f(a)+f(b)+4f\left(\frac{a+b}{2}\right)\right)$, on a $E(f) \leq \frac{(b-a)^3}{2880}\|f^{(4)}\|_\infty$.

III - Application aux fonctions de plusieurs variables

Soit $U \subseteq \mathbb{R}^n$ un ouvert.

1. Homéomorphismes

Lemme 38. Soit $A_0 \in \mathscr{S}_n(\mathbb{R})$ inversible. Alors il existe un voisinage V de A_0 dans $\mathscr{S}_n(\mathbb{R})$ et une application $\psi : V \to \mathrm{GL}_n(\mathbb{R})$ de classe $\mathscr{C}^1$ telle que

$$\forall A \in V,\ A = {}^t\psi(A) A_0 \psi(A)$$

[ROU] p. 209

[DEV]

Lemme 39 (Morse)**.** Soit $f : U \to \mathbb{R}$ une fonction de classe $\mathscr{C}^3$ (où U désigne un ouvert de $\mathbb{R}^n$ contenant l'origine). On suppose :

— $\mathrm{d}f_0 = 0$.

— La matrice symétrique $\mathrm{H}(f)_0$ est inversible.

— La signature de $\mathrm{H}(f)_0$ est $(p, n-p)$.

Alors il existe un difféomorphisme $\phi = (\phi_1, \dots, \phi_n)$ de classe $\mathscr{C}^1$ entre deux voisinage de l'origine de $\mathbb{R}^n$ $V \subseteq U$ et W tel que $\varphi(0) = 0$ et

$$\forall x \in U,\ f(x) - f(0) = \sum_{k=1}^{p} \phi_k^2(x) - \sum_{k=p+1}^{n} \phi_k^2(x)$$

p. 354

Exemple 40. On considère $f : (x,y) \mapsto x^2 - y^2 + \frac{y^4}{4}$. La courbe d'équation

$$f(x,y) = 0$$

est (au changement près du nom des coordonnées) une projection de l'intersection d'un cylindre et d'une sphère tangents. On a

$$f = u^2 - v^2$$

avec $u : (x,y) \mapsto x$ et $v : (x,y) \mapsto y\sqrt{1 - \frac{y^2}{4}}$.

p. 334

2. Conditions d'extrema

Soit $f : U \to \mathbb{R}$ de classe $\mathscr{C}^2$ sur U.

Théorème 41. On suppose $\mathrm{d}f_a = 0$ (a est un **point critique** de f). Alors : [GOU20] p. 336

(i) Si f admet un minimum (resp. maximum) relatif en a, $\mathrm{Hess}(f)_a$ est positive (resp. négative).

(ii) Si $\mathrm{Hess}(f)_a$ définit une forme quadratique définie positive (resp. définie négative), f admet un minimum (resp. maximum) relatif en a.

Exemple 42. On suppose $\mathrm{d}f_a = 0$. On pose $(r,s,t) = \left(\frac{\partial^2}{\partial x_i \partial x_j} f\right)_{i+j=2}$. Alors :

(i) Si $rt - s^2 > 0$ et $r > 0$ (resp. $r < 0$), f admet une minimum (resp. maximum) relatif en a.

(ii) Si $rt - s^2 < 0$, f n'a pas d'extremum en a.

(iii) Si $rt - s^2 = 0$, on ne peut rien conclure.

Exemple 43. La fonction $(x,y) \mapsto x^4 + y^2 - 2(x-y)^2$ a trois points critiques qui sont des minimum locaux : $(0,0)$, $(\sqrt{2}, -\sqrt{2})$ et $(-\sqrt{2}, \sqrt{2})$.

Contre-exemple 44. $x \mapsto x^3$ a sa hessienne positive en 0, mais n'a pas d'extremum en 0.

IV - Application en probabilités

Théorème 45 (Lévy)**.** Soient (X_n) une suite de variables aléatoires réelles et X une variable aléatoire réelle. Alors : [Z-Q] p. 544

$$X_n \xrightarrow{(d)} X \iff \phi_{X_n} \text{ converge simplement vers } \phi_X$$

où ϕ_Y désigne la fonction caractéristique d'une variable aléatoire réelle Y.

Théorème 46 (Central limite)**.** Soit (X_n) une suite de variables aléatoires réelles indépendantes de même loi admettant un moment d'ordre 2. On note m l'espérance et σ^2 la variance commune à ces variables. On pose $S_n = X_1 + \cdots + X_n - nm$. Alors, [G-K] p. 307

$$\left(\frac{S_n}{\sqrt{n}}\right) \xrightarrow{(d)} \mathcal{N}(0, \sigma^2)$$

Application 47 (Théorème de Moivre-Laplace)**.** On suppose que (X_n) est une suite de variables aléatoires indépendantes de même loi $\mathscr{B}(p)$. Alors,

$$\frac{\sum_{k=1}^{n} X_k - np}{\sqrt{n}} \xrightarrow{(d)} \mathscr{N}(0, p(1-p))$$

Application 48 (Formule de Stirling)**.**

$$n! \sim \sqrt{2n\pi}\left(\frac{n}{e}\right)^n$$

p. 556

219 Extremums : existence, caractérisation, recherche. Exemples et applications.

I - Existence et unicité

Définition 1. Soient U un ouvert d'un espace vectoriel normé E et $f : U \to \mathbb{R}$. [R-R] p. 210

— On dit que f admet un **maximum local** (resp. **minimum local**) en $a \in U$ si

$$\exists r > 0 \text{ tel } \forall x \in B(a,r),\ f(x) \leq f(a) (\text{resp. } f(x) \geq f(a))$$

— On dit que f admet un **extremum local** en $a \in U$ si elle admet un minimum ou un maximum local.

1. Utilisation de la compacité

Théorème 2 (Des bornes)**.** Soient E un espace compact et $f : E \to \mathbb{R}$ continue. Alors, il existe deux éléments a et b de E vérifiant [GOU20] p. 31

$$f(a) = \inf_{x \in E} f(x) \text{ et } f(b) = \sup_{x \in E} f(x)$$

Contre-exemple 3. La fonction [HAU] p. 202

$$\begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \begin{cases} \frac{(-1)^q (q-1)}{q} & \text{si } x \in \mathbb{Q} \setminus \{0\} \text{ avec } \frac{p}{q} \text{ le représentant irréductible de } x \\ 0 & \text{sinon} \end{cases} \end{array}$$

est minorée par -1, majorée par 1, mais n'atteint ses bornes sur aucun intervalle d'intérieur non vide de $\mathbb{R}$.

Corollaire 4. Soient (E,d) un espace métrique et K_1, K_2 deux compacts de E. Alors, [GOU20] p. 33

$$\exists (x_1,x_2) \in K_1 \times K_2 \text{ tel que } d(x_1,x_2) = \inf_{(x,y) \in K_1 \times K_2} d(x,y)$$

Corollaire 5 (Point fixe dans un compact)**.** Soit (E,d) un espace métrique compact et $f : E \to E$ telle que [ROU] p. 171

$$\forall x, y \in E,\ x \neq y \implies d(f(x),f(y)) < d(x,y)$$

alors f admet un unique point fixe et pour tout $x_0 \in E$, la suite des itérés

$$x_{n+1} = f(x_n)$$

converge vers ce point fixe.

Exemple 6. sin admet un unique point fixe sur $[0,1]$.

Contre-exemple 7. La fonction

$$\begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \begin{cases} 1 & \text{si } x < 0 \\ x + \frac{1}{1+x} & \text{sinon} \end{cases} \end{array}$$

est continue, contractante et sans point fixe.

[GOU20] p. 35

Corollaire 8 (Théorème de Heine)**.** Une application continue sur un compact y est uniformément continue.

p. 31

Application 9 (Théorème de d'Alembert-Gauss)**.** Tout polynôme non constant de $\mathbb{C}$ admet une racine dans $\mathbb{C}$.

[DAN] p. 58

2. Utilisation de la convexité

Soit $I \subseteq \mathbb{R}$ un intervalle non réduit à un point.

Proposition 10. Une fonction $f : \mathbb{R} \to \mathbb{R}$ est constante si et seulement si elle est convexe et majorée.

[ROM19-1] p. 234

Contre-exemple 11. La fonction f définie sur $\mathbb{R}^+$ par $f(x) = \frac{1}{1+x}$ est convexe, majorée, mais non constante.

Proposition 12. Si $f : I \to \mathbb{R}$ est convexe et est dérivable en un point $\alpha \in \mathring{I}$ tel que $f'(\alpha) = 0$, alors f admet un minimum global en α.

Proposition 13. Si $f : I \to \mathbb{R}$ est convexe et admet un minimum local, alors ce minimum est global.

3. Utilisation de l'holomorphie

Soient Ω un ouvert connexe de $\mathbb{C}$ et $f : \Omega \to \mathbb{C}$.

[QUE] p. 102

Proposition 14 (Inégalités de Cauchy)**.** On suppose f holomorphe au voisinage du disque $\overline{D}(a,R)$. On note c_n les coefficients du développement en série entière de f en a. Alors,

$$\forall n \in \mathbb{N},\ \forall r \in [0,R],\ |c_n| \leq \frac{M(r)}{r^n}$$

où $M(r) = \sup_{|z-a|=r} |f(z)|$.

Corollaire 15 (Théorème de Liouville)**.** On suppose f holomorphe sur $\mathbb{C}$ tout entier. Si f est bornée, alors f est constante.

Théorème 16 (Principe du maximum)**.** On suppose Ω borné et f holomorphe dans Ω et continue dans $\overline{\Omega}$. On note M le sup de f sur la frontière (compacte) de Ω. Alors,

p. 107

$$\forall z \in \Omega,\ |f(z)| \leq M$$

4. Utilisation de propriétés hilbertiennes

Soit H un espace de Hilbert de norme $\|.\|$ et on note $\langle .,. \rangle$ le produit scalaire associé.

[LI] p. 32

Lemme 17 (Identité du parallélogramme)**.**

$$\forall x, y \in H,\ \|x+y\|^2 + \|x-y\|^2 = 2(\|x\|^2\|y\|^2)$$

et cette identité caractérise les normes issues d'un produit scalaire.

[DEV]

Théorème 18 (Projection sur un convexe fermé)**.** Soit $C \subseteq H$ un convexe fermé non-vide. Alors :

$$\forall x \in H, \exists! y \in C \text{ tel que } d(x,C) = \inf_{z \in C} \|x-z\| = d(x,y)$$

On peut donc noter $y = P_C(x)$, le **projeté orthogonal de** x **sur** C. Il s'agit de l'unique point de C vérifiant

$$\forall z \in C,\ \langle x - P_C(x), z - P_C(x) \rangle \leq 0$$

Théorème 19. Si F est un sous espace vectoriel fermé dans H, alors P_F est une application linéaire continue. De plus, pour tout $x \in H$, $P_F(x)$ est l'unique point $y \in F$ tel que $x - y \in F^\perp$.

Application 20. Soit F un sous-espace vectoriel de H. Alors,

$$\overline{F} = H \iff F^{\perp} = 0$$

Application 21 (Théorème de représentation de Riesz)**.**

$$\forall \varphi \in H', \exists! y \in H, \text{ tel que } \forall x \in H, \varphi(x) = \langle x, y \rangle$$

et de plus, $|||\varphi||| = \|y\|$.

Corollaire 22.

$$\forall T \in H', \exists! U \in H' \text{ tel que } \forall x, y \in H, \langle T(x), y \rangle = \langle x, U(y) \rangle$$

On note alors $U = T^*$: c'est **l'adjoint** de T. On a alors $|||T||| = |||T^*|||$.

Application 23. Soit $J : H \to \mathbb{R}$ une fonction convexe, continue et vérifiant

$$\forall (x_k) \in H^{\mathbb{N}} \text{ telle que } \|x_k\| \longrightarrow_{k \to +\infty} +\infty \text{ alors } J(x_k) \longrightarrow_{k \to +\infty} +\infty$$

Alors, il existe $a \in H$ tel que

$$J(a) = \inf_{h \in H} J(h)$$

[I-P] p. 336

II - Extrema et calcul différentiel

Soit $f : U \to \mathbb{R}$ différentiable en un point a de U, où U est un ouvert de $\mathbb{R}^n$.

1. Condition du premier ordre

Définition 24. Si $df_a = 0$, on dit que a est un **point critique** de f.

[R-R] p. 210

Remarque 25. Cela revient à dire que toutes les dérivées partielles de f s'annulent en a.

Proposition 26. Si f admet un extremum local en a, alors a est un point critique de f.

Contre-exemple 27. $(x, y) \mapsto x^2 - y^2$ a un point critique en $(0,0)$, mais n'a pas d'extremum en $(0,0)$.

[HAU] p. 281

2. Condition du second ordre

On suppose f de classe $\mathscr{C}^2$ sur U.

[GOU20] p. 336

Définition 28. La matrice **hessienne** de f en a, notée $\mathrm{Hess}(f)_a$, est définie par

$$\mathrm{Hess}(f)_a = \left(\frac{\partial^2 f}{\partial x_i \partial x_j}\right)_{i,j\in[\![1,n]\!]}$$

Remarque 29. Pour f de classe $\mathscr{C}^2$, $\mathrm{Hess}(f)_a$ est symétrique.

Théorème 30. On suppose $\mathrm{d}f_a = 0$. Alors :

(i) Si f admet un minimum (resp. maximum) relatif en a, $\mathrm{Hess}(f)_a$ est positive (resp. négative).

(ii) Si $\mathrm{Hess}(f)_a$ définit une forme quadratique définie positive (resp. définie négative), f admet un minimum (resp. maximum) relatif en a.

Exemple 31. On suppose $\mathrm{d}f_a = 0$. On pose $(r,s,t) = \left(\frac{\partial^2}{\partial x_i \partial x_j} f\right)_{i+j=2}$. Alors :

(i) Si $rt - s^2 > 0$ et $r > 0$ (resp. $r < 0$), f admet une minimum (resp. maximum) relatif en a.

(ii) Si $rt - s^2 < 0$, f n'a pas d'extremum en a.

(iii) Si $rt - s^2 = 0$, on ne peut rien conclure.

Exemple 32. La fonction $(x,y) \mapsto x^4 + y^2 - 2(x-y)^2$ a trois points critiques qui sont des minimum locaux : $(0,0)$, $(\sqrt{2}, -\sqrt{2})$ et $(-\sqrt{2}, \sqrt{2})$.

Contre-exemple 33. $x \mapsto x^3$ a sa hessienne positive en 0, mais n'a pas d'extremum en 0.

3. Extrema liés

p. 337

Théorème 34 (Extrema liés)**.** Soient $f, g_1, \dots, g_r : U \to \mathbb{R}$ des fonctions de classe $\mathscr{C}^1$. On note $\Gamma = \{x \in U \mid g_1(x) = \cdots = g_r(x) = 0\}$. Si $f_{|\Gamma}$ admet un extremum relatif en $a \in \Gamma$ et si les formes linéaires $\mathrm{d}(g_1)_a, \dots, \mathrm{d}(g_r)_a$ sont linéairement indépendantes, alors il existe des uniques $\lambda_1, \dots, \lambda_r$ tels que

$$\mathrm{d}f_a = \lambda_1 \mathrm{d}(g_1)_a + \cdots + \lambda_r \mathrm{d}(g_r)_a$$

Définition 35. Les $\lambda_1, \dots, \lambda_r$ du théorème précédent sont appelés appelés **multiplicateurs de Lagrange**.

Remarque 36. La relation finale du Théorème 34 équivaut à

$$\bigcap_{i=1}^{n} \mathrm{Ker}(\mathrm{d}(g_i)_a) \subseteq \mathrm{Ker}(\mathrm{d}f_a)$$

et elle exprime que $\mathrm{d}f_a$ est nulle sur l'espace tangent à Γ en a (ie. ∇f_a est orthogonal à l'espace tangent à Γ en a).

[BMP] p. 21

Contre-exemple 37. On pose $g : (x,y) \mapsto x^3 - y^2$ et on considère $f : (x,y) \mapsto x + y^2$. On cherche à minimiser f sous la contrainte $g(x,y) = 0$.

Alors, le minimum (global) de f sous cette contrainte est atteint en $(0,0)$, la différentielle de g en $(0,0)$ est nulle et la relation finale du Théorème 34 n'est pas vraie.

Application 38 (Théorème spectral)**.** Tout endomorphisme symétrique d'un espace euclidien se diagonalise dans une base orthonormée.

Application 39.

p. 35

$$\mathrm{SO}_n(\mathbb{R}) = \left\{ M \in \mathscr{M}_n(\mathbb{R}) \mid \|M\|^2 = \inf_{P \in \mathrm{SL}_n(\mathbb{R})} \|P\|^2 \right\}$$

où $\|.\| : M \mapsto \sqrt{\mathrm{trace}({}^tMM)}$ (ie. $\mathrm{SO}_n(\mathbb{R})$ est l'ensemble des matrices de $\mathrm{SL}_n(\mathbb{R})$ qui minimisent la norme euclidienne canonique de $\mathscr{M}_n(\mathbb{R})$).

Application 40 (Inégalité arithmético-géométrique)**.**

[GOU20] p. 339

$$\forall (x_1, \dots, x_n) \in (\mathbb{R}^+)^n, \left(\prod_{i=1}^{n} x_i \right)^{\frac{1}{n}} \leq \frac{1}{n} \sum_{i=1}^{n} x_i$$

Application 41 (Inégalité d'Hadamard)**.**

[ROU] p. 409

$$\forall (x_1, \dots, x_n) \in \mathbb{R}^n, \det(x_1, \dots, x_n) \leq \|x_1\| \dots \|x_n\|$$

avec égalité si et seulement si $(x_1, \dots, x_n)$ est une base orthogonale de $\mathbb{R}^n$.

III - Algorithmes d'optimisation numérique

1. Méthode de Newton

[DEV]

Théorème 42 (Méthode de Newton)**.** Soit $f : [c,d] \to \mathbb{R}$ une fonction de classe $\mathscr{C}^2$ strictement croissante sur $[c,d]$. On considère la fonction

$$\varphi : \begin{array}{ccc} [c,d] & \to & \mathbb{R} \\ x & \mapsto & x - \frac{f(x)}{f'(x)} \end{array}$$

(qui est bien définie car $f' > 0$). Alors :

(i) $\exists! a \in [c,d]$ tel que $f(a) = 0$.

(ii) $\exists \alpha > 0$ tel que $I = [a-\alpha, a+\alpha]$ est stable par φ.

(iii) La suite (x_n) des itérés (définie par récurrence par $x_{n+1} = \varphi(x_n)$ pour tout $n \geq 0$) converge quadratiquement vers a pour tout $x_0 \in I$.

[ROU] p. 152

Corollaire 43. En reprenant les hypothèses et notations du théorème précédent, et en supposant de plus f strictement convexe sur $[c,d]$, le résultat du théorème est vrai sur $I = [a,d]$. De plus :

(i) (x_n) est strictement décroissante (ou constante).

(ii) $x_{n+1} - a \sim \frac{f''(a)}{2f'(a)}(x_n - a)^2$ pour $x_0 > a$.

Exemple 44.

— On fixe $y > 0$. En itérant la fonction $F : x \mapsto \frac{1}{2}\left(x + \frac{y}{x}\right)$ pour un nombre de départ compris entre c et d où $0 < c < d$ et $c^2 < 0 < d^2$, on peut obtenir une approximation du nombre $\sqrt{y}$.

— En itérant la fonction $F : x \mapsto \frac{x^2+1}{2x-1}$ pour un nombre de départ supérieur à 2, on peut obtenir une approximation du nombre d'or $\varphi = \frac{1+\sqrt{5}}{2}$.

2. Lien avec les systèmes linéaires

Proposition 45. Soient $A \in \mathscr{S}_n^{++}(\mathbb{R})$ et $b \in \mathbb{R}^n$. On pose $f : x \mapsto \frac{1}{2}\langle Ax, x\rangle + \langle b, x\rangle$. Alors, minimiser f sur $\mathbb{R}^n$ revient à résoudre le système linéaire $Ax = b$.

[BMP] p. 24

221 Équations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications.

Dans toute la suite, $\mathbb{K}$ désignera le corps $\mathbb{R}$ ou $\mathbb{C}$.

I - Généralités

1. Définitions

Définition 1. Soient $n \in \mathbb{N}^*$, E un espace de Banach et $\Omega \subseteq \mathbb{R} \times E^n$ un ouvert. Soit $F : \Omega \times \mathbb{R}^n \to E$ une fonction. [GOU20] p. 373

— On appelle **équation différentielle** une équation de la forme

$$y^{(n)} = F(t, y, y', \dots, y^{(n-1)}) \qquad (*)$$

(ie. une équation portant sur les dérivées d'une fonction.)

— Toute application $\varphi : I \to E$ (où I est un intervalle de $\mathbb{R}$) n fois dérivable vérifiant :

(i) $\forall t \in I, (t, \varphi(t), \dots, \varphi^{(n-1)}(t)) \in \Omega$;

(ii) $\forall t \in I, F(t, \varphi(t), \dots, \varphi^{(n-1)}(t)) = \varphi^{(n)}(t)$;

est une **solution** de $(*)$. On note $\mathcal{S}_*$ l'ensemble des solutions de $(*)$.

— Une solution $\varphi : I \to E$ de $(*)$ est dite **maximale** s'il n'existe pas d'autre solution $\psi : J \to E$ (où J est un intervalle de $\mathbb{R}$) de $(*)$ telle que $I \subseteq J$, $I \neq J$ et $\psi = \varphi$ sir I.

— On appelle **problème de Cauchy** de $(*)$ en $(t_0, x_0, \dots, x_{n-1})$ la recherche d'une solution $\varphi : I \to E$ de $(*)$ vérifiant

$$\forall t_0 \in I, \varphi(t_0) = x_0, \dots, \varphi^{(n-1)}(t_0) = x_{n-1}$$

Définition 2. Toute équation différentielle sur $\mathbb{K}^n$ d'ordre $p \geq 1$ du type p. 377

$$Y^{(p)} = A_{p-1}(t)Y^{(p-1)} + \cdots + A_0(t)Y + B(t) \qquad (L)$$

(où $A_{p-1}, \dots, A_0$ sont des fonctions continues d'un intervalle I de $\mathbb{R}$ non réduit à un point dans $\mathcal{M}_n(\mathbb{K})$ et $B : I \to \mathbb{K}^n$ est une fonction continue) est appelée **équation différentielle linéaire** d'ordre p.

Si de plus $B = 0$, alors (L) est qualifiée d'**homogène**.

Définition 3. Si $n \geq 2$, on parle de **système différentiel linéaire**. Si $n = 1$, on parle d'équation différentielle linéaire **scalaire**.

Remarque 4. L'équation (L) précédente peut aussi s'écrire :

$$\begin{pmatrix} Y \\ Y' \\ \vdots \\ \vdots \\ Y^{(p-1)} \end{pmatrix}' = \begin{pmatrix} 0 & I_n & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & I_n \\ A_0(t) & \dots & \dots & \dots & A_{p-1}(t) \end{pmatrix} \begin{pmatrix} Y \\ Y' \\ \vdots \\ \vdots \\ Y^{(p-1)} \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ \vdots \\ \vdots \\ B(t) \end{pmatrix}$$

Ainsi, nous avons ramené l'équation différentielle linéaire (L) d'ordre p à une équation différentielle linéaire d'ordre 1. Donc, pour cette raison, on peut se limiter à l'étude des équations différentielles linéaires d'ordre 1.

2. Structure de l'ensemble des solutions

[DEV]

Théorème 5 (Cauchy-Lipschitz linéaire)**.** Soient $A : I \to \mathcal{M}_n(\mathbb{K})$ et $B : I \to \mathbb{K}^d$ deux fonctions continues. Alors $\forall t_0 \in I$, le problème de Cauchy

$$\begin{cases} Y' = A(t)Y + B(t) \\ Y(t_0) = y_0 \end{cases}$$

admet une unique solution définie sur I tout entier.

[DAN] p. 520

Remarque 6 (Version linéaire d'ordre p). Soient $A_{p-1}, \dots, A_0$ des fonctions continues d'un intervalle I de $\mathbb{R}$ non réduit à un point dans $\mathcal{M}_n(\mathbb{K})$ et $B : I \to \mathbb{K}^n$ une fonction continue. Soient $X_0, \dots, X_{p-1} \in \mathbb{K}^n$. Alors, $\forall t_0 \in I$, le problème de Cauchy

$$\begin{cases} Y^{(p)} = A_{p-1}(t)Y^{(p-1)} + \cdots + A_0(t)Y + B(t) & \\ Y^{(k)}(t_0) = X_k & \forall k \in [\![1, p-1]\!] \end{cases}$$

admet une unique solution définie sur I tout entier.

[GOU20] p. 378

Exemple 7. Considérons l'équation $y' - y = 0$. Comme la fonction nulle est solution maximale, il s'agit de l'unique solution qui s'annule sur $\mathbb{R}$.

[ROM19-1] p. 402

Corollaire 8. L'ensemble des solutions d'une équation différentielle linéaire homogène d'ordre p défini sur un intervalle I est un sous-espace vectoriel de $\mathcal{C}^1(I, \mathbb{K}^n)$ de dimension np.

[GOU20] p. 278

Corollaire 9. Soit (H) l'équation différentielle linéaire homogène associée à une équation différentielle linéaire (L) et soit $V_0 \in \mathcal{S}_L$. Alors $\mathcal{S}_L = V_0 + \mathcal{S}_H$, et $\mathcal{S}_L$ est un espace affine de même dimension que $\mathcal{S}_H$.

3. Wronskien

Définition 10. Soient $V_1, \dots, V_n$ n solutions d'une équation différentielle linéaire homogène (H) définies sur un intervalle I. On appelle **wronskien** de $V_1, \dots, V_n$ l'application

$$W_{(V_1,\dots,V_n)} : \begin{array}{ccc} I & \to & \mathbb{K} \\ t & \mapsto & \det(V_1(t), \dots, V_n(t)) \end{array}$$

Exemple 11. Soient $v_1, \dots, v_p$ p solutions de $y^{(p)} = a_{p-1}(t)y^{(p-1)} + \cdots + a_0(t)y$ définies sur un intervalle I (où $\forall i$, $a_i : I \to \mathbb{K}$ est continue). Alors

$$\forall t \in I,\ W_{(v_1,\dots,v_p)}(t) = \begin{vmatrix} v_1(t) & \dots & v_p(t) \\ \vdots & & \vdots \\ v_1^{(p-1)}(t) & \dots & v_p^{(p-1)}(t) \end{vmatrix}$$

Exemple 12. Soient u et v deux solutions de $y'' = a(t)y' + b(t)y$ définies sur un intervalle I. Alors

$$\forall t \in I,\ W_{(u,v)}(t) = u(t)v'(t) - u'(t)v(t)$$

Proposition 13. Le rang de n solutions d'une équation différentielle linéaire homogène $V_1(t), \dots, V_n(t)$ est indépendant de t.

Corollaire 14. Soient $V_1, \dots, V_n$ n solutions d'une équation différentielle linéaire homogène (H). Alors $(V_1, \dots, V_n)$ est une base de $\mathcal{S}_H$ si et seulement si $\exists t_0$ tel que $W_{(V_1,\dots,V_n)}(t_0) \neq 0$.

Proposition 15. Soient $V_1, \dots, V_n$ n solutions d'une équation différentielle linéaire homogène (H). Alors $W_{(V_1,\dots,V_n)}$ est solution de l'équation différentielle linéaire homogène

$$Y' = \operatorname{trace}(A)Y$$

et pour tout t_0 élément de I, on a $\forall t \in I, W_{(V_1,\dots,V_n)}(t) = W_{(V_1,\dots,V_n)}(t_0)\exp(\int_{t_0}^{t} \operatorname{trace}(A(u))\,\mathrm{d}u)$.

p. 388

II - Résolution

1. Cas d'une équation différentielle linéaire scalaire

Proposition 16. Les solutions d'une équation différentielle linéaire homogène scalaire $y' = a(t)y$ sont proportionnelles à $t \mapsto e^{A(t)}$ où A est une primitive de a.

p. 379

Corollaire 17 (Variation de la constante)**.** Soient $(L) : y' = a(t)y + b(t)$ une équation différentielle linéaire scalaire et A une primitive de a. Alors,

$$\mathcal{S}_L = \left\{ t \mapsto \lambda(t)e^{A(t)} \mid \lambda'(t) = b(t)e^{-A(t)} \right\}$$

Exemple 18. L'ensemble des solutions de l'équation différentielle $(L) : y' + y = \sin(t)$ est

$$\mathcal{S}_L = \left\{ t \mapsto \frac{\sin(t) - \cos(t)}{2} + \mu e^{-t} \,\middle|\, \mu \in \mathbb{R} \right\}$$

Exemple 19. À cause du principe de "recollement" des solutions, la seule solution définie sur $\mathbb{R}$ de $(1-t^2)y' + ty = 0$ est la fonction nulle.

2. Cas d'un système différentiel linéaire

Proposition 20. Soient $V_1, \dots, V_n$ n solutions linéairement indépendantes d'une équation différentielle linéaire homogène $(H) : Y' = A(t)Y$. Alors,

$$\mathcal{S}_H = \left\{ \sum_{i=1}^{n} \lambda_i V_i \mid \lambda_i \in \mathbb{K} \right\}$$

Corollaire 21 (Variation de la constante)**.** Soit $(L) : Y' = A(t)Y + B(t)$ une équation différentielle linéaire. On note par (H) le équation différentielle linéaire homogène associée. Alors, si $V_1, \dots, V_n$ sont n solutions de (H), on a :

$$\mathcal{S}_L = \left\{ \sum_{i=1}^{n} \lambda_i(t) V_i \mid \sum_{i=1}^{n} \lambda_i'(t) V_i(t) = B(t) \right\}$$

Exemple 22. Soit $(L) : y'' = a(t)y' + b(t)y + c(t)$. On note u et v deux solutions de l'équation

différentielle linéaire homogène associée. Alors,

$$\mathcal{S}_L = \left\{ t \mapsto \lambda(t)u(t) + \mu(t)v(t) \mid \begin{cases} \lambda' u + \mu' v = 0 \\ \lambda' u' + \mu' v' = c \end{cases} \right\}$$

Exemple 23. On considère l'équation différentielle $(L) : y'' + y = \tan(t)$. Alors,

$$\mathcal{S}_L = \left\{ t \mapsto \alpha\cos(t) + \beta\sin(t) - \cos(t)\ln\left(\tan\left(\frac{\pi}{4} + \frac{t}{2}\right)\right) \mid \alpha, \beta \in \mathbb{R} \right\}$$

3. Cas où les coefficients sont constants

Définition 24. Soit $A \in \mathcal{M}_n(\mathbb{K})$. On définit

$$e^A = \exp(A) = \sum_{k=0}^{+\infty} \frac{A^k}{k!}$$

l'**exponentielle** de la matrice A.

Proposition 25. Une équation différentielle linéaire homogène $(H) : Y' = AY$ (où $A \in \mathcal{M}_n(\mathbb{R})$ est constante en t) a ses solutions maximales définies sur $\mathbb{R}$ et le problème de Cauchy

$$\begin{cases} Y' = AY \\ Y(0) = y_0 \end{cases}$$

a pour (unique) solution $t \mapsto e^{tA} y_0$.

Remarque 26. En reprenant les notations précédentes, si $\mathbb{K} = \mathbb{R}$, on peut réduire A dans $\mathbb{C}$ puis écrire les solutions de (H) sous la forme $\varphi(t) + \overline{\varphi(t)}$ (où φ est une solution complexe de (H)).

Corollaire 27. On considère une équation différentielle linéaire homogène $(H) : y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_0 y = 0$. On factorise P_H, le **polynôme caractéristique** de l'équation dans $\mathbb{C}$,

$$P_H = X^n + a_{n-1}X^{n-1} + \cdots + a_0 = \prod_{i=1}^{k} (X - r_i)^{m_i}$$

Alors,

$$\mathcal{S}_H = \left\{ t \mapsto \sum_{i=1}^{k} e^{r_i t} P_i(t) \right\}$$

où les P_i sont des polynômes de degré $< m_i$.

Exemple 28. On considère l'équation différentielle $(H) : y'' + ay' + by = 0$. Soient r_1 et r_2 les deux racines de P_H dans $\mathbb{C}$.

— Si $r_1 \neq r_2$, $\mathcal{S}_H = \{t \mapsto \lambda e^{r_1 t} + \mu e^{r_2 t} \mid \lambda, \mu \in \mathbb{C}\}$.

— Si $r_1 = r_2$, $\mathcal{S}_H = \{t \mapsto (\lambda t + \mu) e^{rt} \mid \lambda, \mu \in K\}$.

4. Quelques autres techniques de résolution

a. Abaissement de l'ordre

Proposition 29. On considère une équation différentielle linéaire homogène $(H) : y^{(n)} = a_{n-1}(t)y^{(n-1)} + \cdots + a_0(t)y$. Soit $\varphi \in \mathcal{S}_H$, alors $f = g\varphi$ est solution de (H) si et seulement si

$$\sum_{k=1}^{n} \binom{n}{k} g^k \varphi^{(n-k)} = a_{n-1}(t) \sum_{k=1}^{n-1} \binom{n-1}{k} g^k \varphi^{(n-1-k)} + \cdots + a_1(t)(g'\varphi)$$

ie. g' est solution d'une équation différentielle d'ordre $n-1$.

Exemple 30. Soit φ une solution de $(H) : y'' = a(t)y' + b(t)y$, alors $f = g\varphi$ est solution de (H) si et seulement si $2g'\varphi' + g''\varphi = a(t)g'\varphi$.

b. Utilisation des séries entières

Proposition 31. Soient $a_0, \ldots, a_{p-1}$ et b des fonctions à valeurs dans $\mathbb{K}$ développables en série entière sur un intervalle ouvert $]-R, R[$ (R étant un réel strictement positif). Soient $y_0, \ldots, y_{p-1} \in \mathbb{C}$. On considère le problème de Cauchy :

$$\begin{cases} y^{(p)} = a_0(t)y + \cdots + a_{p-1}(t)y^{(p-1)} + b(t) \\ y^{(k)}(0) = y_k \qquad\qquad \forall k \in [\![0, p-1]\!] \end{cases} \tag{$*$}$$

Alors $(*)$ admet une unique solution développable en série entière sur $]-R, R[$.

[ROM19-1] p. 401

Exemple 32. La fonction $\sin : \mathbb{R} \to [1, 1]$ est l'unique solution du problème de Cauchy

$$\begin{cases} y'' = y \\ y(0) = 0 \\ y'(0) = 1 \end{cases}$$

p. 412

Application 33. La fonction $f_\alpha : x \mapsto (1+x)^\alpha$ où $\alpha \in \mathbb{R} \setminus \mathbb{N}$ est développable en série entière de rayon de convergence 1 et

$$\forall x \in]-1,1[,\ f_\alpha(x) = 1 + \sum_{n=1}^{+\infty} \frac{\alpha(\alpha-1)\dots(\alpha-n+1)}{n!} x^n$$

III - Études qualitatives

Lemme 34 (Grönwall)**.** Soient $\varphi, \psi, y : [a,b] \to \mathbb{R}^+$ continues vérifiant $\forall t \in [a,b],\ y(t) \leq \varphi(t)\left|\int_a^t \psi(s)y(s)\,\mathrm{d}s\right|$. Alors,

$$\forall t \in I,\ y(t) \leq \varphi(t) + \int_a^t \varphi(s)\psi(s)\exp\left(\int_s^t \psi(u)\,\mathrm{d}u\right)\mathrm{d}s$$

[GOU20] p. 397

Corollaire 35. Soient $\varphi, y : [a,b] \to \mathbb{R}^+$ continues et vérifiant $\exists c \geq 0,\ \forall t \in [a,b],\ y(t) \leq c + \int_a^t \varphi(s)y(s)\,\mathrm{d}s$. Alors,

$$\forall t \in [a,b],\ y(t) \leq c\exp\left(\int_a^t \varphi(s)\,\mathrm{d}s\right)$$

Application 36. Soit $q : \mathbb{R}^+ \to \mathbb{R}_*^+$ croissante de classe $\mathscr{C}^1$. Alors les solutions de $y'' + q(t)y = 0$ sont bornées sur $\mathbb{R}^+$.

Théorème 37 (Floquet)**.** On considère l'équation $(H) : Y' = A(t)Y$ où $A : \mathbb{R} \to \mathbb{C}$ est une fonction continue et T-périodique. Alors, (H) admet une solution V non nulle telle que

$$\exists \lambda \in \mathbb{C}, \forall t \in \mathbb{R},\ V(t+T) = \lambda V(t)$$

p. 387

Théorème 38 (Massera)**.** Si l'équation $Y' = A(t)Y + B(t)$ (où A et B sont T-périodiques) admet une solution bornée sur $\mathbb{R}$, alors elle admet une solution T-périodique.

p. 406

IV - Applications

1. Résolution d'équations différentielles non linéaires

Application 39 (Équations de Bernoulli)**.** Soit $(B) : y' = a(t)y + b(t)y^\alpha$ (où $\alpha \in \mathbb{R} \setminus \{0,1\}$). On pose $z = y^{1-\alpha}$ et on a

$$(B) \iff \frac{1}{1-\alpha} z' = a(t)z + b(t)$$

p. 391

Corollaire 40 (Équations de Ricatti)**.** Soit $(R) : y' = a(t)y^2 + b(t)y + c(t)$ qui admet pour solution particulière φ_0. On pose $y = \varphi_0 + z$ et on a

$$(R) \iff (2a(t)\varphi_0(t) + b(t))z + a(t)z^2$$

qui est une équation de Bernoulli.

Exemple 41. Les solutions maximales de l'équation $y' + y + y^2 + 1 = 0$ sont de la forme $t \mapsto e^{\frac{2i\pi}{3}} + \frac{\sqrt{3}}{e^{i(\sqrt{3}t+\theta)}+i}$, définies que des intervalles ouverts de longueur $\frac{2\pi}{\sqrt{3}}$.

2. Stabilité

Application 42 (Théorème de stabilité de Liapounov)**.** Soit $f \in \mathscr{C}^1(\mathbb{R}^n)$ telle que $f(0) = 0$. On considère le problème de Cauchy

$$\begin{cases} y' = f(y) \\ y(0) = y_0 \end{cases}$$

Si toute valeur propre complexe de $\mathrm{d}f_0$ est de partie réelle strictement négative, alors $\forall y_0$ suffisamment proche de 0, la solution maximale $y(t)$ est bien définie et converge vers 0 en $+\infty$ à une vitesse exponentielle.

[I-P] p. 302

3. Étude d'équations fonctionnelles et matricielles

Application 43. L'ensemble des fonctions $f : \mathbb{R}_*^+ \to \mathbb{R}$ vérifiant $\forall t > 0$, $f'(t) = f\left(\frac{1}{t}\right)$ est l'ensemble des solutions de l'équation différentielle linéaire homogène $t^2y'' + y = 0$.

[GOU20] p. 384

Lemme 44. Soit $\|.\|$ une norme d'algèbre sur $\mathscr{M}_n(\mathbb{C})$, et soit $A \in \mathscr{M}_n(\mathbb{C})$ une matrice dont les valeurs propres sont de partie réelle strictement négative. Alors il existe une fonction polynômiale $P : \mathbb{R} \to \mathbb{R}$ et $\lambda > 0$ tels que $\|e^{tA}\| \leq e^{-\lambda t}P(t)$.

[I-P] p. 177

[DEV]

Application 45 (Équation de Sylvester)**.** Soient A et $B \in \mathscr{M}_n(\mathbb{C})$ deux matrices dont les valeurs propres sont de partie réelle strictement négative. Alors pour tout $C \in \mathscr{M}_n(\mathbb{C})$, l'équation $AX + XB = C$ admet une unique solution X dans $\mathscr{M}_n(\mathbb{C})$.

223 Suites numériques. Convergence, valeurs d'adhérence. Exemples et applications.

Dans toute la suite, $\mathbb{K}$ désignera le corps $\mathbb{R}$ ou $\mathbb{C}$.

I - Convergence des suites numériques

1. Limite d'une suite

Définition 1. Soit E un ensemble non vide. On appelle **suite** à valeurs dans E toute application $u : D \to E$ où D est une partie de $\mathbb{N}$. Lorsque E est une partie de $\mathbb{R}$ (resp. de $\mathbb{C}$), on dit que u est **réelle** (resp. **complexe**). Dans ces deux cas, on parle de **suite numérique**. [AMR11] p. 1

On fixe, pour tout le reste de la leçon, (u_n) une suite numérique à coefficients dans $\mathbb{K}$.

Définition 2. p. 12

— Si $\mathbb{K} = \mathbb{R}$, on dit que (u_n) est **majorée** (resp. **minorée**) s'il existe $A \in \mathbb{R}$ tel que $\forall n \in \mathbb{N}$, $u_n \leq A$ (resp. $A \leq u_n$).

— On dit que (u_n) est **bornée** s'il existe $A \in \mathbb{R}$ tel que $\forall n \in \mathbb{N}$, $|u_n| \leq A$ (resp. $A \leq u_n$). Dans le cas où $\mathbb{K} = \mathbb{R}$, cela revient à dire que (u_n) est majorée et minorée.

— On dit que (u_n) admet $\ell \in \mathbb{K}$ pour **limite** (ou **converge** / **tend** vers ℓ) si,

$$\forall \epsilon > 0, \exists N \in \mathbb{N} \text{ tel que } \forall n \geq N, |u_n - \ell| < \epsilon$$

On le note $\lim_{n\to+\infty} u_n = \ell$ ou $u_n \longrightarrow_{n\to+\infty} \ell$.

— On dit que (u_n) est **convergente** si elle admet une limite. Sinon, on dit qu'elle est **divergente**.

Exemple 3. Si (u_n) est définie par

$$\forall n \geq 1,\ u_n = 1 + \frac{(-1)^n}{n}$$

alors (u_n) converge vers 1.

Théorème 4. On a unicité de la limite dans $\mathbb{K}$.

Proposition 5. Toute suite numérique convergente est bornée.

Contre-exemple 6. $((-1)^n)$ est bornée, non convergente.

Proposition 7. Soit (v_n) une suite numérique bornée. On suppose $\lim_{n\to+\infty} u_n = 0$. Alors $\lim_{n\to+\infty} u_n v_n = 0$.

Proposition 8. On suppose $\lim_{n\to+\infty} u_n = \ell_1 \in \mathbb{K}$. Soit (v_n) une suite numérique qui converge vers $\ell_2 \in \mathbb{K}$. Alors :

(i) $\lim_{n\to+\infty} u_n + v_n = \ell_1 + \ell_2$.

(ii) $\lim_{n\to+\infty} \lambda u_n = \lambda \ell_1$ pour tout $\lambda \in \mathbb{K}$.

(iii) $\lim_{n\to+\infty} u_n v_n = \ell_1 \ell_2$.

(iv) Si $\ell_2 \neq 0$, on a $v_n \neq 0$ à partir d'un certain rang et, $\lim_{n\to+\infty} \frac{u_n}{v_n} = \frac{\ell_1}{\ell_2}$.

Définition 9. On suppose $\mathbb{K} = \mathbb{R}$. p. 20

— On dit que (u_n) **tend vers** $+\infty$ si,

$$\forall A \in \mathbb{R}, \exists N \in \mathbb{N} \text{ tel que } \forall n \geq N,\ u_n \geq A$$

— On dit que (u_n) **tend vers** $-\infty$ si $(-u_n)$ tend vers $+\infty$.

On a les mêmes notations qu'à la Théorème 2.

Proposition 10. On suppose $\lim_{n\to+\infty} u_n = +\infty$.

(i) (u_n) est minorée.

(ii) (u_n) est strictement positive à partir d'un certain rang et $\lim_{n\to+\infty} \frac{1}{u_n} = 0$.

(iii) Soit (v_n) une suite numérique.

— Si (v_n) est convergente ou $\lim_{n\to+\infty} v_n = +\infty$, on a $\lim_{n\to+\infty} u_n + v_n = +\infty$.

— Si $\lim_{n\to+\infty} v_n = +\infty$, on a $\lim_{n\to+\infty} u_n v_n = +\infty$.

Exemple 11. Soit $\lambda \in \mathbb{R}$. Alors, p. 29

$$\lim_{n\to+\infty} \lambda n = \begin{cases} +\infty & \text{si } \lambda > 0 \\ -\infty & \text{si } \lambda < 0 \\ 0 & \text{sinon} \end{cases}$$

2. Convergence de suites réelles

Le résultat suivant justifie de se ramener au cas réel lors de l'étude de la convergence des suites numériques. p. 20

Proposition 12. Soient $(x_n), (y_n)$ deux suites réelles et x, y deux réels. Alors,

$$\lim_{n\to+\infty} x_n + iy_n = x + iy \iff \begin{cases} \lim_{n\to+\infty} x_n & = x \\ \lim_{n\to+\infty} y_n & = y \end{cases}$$

On se place pour le restant de la sous-section dans le cas où $\mathbb{K} = \mathbb{R}$.

Théorème 13 (des gendarmes)**.** Soient (a_n) et (b_n) deux suites réelles de même limite $\ell \in \mathbb{R}$ telles qu'à partir d'un certain rang, on ait $a_n \leq u_n \leq b_n$. Alors, $u_n \longrightarrow_{n\to+\infty} \ell$.

Définition 14. (u_n) est dite **croissante** (resp. **décroissante**) si pour tout entier n, on a $u_{n+1} \geq u_n$ (resp. $u_{n+1} \leq u_n$). Elle est dite **monotone** si elle est croissante ou décroissante.

Théorème 15 (de la limite monotone)**.** Si (u_n) est croissante et majorée ou décroissante et minorée, alors elle est convergente.

Théorème 16 (Suites adjacentes)**.** Si deux suites (u_n) et (v_n) sont adjacentes (ie. (u_n) est croissante, (v_n) est décroissante et la suite différence tend vers 0), alors elles sont convergentes de même limite ℓ qui vérifie

$$\forall n \in \mathbb{N},\ u_n \leq \ell \leq v_n$$

Exemple 17. Les suites $\left(1 - \frac{1}{n}\right)$ et $\left(1 + \frac{1}{n^2}\right)$ sont adjacentes et convergent vers 1.

Corollaire 18 (Segments emboîtés)**.** Soient (a_n) et (b_n) deux suites réelles telles que p. 36

$$\begin{cases} \forall n \in \mathbb{N},\ a_n \leq b_n \\ \forall n \in \mathbb{N},\ [a_{n+1}, b_{n+1}] \subseteq [a_n, b_n] \\ (b_n - a_n) \longrightarrow 0 \end{cases}$$

Alors, il existe un nombre réel unique ℓ tel que $\bigcap_{n\geq 0} [a_n, b_n] = \{\ell\}$.

Application 19 (Critère de Leibniz)**.** Soit (a_n) une suite à termes positifs, décroissantes, p. 97

tendant vers 0. Alors

$$\sum(-1)^n a_n \text{ converge} \quad \text{et} \quad \forall n \in \mathbb{N}, |R_n| = \left| \sum_{k=n+1}^{+\infty} (-1)^k a_k \right| \leq a_{n+1}$$

(voir Section 2.)

Définition 20. Pour cette définition, on ne suppose pas au cas réel. p. 25

— On dit que (u_n) est **négligeable** devant une suite réelle positive (α_n) et on note $u_n = o(\alpha_n)$ si,

$$\forall \epsilon > 0, \exists N \in \mathbb{N}, \text{ tel que } \forall n \geq N, |u_n| \leq \epsilon \alpha_n$$

— On dit que (u_n) est **équivalente** à une suite numérique (v_n) et on note $u_n \sim v_n$, si $(u_n - v_n)$ est négligeable devant $(|u_n|)$.

Proposition 21. En reprenant les notations précédentes,

(i) On suppose (α_n) non nulle à partir d'un certain rang. (u_n) est négligeable devant α_n si et seulement si $\frac{u_n}{\alpha_n} \longrightarrow_{n\to+\infty} 0$.

(ii) On suppose (v_n) non nulle à partir d'un certain rang. (u_n) est équivalente à v_n si et seulement si $\frac{u_n}{\alpha_n} \longrightarrow_{n\to+\infty} 1$.

(iii) $\sim$ est une relation d'équivalence sur l'ensemble des suites de $\mathbb{K}$.

Exemple 22 (Formule de Stirling)**.** p. 353

$$n! \sim \sqrt{2n\pi}\left(\frac{n}{e}\right)^n$$

Proposition 23. Deux suites convergentes équivalentes ont la même limite. p. 28

3. Suites de Cauchy

Définition 24. On dit que (u_n) est **de Cauchy** si p. 34

$$\forall \epsilon > 0, \exists N \in \mathbb{N} \text{ tel que } \forall p > q \geq N, |u_p - u_q| < \epsilon$$

Proposition 25. (i) Une suite convergente est de Cauchy.

(ii) Une suite de Cauchy est bornée.

Théorème 26. Toute suite de Cauchy de $\mathbb{K}$ est convergente dans $\mathbb{K}$.

Contre-exemple 27. La série $\sum \frac{1}{n}$ est une suite de Cauchy de $\mathbb{Q}$ non convergente dans $\mathbb{Q}$. [HAU] p. 312

4. Convergence au sens de Cesàro

Définition 28. À toute suite numérique (u_n) on y associe sa suite (v_n) des **moyennes de Cesàro** où [AMR11] p. 53

$$\forall n \in \mathbb{N}, v_n = \frac{1}{n}\sum_{k=1}^{n} u_k$$

Théorème 29. Si (u_n) converge vers $\ell \in \mathbb{K}$, alors sa suite des moyennes de Cesàro converge vers ℓ. On dit que (u_n) converge **au sens de Cesàro**.

Exemple 30.
— Soit (v_n) une suite numérique dont aucun terme n'est nul, qui converge vers $\ell \neq 0$. Alors,

$$\frac{1}{n}\frac{1}{\sum_{k=1}^{n}\frac{1}{v_k}} \longrightarrow_{n\to+\infty} \frac{1}{\ell}$$

converge vers $\frac{1}{\ell}$.

— Soit (w_n) une suite numérique telle que $(w_{n+1}-w_n)$ converge vers $\ell \in \mathbb{K}$. Alors,

$$\frac{w_n}{n} \longrightarrow_{n\to+\infty} \ell$$

Remarque 31. La réciproque du Théorème 29 est fausse.

Exemple 32. $(-1)^n$ converge au sens de Cesàro vers 0, mais pas au sens usuel.

II - Valeurs d'adhérence

1. Suites extraites

Définition 33. On appelle **sous-suite** ou **suite extraite** de (u_n), toute suite $(u_{\varphi(n)})$ où $\varphi : \mathbb{N} \to \mathbb{N}$ est strictement croissante (on dit que φ est une **extractrice**). p. 14

Proposition 34. Si une suite converge vers $\ell \in \mathbb{K}$, alors toute suite extraite converge vers ℓ.

Définition 35. On appelle **valeur d'adhérence** d'une suite numérique, tout élément de $\mathbb{K}$ limite d'une de ses sous-suites convergentes.

Remarque 36.
— Toute suite numérique convergente ne possède que sa limite comme valeur d'adhérence.
— Une suite possédant une unique valeur d'adhérence n'est pas nécessairement convergente.

Exemple 37. $((1-(-1)^n)n)$ ne possède que 0 comme valeur d'adhérence, mais ne converge pas.

Théorème 38 (Bolzano-Weierstrass)**.** Toute suite numérique bornée possède au moins une sous-suite convergente.

p. 36

Proposition 39. Une suite numérique est convergente si et seulement si elle est bornée et n'a qu'une seule valeur d'adhérence.

[DAN] p. 73

Application 40. Soit (E,d) un espace métrique compact. Soit (v_n) une suite de E telle que $d(v_n, v_{n-1}) \longrightarrow 0$. Alors l'ensemble Γ des valeurs d'adhérence de (v_n) est connexe.

[I-P] p. 116

Corollaire 41 (Lemme de la grenouille)**.** Soient $f : [0,1] \to [0,1]$ continue et (x_n) une suite de $[0,1]$ telle que

$$\begin{cases} x_0 \in [0,1] \\ x_{n+1} = f(x_n) \end{cases}$$

Alors (x_n) converge si et seulement si $\lim_{n\to+\infty} x_{n+1} - x_n = 0$.

2. Limites inférieure et supérieure

On se place dans le cas réel pour toute cette sous-section.

[AMR11] p. 93

Lemme 42. Si (u_n) n'est pas bornée, on peut extraire une sous-suite qui tend vers $\pm\infty$: $\pm\infty$ est une valeur d'adhérence de (u_n) dans $\overline{\mathbb{R}}$.

Définition 43. On appelle **limite inférieure** (resp. **limite supérieure**) de (u_n), notée $\limsup_{n\to+\infty} u_n$ (resp. $\liminf_{n\to+\infty} u_n$) la plus grande (resp. plus petite) de ses valeurs d'adhérence.

[DAN] p. 77

Proposition 44. (u_n) converge si et seulement si $\liminf_{n\to+\infty} u_n = \limsup_{n\to+\infty} u_n$.

III - Suites particulières

1. Suites récurrentes

Définition 45. Soit $E \subseteq \mathbb{K}$. On dit que (u_n) est **récurrente** d'ordre $h \in \mathbb{N}^*$ si on peut écrire

$$\forall n \geq h,\ u_{n+h} = f(u_{n-1}, \dots, u_{n-h}) \qquad (*)$$

où $f : E^h \to E$ et les premières valeurs $u_0, \dots, u_{h-1} \in E$ étant donnés.

[GOU20] p. 200

Théorème 46 (Caractérisation séquentielle de la continuité)**.** En reprenant les notations précédentes, une fonction $g : E \to \mathbb{K}$ est continue si et seulement si pour toute suite numérique convergente $(v_n) \in E^{\mathbb{N}}$ dont on note ℓ la limite, $g(v_n) \longrightarrow_{n\to+\infty} \ell$.

[AMR11] p. 38

Corollaire 47. Si une suite récurrente d'ordre 1 (dont on note f la fonction) converge vers ℓ, alors $f(\ell) = \ell$.

Exemple 48. La suite (u_n) définie par $u_0 \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$ et $\forall n \geq 1,\ u_{n+1} = \sin(u_n)$ converge vers 0.

[DEV]

Application 49 (Méthode de Newton)**.** Soit $g : [c,d] \to \mathbb{R}$ une fonction de classe $\mathscr{C}^2$ strictement croissante sur $[c,d]$. On considère la fonction

$$\varphi : \begin{array}{ccc} [c,d] & \to & \mathbb{R} \\ x & \mapsto & x - \frac{g(x)}{g'(x)} \end{array}$$

(qui est bien définie car $g' > 0$). Alors :

(i) $\exists! a \in [c,d]$ tel que $g(a) = 0$.

(ii) $\exists \alpha > 0$ tel que $I = [a-\alpha, a+\alpha]$ est stable par φ.

(iii) La suite (x_n) des itérés (définie par récurrence par $x_{n+1} = \varphi(x_n)$ pour tout $n \geq 0$) converge quadratiquement vers a pour tout $x_0 \in I$.

[ROU] p. 152

Corollaire 50. En reprenant les hypothèses et notations du théorème précédent, et en supposant de plus g strictement convexe sur $[c,d]$, le résultat du théorème est vrai sur $I = [a,d]$. De plus :

(i) (x_n) est strictement décroissante (ou constante).

(ii) $x_{n+1} - a \sim \frac{f''(a)}{2f'(a)}(x_n - a)^2$ pour $x_0 > a$.

Exemple 51. — On fixe $y > 0$. En itérant la fonction $F : x \mapsto \frac{1}{2}\left(x + \frac{y}{x}\right)$ pour un nombre de départ compris entre c et d où $0 < c < d$ et $c^2 < 0 < d^2$, on peut obtenir une approximation du nombre $\sqrt{y}$.

— En itérant la fonction $F : x \mapsto \frac{x^2+1}{2x-1}$ pour un nombre de départ supérieur à 2, on peut obtenir une approximation du nombre d'or $\varphi = \frac{1+\sqrt{5}}{2}$.

2. Séries numériques

Définition 52. — On appelle **série** de terme général u_n la suite (S_n) définie par

$$\forall n \in \mathbb{N},\ S_n = u_0 + \cdots + u_n$$

On note cette série $\sum u_n$.

— u_n s'appelle le **terme** d'indice n.

— S_n s'appelle la **somme partielle** d'indice n.

[GOU20] p. 208

Définition 53. En reprenant les notations précédentes, on dit que $\sum u_n$ **converge** si la suite (S_n) converge. Dans ce cas, la limite s'appelle la **somme** de la série, et on la note $\sum_{n=0}^{+\infty} u_n$.

Proposition 54. Si $\sum u_n$ converge, alors $\lim_{n\to+\infty} u_n = 0$.

[AMR11] p. 81

Contre-exemple 55. La réciproque est fausse, par exemple en considérant la suite (u_n) définie pour tout $n \in \mathbb{N}$ par $u_n = \ln(1 + \frac{1}{n})$, on a $\sum_{k=1}^{n} u_k = \ln(n+1) \longrightarrow_{n\to+\infty} +\infty$.

Proposition 56. Muni des opérations :

— $\forall (u_n), (v_n) \in \mathbb{K}^{\mathbb{N}},\ \sum u_n + \sum v_n = \sum (u_n + v_n)$,

— $\forall \lambda \in \mathbb{K},\ \forall (u_n) \in \mathbb{K}^{\mathbb{N}},\ \lambda \sum u_n = \sum (\lambda u_n)$,

l'ensemble des séries numériques est un espace vectoriel sur $\mathbb{K}$ dont l'ensemble des séries convergentes est un sous-espace vectoriel.

Proposition 57 (Règle de d'Alembert)**.** Soit $\sum u_n$ une série à termes strictement positifs telle que

$$\lim_{n\to+\infty} \frac{u_{n+1}}{u_n} = \lambda \in [0, +\infty]$$

[GOU20] p. 214

Alors :

(i) Si $\lambda < 1$, $\sum u_n$ converge.

(ii) Si $\lambda > 1$, $\sum u_n$ diverge.

Exemple 58. $\sum \left(1 - \frac{1}{n}\right)^{n^2}$ converge.

[AMR11] p. 94

Exemple 59. $\sum_{k=0}^{10} \frac{1}{n!}$ donne une valeur approchée de e à moins de 3×10^{-8} près par défaut.

p. 108

Proposition 60 (Règle de Cauchy)**.** Soit $\sum u_n$ une série à termes strictement positifs telle que

$$\lim_{n \to +\infty} \sqrt[n]{u_n} = \lambda \in [0, +\infty]$$

[GOU20] p. 214

Alors :

(i) Si $\lambda < 1$, $\sum u_n$ converge.

(ii) Si $\lambda > 1$, $\sum u_n$ diverge.

Exemple 61. $\sum \left(\frac{4n+1}{3n+2}\right)^n$ converge.

[AMR11] p. 112

Lemme 62. Soit $\alpha > 1$. Lorsque n tend vers $+\infty$, on a

$$\sum_{k=n+1}^{+\infty} \frac{1}{n^\alpha} \sim \frac{1}{\alpha - 1} \frac{1}{n^{\alpha - 1}}$$

[I-P] p. 380

[DEV]

Proposition 63 (Développement asymptotique de la série harmonique)**.** On note $\forall n \in \mathbb{N}^*$, $H_n = \sum_{k=1}^{n} \frac{1}{k}$. Alors, quand n tend vers $+\infty$,

$$H_n = \ln(n) + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + o\left(\frac{1}{n^2}\right)$$

224 Exemples de développements asymptotiques de suites et de fonctions.

I - Comparaison de suites et de fonctions

Soit E un espace vectoriel normé sur $\mathbb{R}$.

[GOU20] p. 87

1. Relations de comparaison

Définition 1. Soit X un espace métrique. On considère deux applications $f, g : D \to E$ où $D \subseteq X$. Soit x_0 un point d'accumulation de D.

— On dit que f est **dominée** par g au voisinage de x_0, si

$$\exists C > 0, \exists V \text{ voisinage de } x_0 \text{ tels que } \forall x \in V \cap D, \|f(x)\| \leq C\|g(x)\|$$

On note alors $f(x) = O(g(x))$ quand $x \to x_0$.

— On dit que f est **négligeable** devant g au voisinage de x_0, si

$$\forall \epsilon > 0, \exists V \text{ voisinage de } x_0 \text{ tels que } \forall x \in V \cap D, \|f(x)\| \leq \epsilon\|g(x)\|$$

On note alors $f(x) = o(g(x))$ quand $x \to x_0$.

— On dit que f et g sont **équivalentes** au voisinage de x_0 si $f(x) - g(x) = o(g(x))$ quand $x \to x_0$ et on écrit alors $f(x) \sim g(x)$ quand $x \to x_0$.

Remarque 2. Dans la pratique, on utilisera souvent cette notation pour des fonction de $\mathbb{R}$ dans $\mathbb{C}$ au voisinage d'un point de $\mathbb{R}$ ou de l'infini, ou pour des suites réelles ou complexes (u_n) quand $n \to +\infty$.

[DAN] p. 132

Exemple 3. Soit $f : \mathbb{R} \to \mathbb{R}$. Soit $x_0 \in \overline{\mathbb{R}}$.

— $f = O(1)$ si et seulement si f est une application bornée au voisinage de x_0.

— $f = o(1)$ si et seulement si f admet 0 pour limite en x_0.

— $f = o\left(\frac{1}{x}\right)$ en $+\infty$ signifie que $x \mapsto xf(x)$ admet pour limite 0 en $+\infty$.

Proposition 4. On considère deux applications $f, g : D \to \mathbb{R}$ où $D \subseteq \mathbb{R}$. Soit $x_0 \in \overline{\mathbb{R}}$. On suppose qu'il existe un voisinage V_0 de x_0 tel que g ne s'annule pas. Alors, quand $x \to x_0$:

(i) $f(x) = o(g(x))$ si et seulement si $\frac{f(x)}{g(x)} \longrightarrow_{x \to x_0} 0$.

(ii) $f(x) \sim g(x)$ si et seulement si $\frac{f(x)}{g(x)} \longrightarrow_{x \to x_0} 1$.

Proposition 5. La relation $\sim$ est une relation d'équivalence, compatible avec le produit et la puissance. Si deux fonctions f_1 et f_2 équivalentes au voisinage d'un point admettent des limites ℓ_1 et ℓ_2 en ce point, alors $\ell_1 = \ell_2$.

Contre-exemple 6. — $\sim$ n'est pas compatible avec l'addition. Par exemple, quand $x \to +\infty$,

$$x + \sqrt{x} \sim x,\ -x \sim -x + \ln(x) \text{ mais } \sqrt{x} \not\sim \ln(x)$$

— $\sim$ n'est pas compatible avec la composition. Par exemple, quand $x \to +\infty$,

$$x \sim x+1 \text{ mais } e^x \not\sim e^{x+1}$$

2. Développement limité

Dans cette partie, I désigne un intervalle de $\mathbb{R}$ non réduit à un point. Soit $f : I \to E$ une application. On suppose $0 \in I$.

[GOU20] p. 89

Définition 7. On dit que f admet un **développement limité** à l'ordre $n \in \mathbb{N}^*$ s'il existe $a_0, \dots, a_n \in E$ tels que, au voisinage de 0,

$$f(x) = \sum_{k=0}^{n} a_k x^k + o(x^n)$$

Remarque 8. On pourrait de même définir les développements limités au voisinage d'un point $a \in \bar{I}$.

Proposition 9. (i) Un développement limité, s'il existe, est unique.

(ii) Si f admet un développement limité en 0 à l'ordre $n \geq 1$, f est dérivable en 0 et sa dérivée en 0 vaut a_1.

(iii) Si f est paire (resp. impaire), les coefficients du développement limité d'indice impair (resp. pair) sont nuls.

(iv) Si f est n fois dérivable en 0, f' admet un développement limité en 0 : $f'(x) = \sum_{k=1}^{n} a_k x^{k-1} + o(x^{n-1})$.

(v) Si f est dérivable sur I et f' admet un développement limité en 0 : $f'(x) = \sum_{k=0}^{n} a_k x^k + o(x^n)$; alors, f admet un développement limité en 0 donné par $f(x) = \sum_{k=0}^{n} \frac{a_k}{(k+1)!} x^{k+1} + o(x^{k+1})$.

(vi) Les règles de somme, produit, quotient et composition obéissent aux mêmes règles que pour les polynômes (sous réserve de bonne définition).

Théorème 10 (Formule de Taylor-Young)**.** On suppose f de classe $\mathscr{C}^n$ sur I telle que $f^{(n+1)}(x)$ existe pour $x \in I$. Alors, quand $h \longrightarrow 0$, on a

$$f(x+h) = \sum_{k=0}^{n+1} \frac{f^{(k)}(x)}{k!} h^k + o(h^{n+1})$$

Proposition 11. Si f est n fois dérivable en 0, alors f admet un développement limité à l'ordre n en 0 :

$$f(x) = \sum_{k=0}^{n+1} \frac{f^{(k)}(0)}{k!} x^k + o(x^{n+1})$$

Exemple 12. En 0, on a les développements limités usuels suivants.

- $e^x = \sum_{k=0}^{n} \frac{x^k}{k!} + o(x^n)$.
- $\sin(x) = \sum_{k=0}^{n} (-1)^k \frac{x^{2k+1}}{(2k+1)!} + o(x^{2n+2})$.
- $\cos(x) = \sum_{k=0}^{n} (-1)^k \frac{x^{2k}}{(2k)!} + o(x^{2n+1})$.
- $\sinh(x) = \sum_{k=0}^{n} \frac{x^{2k+1}}{(2k+1)!} + o(x^{2n+2})$.
- $\cosh(x) = \sum_{k=0}^{n} \frac{x^{2k}}{(2k)!} + o(x^{2n+1})$.
- Pour tout $\alpha \in \mathbb{R}$, $(1+x)^\alpha = \sum_{k=0}^{n} \frac{\alpha(\alpha-1)\ldots(\alpha-k+1)}{k!} + o(x^n)$.

Application 13.

$$\lim_{x \to 0} \frac{\tan(x) - x}{\sin(x) - x} = -2$$

3. Développement asymptotique

Définition 14. Soient X un espace métrique et $x_0 \in X$. On appelle **échelle de comparaison** un ensemble $\mathscr{E}$ de fonctions définies au voisinage de x_0 dans X, sauf éventuellement en x_0, et vérifiant la propriété suivante : si $f, g \in \mathscr{E}$, alors $f = g$ ou bien $f = o(g)$ ou bien $g = o(f)$.

Exemple 15. Au voisinage de $+\infty$ pour les fonctions de la variable réelle, les fonctions du type $x \mapsto x^\alpha$ pour $\alpha \in \mathbb{R}$ forment une échelle de comparaison.

Définition 16. Soit X un espace métrique. On considère deux applications $f, g : D \to E$ où $D \subseteq X$. Soient x_0 un point d'accumulation de D et $k \in \mathbb{N}^*$. On appelle **développement asymptotique** à k termes de f par rapport à une échelle de comparaison $\mathscr{E}$ au voisinage de

x_0 toute expression de la forme

$$\sum_{i=1}^{k} c_i f_i$$

vérifiant

(i) $c_1, \dots, c_k \in E$ sont des constantes multiplicatives.

(ii) $f_1, \dots, f_k \in \mathscr{E}$ avec pour tout $i \in [\![1, k]\!]$, $f_{i+1}(x) = o(f_i(x))$.

(iii) $f(x) = \sum_{i=1}^{k} c_i f_i + o(f_k(x))$ quand $x \to x_0$.

$c_1 f_1$ est appelée **partie principale** de f au point x_0.

Remarque 17. En reprenant les notations précédentes :

— $f(x) \sim c_1 f_1(x)$ quand $x \to x_0$.

— Un tel développement, s'il existe, est unique.

II - Exemples de développements asymptotiques de suites

1. Séries numériques

Proposition 18 (Comparaison série - intégrale)**.** Soit $f : \mathbb{R}^+ \to \mathbb{R}^+$ une fonction positive, continue par morceaux et décroissante sur $\mathbb{R}^+$. Alors la suite (U_n) définie par

$$\forall n \in \mathbb{N},\ \sum_{k=0}^{n} f(k) - \int_0^n f(t)\,\mathrm{d}t$$

est convergente. En particulier, la série $\sum f(n)$ et l'intégrale $\int_0^{+\infty} f(t)\,\mathrm{d}t$ sont de même nature.

p. 212

Lemme 19. Soit $\alpha > 1$. Lorsque n tend vers $+\infty$, on a

$$\sum_{k=n+1}^{+\infty} \frac{1}{n^\alpha} \sim \frac{1}{\alpha - 1} \frac{1}{n^{\alpha-1}}$$

[I-P] p. 380

[DEV]

Proposition 20 (Développement asymptotique de la série harmonique)**.** On note $\forall n \in \mathbb{N}^*$, $H_n = \sum_{k=1}^{n} \frac{1}{k}$. Alors, quand n tend vers $+\infty$,

$$H_n = \ln(n) + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + o\left(\frac{1}{n^2}\right)$$

Application 21 (Série de Bertrand)**.** La série de Bertrand $\sum \frac{1}{n^\alpha \ln(n)^\beta}$ converge si et seulement si $\alpha > 1$ ou si $\alpha = 1$ et $\beta > 1$.

[GOU20] p. 212

2. Suites récurrentes

Définition 22. À toute suite numérique (u_n) on y associe sa suite (v_n) des **moyennes de Cesàro** où

$$\forall n \in \mathbb{N}, v_n = \frac{1}{n}\sum_{k=1}^{n} u_k$$

[AMR11] p. 53

Théorème 23. Si (u_n) converge vers $\ell \in \mathbb{K}$, alors sa suite des moyennes de Cesàro converge vers ℓ. On dit que (u_n) converge **au sens de Cesàro**.

Proposition 24. Soit f une application continue définie au voisinage de 0^+ admettantun développement asymptotique en 0 de la forme $f(x) = x - ax^\alpha + o(x^\alpha)$, où $a > 0$ et $\alpha > 1$. Alors pour $u_0 > 0$ assez petit, la suite (u_n) définie par $u_{n+1} = f(u_n)$ pour $n \in \mathbb{N}$ vérifie

$$u_n \sim \frac{1}{(na(\alpha-1))^{\frac{1}{\alpha-1}}}$$

[FGN3] p. 142

Exemple 25. Si $f = \sin$ et (u_n) est définie par $u_0 \in [0, 2\pi]$ et $\forall n \in \mathbb{N}$, $u_{n+1} = f(u_n)$, on a l'équivalent en $+\infty$:

$$u_n \sim \sqrt{\frac{3}{n}}$$

Proposition 26. En reprenant les notations précédentes, on a, pour $u_0 \in \left]0, \frac{\pi}{2}\right]$,

$$u_n = \sqrt{\frac{3}{n}} - \frac{3\sqrt{3}}{10}\frac{\ln(n)}{n\sqrt{n}} + o\left(\frac{\ln(n)}{n\sqrt{n}}\right)$$

[GOU20] p. 228

Exemple 27. On définit (u_n) par $u_0 \in \mathbb{R}$ et $\forall n \in \mathbb{N}$, $u_{n+1} = u_n + e^{-u_n}$, on a l'équivalent en $+\infty$:

$$u_n = n + \frac{\ln(n)}{2n} + o\left(\frac{\ln(n)}{n}\right)$$

[FGN3] p. 148

[DEV]

Théorème 28 (Méthode de Newton)**.** Soit $f : [c,d] \to \mathbb{R}$ une fonction de classe $\mathscr{C}^2$ strictement croissante sur $[c,d]$. On considère la fonction

$$\varphi : \begin{array}{ccc} [c,d] & \to & \mathbb{R} \\ x & \mapsto & x - \frac{f(x)}{f'(x)} \end{array}$$

(qui est bien définie car $f' > 0$). Alors :

[ROU] p. 152

(i) $\exists! a \in [c,d]$ tel que $f(a) = 0$.

(ii) $\exists \alpha > 0$ tel que $I = [a-\alpha, a+\alpha]$ est stable par φ.

(iii) La suite (x_n) des itérés (définie par récurrence par $x_{n+1} = \varphi(x_n)$ pour tout $n \geq 0$) converge quadratiquement vers a pour tout $x_0 \in I$.

Corollaire 29. En reprenant les hypothèses et notations du théorème précédent, et en supposant de plus f strictement convexe sur $[c,d]$, le résultat du théorème est vrai sur $I = [a,d]$. De plus :

(i) (x_n) est strictement décroissante (ou constante).

(ii) $x_{n+1} - a \sim \frac{f''(a)}{2f'(a)}(x_n - a)^2$ pour $x_0 > a$.

Exemple 30.
— On fixe $y > 0$. En itérant la fonction $F : x \mapsto \frac{1}{2}\left(x + \frac{y}{x}\right)$ pour un nombre de départ compris entre c et d où $0 < c < d$ et $c^2 < 0 < d^2$, on peut obtenir une approximation du nombre $\sqrt{y}$.

— En itérant la fonction $F : x \mapsto \frac{x^2+1}{2x-1}$ pour un nombre de départ supérieur à 2, on peut obtenir une approximation du nombre d'or $\varphi = \frac{1+\sqrt{5}}{2}$.

3. Suites définies implicitement

Exemple 31. Soit $n \in \mathbb{N}$. Soit a_n la plus grande racine réelle de $X^{2n} - 2nX + 1$. Alors,

$$a_n = 1 + \frac{\ln(2n)}{2n} + o\left(\frac{\ln(n)}{n}\right)$$

[FGN3] p. 181

Exemple 32. Soit (u_n) une suite de réels vérifiant $\forall n \in \mathbb{N}$, $u_n^5 + nu_n - 1 = 0$. Alors,

$$u_n = \frac{1}{n} - \frac{1}{n^6} + o\left(\frac{1}{n^6}\right)$$

Exemple 33. Soit $c > 0$. On note x_n l'unique racine réelle de $x \mapsto x\sin(x) - c\cos(x)$. Alors,

$$x_n - n\pi \sim \frac{c}{n\pi}$$

III - Exemples de développements asymptotiques de fonctions

1. Fonctions définies par la somme d'une série

Théorème 34 (Central limite)**.** Soit (X_n) une suite de variables aléatoires réelles indépendantes de même loi admettant un moment d'ordre 2. On note m l'espérance et σ^2 la variance commune à ces variables. On pose $S_n = X_1 + \cdots + X_n - nm$. Alors,

$$\left(\frac{S_n}{\sqrt{n}}\right) \xrightarrow{(d)} \mathcal{N}(0,\sigma^2)$$

[G-K] p. 307

Application 35 (Théorème de Moivre-Laplace)**.** On suppose que (X_n) est une suite de variables aléatoires indépendantes de même loi $\mathcal{B}(p)$. Alors,

$$\frac{\sum_{k=1}^{n} X_k - np}{\sqrt{n}} \xrightarrow{(d)} \mathcal{N}(0, p(1-p))$$

Lemme 36. Soient X et Y deux variables aléatoires indépendantes telles que $X \sim \Gamma(a,\gamma)$ et $Y \sim \Gamma(b,\gamma)$. Alors $Z = X + Y \sim \Gamma(a+b,\gamma)$.

p. 180

Application 37 (Formule de Stirling)**.**

$$n! \sim \sqrt{2n\pi}\left(\frac{n}{e}\right)^n$$

p. 556

Proposition 38. Soit $f : \mathbb{R}^+ \to \mathbb{R}$ une fonction continue par morceaux et décroissante, telle que l'intégrale $\int_0^{+\infty} f(t)\,\mathrm{d}t$ converge et est non nulle. Alors, $\sum_{n=1}^{+\infty} f(nt)$ converge et,

$$\sum_{n=1}^{+\infty} f(nt) \sim \frac{1}{t}\sum_{n=0}^{+\infty} f(t)\,\mathrm{d}t$$

[GOU20] p. 159

Exemple 39.

$$\sum_{n=1}^{+\infty} x^{n^2} \sim \frac{c}{\sqrt{-\ln(x)}} \sim \frac{c}{\sqrt{1-x}}$$

où $c = \int_0^{+\infty} e^{-u^2}\,\mathrm{d}u = \frac{\sqrt{\pi}}{2}$.

2. Fonctions définies par une intégrale

Théorème 40. Soient $[a,b[$ un intervalle semi-ouvert de $\mathbb{R}$ (avec $-\infty < a < b \leq +\infty$), E un espace de Banach sur $\mathbb{R}$, $f : [a,b[\to E$ et $g : [a,b[\to \mathbb{R}_*^+$ deux applications continues par morceaux sur $[a,b[$. p. 163

(i) Si $\int_a^b g(t)\,\mathrm{d}t$ diverge, alors quand $x \to b^-$,
- Si $f(t) = O(g(t))$, alors $\int_a^x f(t)\,\mathrm{d}t = O\left(\int_a^x g(t)\,\mathrm{d}t\right)$.
- Si $f(t) = o(g(t))$, alors $\int_a^x f(t)\,\mathrm{d}t = o\left(\int_a^x g(t)\,\mathrm{d}t\right)$.
- Si $f(t) \sim g(t)$, alors $\int_a^x f(t)\,\mathrm{d}t \sim \int_a^x g(t)\,\mathrm{d}t$.

(ii) Si $\int_a^b g(t)\,\mathrm{d}t$ converge, alors quand $x \to b^-$,
- Si $f(t) = O(g(t))$, alors $\int_x^b f(t)\,\mathrm{d}t = O\left(\int_x^b g(t)\,\mathrm{d}t\right)$.
- Si $f(t) = o(g(t))$, alors $\int_x^b f(t)\,\mathrm{d}t = o\left(\int_x^b g(t)\,\mathrm{d}t\right)$.
- Si $f(t) \sim g(t)$, alors $\int_x^b f(t)\,\mathrm{d}t \sim \int_x^b g(t)\,\mathrm{d}t$.

Exemple 41. Lorsque $x \to +\infty$:

$$\ln x = \int_1^x \frac{1}{t}\,\mathrm{d}t = o\left(\int_1^x t^{\alpha-1}\,\mathrm{d}t\right) = o(x^\alpha)$$

pour tout $\alpha > 0$.

Application 42. Soient $a \in \mathbb{R}$ et $g : [a,+\infty[\to \mathbb{R}$ une application de classe $\mathscr{C}^1$. On suppose que g ne s'annule pas au voisinage de $+\infty$ et que lorsque $x \to +\infty$, on a

$$\frac{g'(x)}{g(x)} \sim \frac{\mu}{x}$$

pour $\mu \notin \{-1, 0\}$. Alors,

(i) Si $\mu > -1$, $\int_a^{+\infty} g(t)\,\mathrm{d}t$ diverge et $\int_a^x g(t)\,\mathrm{d}t \sim \frac{xg(x)}{\mu+1}$ quand $x \to +\infty$.

(ii) Si $\mu < -1$, $\int_a^{+\infty} g(t)\,\mathrm{d}t$ converge et $\int_x^{+\infty} g(t)\,\mathrm{d}t \sim -\frac{xg(x)}{\mu+1}$ quand $x \to +\infty$.

Exemple 43. Lorsque $x \to +\infty$: p. 173

$$\int_2^x \frac{\mathrm{d}t}{\ln(t)} = \sum_{i=1}^{k} \frac{x}{\ln(x)^i}(i-1)! + o\left(\frac{x}{\ln(x)^k}\right)$$

Proposition 44. La fonction Γ définie pour tout $x > 0$ par $\Gamma(x) = \int_0^{+\infty} t^{x-1}e^{-t}\,\mathrm{d}t$ vérifie : **[ROM21]** p. 364

(i) $\forall x \in \mathbb{R}_*^+, \Gamma(x+1) = x\Gamma(x)$.

(ii) $\Gamma(1) = 1$.

(iii) Γ est log-convexe sur $\mathbb{R}_*^+$.

De plus,

$$\forall x \in]0,1], \Gamma(x) = \lim_{n\to+\infty} \frac{n^x n!}{(x+n)\dots(x+1)x}$$

(que l'on peut étendre à $\mathbb{R}_*^+$ entier).

Théorème 45 (Formule de Stirling généralisée)**.**

[GOU20] p. 166

$$\Gamma(x) \sim \sqrt{2\pi x}\left(\frac{x}{e}\right)^x$$

226 Suites vectorielles et réelles définies par une relation de récurrence $u_{n+1} = f(u_n)$. Exemples. Applications à la résolution approchée d'équations.

I - Suites récurrentes

1. Définition et premières propriétés

Définition 1. Soit E un ensemble. On dit qu'une suite (u_n) d'éléments de E est **récurrente** d'ordre $h \in \mathbb{N}^*$ si on peut écrire

$$\forall n \geq h,\ u_{n+h} = f(u_{n-1}, \dots, u_{n-h}) \qquad (*)$$

où $f : E^h \to E$ et les premières valeurs $u_0, \dots, u_{h-1} \in E$ étant donnés.

[DAN] p. 145

Exemple 2. On considère la suite numérique (u_n) définie par

$$\begin{cases} u_0 = 0 \\ u_1 = -1 \\ \forall n \in \mathbb{N},\ u_{n+2} = 5u_{n+1} - 6u_n \end{cases}$$

et on a,

$$\forall n \in \mathbb{N},\ u_n = 2^n - 3^n$$

Exemple 3. On considère les suite numérique (u_n) et (v_n) définies par

$$\begin{cases} u_0 \geq 0 \\ \forall n \in \mathbb{N},\ u_{n+1} = \sqrt{\frac{1+u_n}{2}} \end{cases} \quad \text{et } \forall n \in \mathbb{N},\ v_n = \prod_{k=0}^{n} u_k$$

Alors, pour $u_0 = \cos(\theta)$, on a

$$\forall n \in \mathbb{N},\ v_n = \prod_{k=1}^{n} \cos\left(\frac{\theta}{2^k}\right) = \frac{\sin(\theta)}{2^n \sin\left(\frac{\theta}{2^n}\right)}$$

donc

$$\lim_{n \to +\infty} v_n = \frac{\sin(\theta)}{\theta}$$

[GOU20] p. 206

Application 4 (Formule de Viète)**.**

$$\frac{2}{\pi} = \sqrt{\frac{1}{2}} \times \sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2}}} \times \dots$$

Exemple 5. La suite de fonctions polynômiales (P_n) définie par récurrence par : [FGN3] p. 160

$$P_0 : z \mapsto 1, P_1 : z \mapsto z, \text{ et } \forall n \geq 1, zP_n : z \mapsto P_{n-1}(z) - P_{n+1}(z)$$

est une suite bornée si et seulement si $z = \pm 1$.

Théorème 6. Soit (E, d) un espace métrique compact. Soit (u_n) une suite de E telle que $d(u_n, u_{n-1}) \longrightarrow 0$. Alors l'ensemble Γ des valeurs d'adhérence de (u_n) est connexe. [I-P] p. 116

Corollaire 7 (Lemme de la grenouille)**.** Soient $f : [0,1] \to [0,1]$ continue et (x_n) une suite de $[0,1]$ telle que

$$\begin{cases} x_0 \in [0,1] \\ x_{n+1} = f(x_n) \end{cases}$$

Alors (x_n) converge si et seulement si $\lim_{n\to+\infty} x_{n+1} - x_n = 0$.

2. Récurrences classiques

Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. On fixe (u_n) une suite récurrente d'ordre 1 définie par $u_{n+1} = f(u_n)$ où $f : \mathbb{K} \to \mathbb{K}$. [GOU20] p. 201

Définition 8.
- Si f est une translation (ie. f est de la forme $f : x \mapsto x + b$ où $b \in \mathbb{K}$), alors (u_n) est une suite **arithmétique** de raison b.
- Si f est linéaire (ie. f est de la forme $f : x \mapsto ax$ où $a \in \mathbb{K}$), alors (u_n) est une suite **géométrique** de raison a.
- Si f est affine (ie. f est de la forme $f : x \mapsto ax + b$ où $a, b \in \mathbb{K}$), alors (u_n) est une suite **arithmético-géométrique**.
- Si f est homographique (ie. f est de la forme $f : x \mapsto \frac{ax+b}{cx+d}$ où $a, b, c, d \in E$ et $ad - bc \neq 0$), alors (u_n) vérifie une **récurrence homographique**.

Proposition 9.
(i) Si (u_n) est arithmétique de raison b, alors $\forall n \in \mathbb{N}$, $u_n = u_0 + nb$.
(ii) Si (u_n) est géométrique de raison a, alors $\forall n \in \mathbb{N}$, $u_n = a^n u_0$.
(iii) Si (u_n) est arithmético-géométrique et si $1 - a \neq 0$, en posant $r = (1-a)^{-1} b$, on a $\forall n \in \mathbb{N}$, $u_n = a^n(u_0 - r) + r$.

Proposition 10. Supposons que (u_n) vérifie une récurrence homographique. On considère l'équation

$$f(x) = x \iff cx^2 - (a-d)x - b = 0 \qquad (E)$$

Alors :

1. Si (E) admet deux racines distinctes r_1 et r_2, on a $\forall n \in \mathbb{N}$, $\frac{u_n - r_1}{u_n - r_2} = k^n \frac{u_0 - r_1}{u_0 - r_2}$ où $k = \frac{a - r_1 c}{a - r_2 c}$.
2. Si (E) admet une racine double r, on a $\forall n \in \mathbb{N}$, $\frac{1}{u_n - r} = \frac{1}{u_0 - r} + kn$ où $k = \frac{c}{a - rc}$.

Remarque 11. Ces formules permettent de décider s'il existe un rang n tel que le dénominateur de f s'annule, auquel cas les termes ultérieurs de la suite ne sont pas définis.

Exemple 12. Pour la relation $u_{n+1} = \frac{2u_n + 1}{u_n + 2}$, l'équation (E) admet ± 1 pour solutions, donc $\frac{u_n + 1}{u_n - 1} = 3^n \frac{u_0 + 1}{u_0 - 1}$.

3. Suites récurrentes vectorielles

Proposition 13 (Déterminant circulant)**.** Soient $n \in \mathbb{N}^*$ et $a_1, \dots, a_n \in \mathbb{C}$. On pose $\omega = e^{\frac{2i\pi}{n}}$. Alors

$$\begin{vmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \dots & a_0 \end{vmatrix} = \prod_{j=0}^{n-1} P(\omega^j)$$

où $P = \sum_{k=0}^{n-1} a_k X^k$.

[GOU21] p. 153

[DEV]

Application 14 (Suite de polygones)**.** Soit P_0 un polygone dont les sommets sont $\{z_{0,1}, \dots, z_{0,n}\}$. On définit la suite de polygones (P_k) par récurrence en disant que, pour tout $k \in \mathbb{N}^*$, les sommets de P_{k+1} sont les milieux des arêtes de P_k.

Alors la suite (P_k) converge vers l'isobarycentre de P_0.

[I-P] p. 389

II - Outils pour étudier les suites récurrentes

1. Stabilité de l'intervalle et continuité

Soient $I \subseteq \mathbb{R}$ un intervalle de $\mathbb{R}$. On fixe (u_n) une suite récurrente d'ordre 1 définie par $u_{n+1} = f(u_n)$ où $f : I \to \mathbb{R}$.

[AMR11] p. 38

Théorème 15 (Caractérisation séquentielle de la continuité)**.** En reprenant les notations précédentes, une fonction $g : I \to \mathbb{R}$ est continue si et seulement si pour toute suite réelle convergente $(v_n) \in I^{\mathbb{N}}$ dont on note ℓ la limite, $g(v_n) \longrightarrow_{n\to+\infty} \ell$.

Corollaire 16. Si une suite récurrente d'ordre 1 (dont on note f la fonction) converge vers ℓ, alors $f(\ell) = \ell$.

Exemple 17. La suite (u_n) définie par $u_0 \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$ et $\forall n \geq 1$, $u_{n+1} = \sin(u_n)$ converge vers 0.

Proposition 18. (i) Si f est croissante, alors (u_n) est monotone et son sens de monotonie est donnée par le signe de $u_1 - u_0$.

(ii) Si f est décroissante, alors (u_{2n}) et (u_{2n+1}) sont monotones et leur sens de monotonie est opposé.

[GOU20] p. 200

Exemple 19. La suite réelle (u_n) définie par récurrence par :

$$u_0 \in [0,1[\text{ et } \forall n \geq 0,\ u_{n+1} = \frac{1}{2-\sqrt{u_n}}$$

est une suite qui converge vers 1.

2. Équation caractéristique

Définition 20. Une suite (u_n) à valeurs dans $\mathbb{C}$ vérifie une **récurrence linéaire homogène** d'ordre h si

$$\forall n \in \mathbb{N}, \quad u_{n+h} = a_{h-1}u_{n+h-1} + \cdots + a_0 u_0 \qquad (*)$$

où $a_1, \ldots, a_h \in \mathbb{C}$.

Proposition 21. Si on note $r_1, \ldots, r_q$ les racines du polynôme caractéristique de $(*)$ (de multiplicités respectives $\alpha_1, \ldots, \alpha_q$), alors l'ensemble des suites vérifiant $(*)$ est l'ensemble des suites (u_n) telles que :

$$u_n = P_1(n)r_1^n + \cdots + P_q(n)r_q^n$$

où $\forall i \in [\![1, q]\!]$, P_i est un polynôme de degré strictement inférieur à α_i.

Exemple 22. Soit (u_n) la suite définie par $\forall n \in \mathbb{N}$, $u_n = au_{n-1} + bu_{n-2}$. Son polynôme caractéristique est $P = X^2 - aX - b$.

1. Si P a deux racines distinctes r_1 et r_2, alors $\forall n \in \mathbb{N}$, $u_n = \lambda r_1^n + \mu r_2^n$ où λ et μ sont tels

que $u_0 = \lambda + \mu$ et $u_1 = \lambda r_1 + \mu r_2$.

2. Si P a une racine double r, alors $\forall n \in \mathbb{N}$, $u_n = (\lambda n + \mu) r^n$ où λ et μ sont tels que $u_0 = \mu$ et $u_1 = (\lambda + \mu) r$.

Exemple 23. Soit (F_n) la suite de Fibonacci définie par $F_0 = 0$, $F_1 = 1$ et $\forall n \geq 2$, $F_n = F_{n-1} + F_{n-2}$. Alors,

$$\forall n \in \mathbb{N}, F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right)$$

[AMR11] p. 47

Exemple 24. La suite (u_n) définie par $u_0 = 1$ et $u_{n+2} = u_n - u_{n+1}$ est à termes positifs si et seulement si $u_1 = \frac{1-\sqrt{5}}{2}$.

3. Développement asymptotique

Définition 25. À toute suite numérique (u_n) on y associe sa suite (v_n) des **moyennes de Cesàro** où

$$\forall n \in \mathbb{N}, v_n = \frac{1}{n} \sum_{k=1}^{n} u_k$$

p. 53

Théorème 26. Si (u_n) converge vers $\ell \in \mathbb{K}$, alors sa suite des moyennes de Cesàro converge vers ℓ. On dit que (u_n) converge **au sens de Cesàro**.

Proposition 27. Soit f une application continue définie au voisinage de 0^+ admettantun développement asymptotique en 0 de la forme $f(x) = x - ax^\alpha + o(x^\alpha)$, où $a > 0$ et $\alpha > 1$. Alors pour $u_0 > 0$ assez petit, la suite (u_n) définie par $u_{n+1} = f(u_n)$ pour $n \in \mathbb{N}$ vérifie

$$u_n \sim \frac{1}{(na(\alpha-1))^{\frac{1}{\alpha-1}}}$$

[FGN3] p. 142

Exemple 28. Si $f = \sin$ et (u_n) est définie par $u_0 \in [0, 2\pi]$ et $\forall n \in \mathbb{N}$, $u_{n+1} = f(u_n)$, on a l'équivalent en $+\infty$:

$$u_n \sim \sqrt{\frac{3}{n}}$$

[GOU20] p. 228

Proposition 29. En reprenant les notations précédentes, on a, pour $u_0 \in \left]0, \frac{\pi}{2}\right]$,

$$u_n = \sqrt{\frac{3}{n}} - \frac{3\sqrt{3}}{10}\frac{\ln(n)}{n\sqrt{n}} + o\left(\frac{\ln(n)}{n\sqrt{n}}\right)$$

Exemple 30. On définit (u_n) par $u_0 \in \mathbb{R}$ et $\forall n \in \mathbb{N}$, $u_{n+1} = u_n + e^{-u_n}$, on a l'équivalent en $+\infty$: [FGN3] p. 148

$$u_n = n + \frac{\ln(n)}{2n} + o\left(\frac{\ln(n)}{n}\right)$$

III - Applications à la résolution approchée d'équations

1. Point fixe et itération

Théorème 31 (Point fixe de Banach)**.** Soient (E, d) un espace métrique complet et $f : E \to E$ une application contractant (ie. $\exists k \in]0,1[$ tel que $\forall x, y \in E$, $d(f(x), f(y)) \leq k d(x, y)$). Alors, [DAN] p. 146

$$\exists! x \in E \text{ tel que } f(x) = x$$

De plus la suite des itérés définie par $x_0 \in E$ et $\forall n \in \mathbb{N}, x_{n+1} = f(x_n)$ converge vers x.

Théorème 32 (Point fixe dans un compact)**.** Soit (E, d) un espace métrique compact et $f : E \to E$ telle que

$$\forall x, y \in E,\ x \neq y \implies d(f(x), f(y)) < d(x, y)$$

alors f admet un unique point fixe et pour tout $x_0 \in E$, la suite des itérés

$$x_{n+1} = f(x_n)$$

converge vers ce point fixe.

Application 33. Soient $a, b \in \mathbb{R}$ et $f : [a, b] \to \mathbb{R}$ dérivable, strictement croissante et telle que $f(a) < 0$, $f(b) > 0$ et $0 < m \leq f'(x) \leq M$ sur $[a, b]$. On pose $\varphi : x \mapsto x - \frac{1}{M} f(x)$. On considère l'équation : [DEM] p. 95

$$f(x) = 0 \iff \varphi(x) = x \qquad (E)$$

Alors :

(i) (E) admet une unique solution x et pour tout point initial $x_0 \in [a, b]$, la suite des itérés (x_n) définie par $\forall n \in \mathbb{N}$, $x_{n+1} = \varphi(x_n)$ converge vers x.

(ii) La vitesse de convergence est estimée par la suite géométrique $\left(1 - \frac{m}{M}\right)$: il faut que les bornes m et M soient proches.

Remarque 34. Cela marche aussi dans le cas où $f(a) > 0$, $f(b) < 0$ et $-M \leq f'(x) \leq -m < 0$ (il suffit alors de changer f en $-f$).

Définition 35. Soient I un intervalle fermé de $\mathbb{R}$ et $\varphi : I \to I$ une application de classe $\mathscr{C}^1$. Soit $a \in I$ un point fixe de φ.

— Si $|\varphi'(a)| < 1$, on dit que a est **attractif**. Si de plus $\varphi'(a) = 0$, a est **superattractif**.

— Si $|\varphi'(a)| > 1$, on dit que a est **répulsif**.

Proposition 36. On reprend les notations précédentes et on considère la suite des itérés (x_n) (avec $x_0 \in I$ et $\forall n \in \mathbb{N}$, $x_{n+1} = \varphi(x_n)$). Alors :

(i) Si a est attractif, (x_n) converge à une vitesse géométrique :

$$|x_n - a| \leq k^n |x_0 - a|$$

(ii) Si a est superattractif et φ est $\mathscr{C}^2$ telle que $|\varphi''| < M$ sur I, alors la vitesse de convergence est hypergéométrique :

$$|x_n - a| \leq \frac{2}{M} 10^{-2^n}$$

(iii) Si a est répulsif, il existe $h > 0$ tel que $\varphi_{|[a-h,a+h]}$ admette une application réciproque φ^{-1} définie sur $\varphi([a-h, a+h])$ et le point a est attractif pour φ^{-1}.

Exemple 37. Soit $f : x \mapsto x^3 - 4x + 1$. On pose $\varphi : x \mapsto \frac{1}{4}(x^3 + 1)$ et on considère

$$f(x) = 0 \iff \varphi(x) = x \qquad (E)$$

Alors (E) possède trois solutions réelles $a_1 < a_2 < a_3$ telles que :

— $a_1 \in]-2,5; -2[$.

— $a_2 \in]0; 0,5[$ et a_2 est attractif.

— $a_3 \in]1,5; 2[$.

2. Méthode de Newton

[DEV]

Théorème 38 (Méthode de Newton)**.** Soit $f : [c,d] \to \mathbb{R}$ une fonction de classe $\mathscr{C}^2$ strictement croissante sur $[c,d]$. On considère la fonction

$$\varphi : \begin{array}{ccc} [c,d] & \to & \mathbb{R} \\ x & \mapsto & x - \frac{f(x)}{f'(x)} \end{array}$$

(qui est bien définie car $f' > 0$). Alors :

[ROU] p. 152

(i) $\exists! a \in [c,d]$ tel que $f(a) = 0$.

(ii) $\exists \alpha > 0$ tel que $I = [a-\alpha, a+\alpha]$ est stable par φ.

(iii) La suite (x_n) des itérés (définie par récurrence par $x_{n+1} = \varphi(x_n)$ pour tout $n \geq 0$) converge quadratiquement vers a pour tout $x_0 \in I$.

Corollaire 39. En reprenant les hypothèses et notations du théorème précédent, et en supposant de plus f strictement convexe sur $[c,d]$, le résultat du théorème est vrai sur $I = [a,d]$. De plus :

(i) (x_n) est strictement décroissante (ou constante).

(ii) $x_{n+1} - a \sim \frac{f''(a)}{2f'(a)}(x_n - a)^2$ pour $x_0 > a$.

Exemple 40.
— On fixe $y > 0$. En itérant la fonction $F : x \mapsto \frac{1}{2}\left(x + \frac{y}{x}\right)$ pour un nombre de départ compris entre c et d où $0 < c < d$ et $c^2 < 0 < d^2$, on peut obtenir une approximation du nombre $\sqrt{y}$.

— En itérant la fonction $F : x \mapsto \frac{x^2+1}{2x-1}$ pour un nombre de départ supérieur à 2, on peut obtenir une approximation du nombre d'or $\varphi = \frac{1+\sqrt{5}}{2}$.

Exemple 41. La méthode de Newton appliquée à la fonction $x \mapsto x^3 - 4x + 1$ dans le but d'approximer ses zéros donne :

[DEM] p. 102

x_0	-2	0	2
x_1	$-2,125$	$0,25$	$1,875$
x_2	$-2,114975450$	$0,254098361$	$1,860978520$
x_3	$-2,114907545$	$0,254101688$	$1,860805877$
x_4	$-2,114907541$	$= x_3$	$1,860805853$
x_5	$= x_4$		$= x_4$

3. Généralisation à $\mathbb{R}^m$

p. 110

Théorème 42 (Méthode de Newton-Raphson)**.** Soit $f : \Omega \to \mathbb{R}^m$ (où $\Omega \subset \mathbb{R}^m$ est un ouvert) de classe $\mathscr{C}^1$ telle que $f(a) = 0$. On suppose que $\mathrm{d}f_a$ est inversible. Alors il existe un voisinage U de a dans Ω tel que $\varphi : x \mapsto x - (\mathrm{d}f_x)^{-1}(f(x))$ soit bien définie sur U et la suite des itérés $x_{n+1} = \varphi(x_n)$ converge quadratiquement vers a.

Exemple 43. On considère le système

$$\begin{cases} x^2 + xy - 2y^2 = 4 \\ xe^x + ye^y = 0 \end{cases} \qquad (S)$$

On pose $X_0 = \begin{pmatrix} -2 \\ 0,2 \end{pmatrix}$ et $\Delta(x,y) = (2x+y)(y+1)e^y - (x-4y)(x+1)e^x$ ainsi que :

$$\varphi\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} - \frac{1}{\Delta(x,y)} \begin{pmatrix} (y+1)e^y & -x+4y \\ -(x+1)e^x & 2x+y \end{pmatrix} \begin{pmatrix} x^2+xy-2y^2-4 \\ xe^x+ye^y \end{pmatrix}$$

Alors la suite des itérés $(X_n) = \begin{pmatrix} x_n \\ y_n \end{pmatrix}$ converge vers l'unique solution de (S) et on a :

n	x_n	y_n
0	-2	$0,2$
1	$-2,130690999$	$0,205937784$
2	$-2,126935837$	$0,206277868$
3	$-2,126932304$	$0,206278156$

Annexes

[I-P]
p. 389

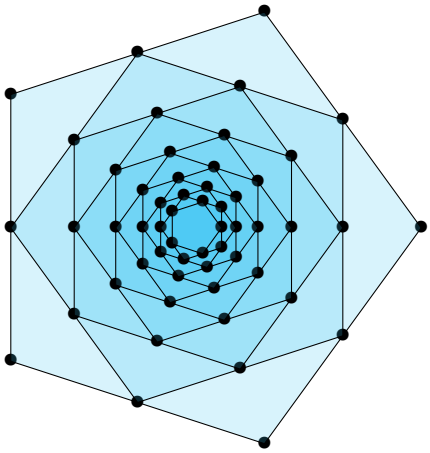


FIGURE I.25 – La suite de polygones.

228 Continuité, dérivabilité des fonctions réelles d'une variable réelle. Exemples et applications.

Soient I un intervalle de $\mathbb{R}$ non réduit à un point et $f : I \to \mathbb{R}$ une fonction.

I - Continuité et dérivabilité

1. Continuité

Définition 1. — f est **continue au point** $a \in I$ si

$$\forall \epsilon > 0, \exists \eta > 0, \forall x \in I, |x-a| < \eta \implies |f(x)-f(a)| < \epsilon$$

— f est **continue sur** I si f est continue en tout point de I.

[ROM19-1] p. 163

Exemple 2. Pour tout entier n, $x \mapsto x^n$ est continue sur $\mathbb{R}$.

Théorème 3 (Caractérisations séquentielle et topologique de la continuité)**.** (i) f est continue en $a \in I$ si et seulement si toute suite de points de I qui converge vers a est transformée par f en une suite convergente vers $f(a)$.

(ii) f est continue en $a \in I$ si et seulement si l'image réciproque par f de tout ouvert (resp. fermé) de $\mathbb{R}$ est un ouvert (resp. fermé) de I.

Exemple 4. La fonction $x \mapsto \cos\left(\frac{1}{x}\right)$ définie sur $\mathbb{R}_*$ n'est pas continue en 0.

Proposition 5. Si f et g sont deux fonctions définies sur I à valeurs réelles et continues en $a \in I$, alors $|f|$, $f+g$, fg, $\min(f,g)$ et $\max(f,g)$ sont continues en a.

2. Uniforme continuité

Définition 6. f est **uniformément continue sur** I si

$$\forall \epsilon > 0, \exists \eta > 0, \forall x, y \in I, |x-y| < \eta \implies |f(x)-f(y) < \epsilon$$

[GOU20] p. 12

Remarque 7. En particulier, une fonction uniformément continue sur un intervalle est continue sur ce même intervalle.

Exemple 8. Une fonction lipschitzienne sur I est uniformément continue sur I.

Contre-exemple 9. La fonction $x \mapsto \frac{1}{x}$ définie sur $]0,1]$ est continue mais n'est pas uniformément continue.

Proposition 10. On se place dans le cas où $I = \mathbb{R}^+$ et on suppose f uniformément continue sur $\mathbb{R}^+$. Alors,

$$\exists \alpha, \beta \in \mathbb{R}_*^+ \text{ tels que } \forall x \in \mathbb{R}^+, |f(x)| \leq \alpha x + \beta$$

p. 18

Théorème 11 (Prolongement des applications uniformément continues)**.** Soit $J \subseteq I$ dense dans I et soit $g : J \to \mathbb{R}$ uniformément continue sur J. Alors,

$$\exists ! h : I \to \mathbb{R} \text{ uniformément continue et telle que } h_{|J} = g$$

p. 24

3. Dérivabilité

Définition 12. On dit que f est **dérivable en** $a \in I$ si

$$\lim_{\substack{t \to a \\ t \neq a}} \frac{f(t) - f(a)}{t - a}$$

existe. Lorsque cette limite existe, elle est notée $f'(a)$.

p. 71

Remarque 13.
- De même, f est **dérivable à gauche (resp. à droite) en** $a \in I$ si $\lim_{\substack{t \to a \\ t<a \\ t \in I}} \frac{f(t)-f(a)}{t-a}$ existe (resp. $\lim_{\substack{t \to a \\ t>a \\ t \in I}} \frac{f(t)-f(a)}{t-a}$ existe). On la note alors $f'_g(a)$ (resp. $f'_d(a)$).
- f est dérivable en $a \in I$ si et seulement si f est dérivable à gauche, à droite et $f'_g(a) = f'_d(a)$.
- f est dérivable en $a \in I$ si et seulement si, quand x tend vers a,

$$\exists \ell \in \mathbb{R}, f(x) = f(a) + (x-a)\ell + o(x-a)$$

Proposition 14. Si f est dérivable en $a \in I$, alors f est continue en a.

Contre-exemple 15. On note Δ la fonction définie sur $\mathbb{R}$ 1-périodique et telle que la restriction à $\left[-\frac{1}{2}, \frac{1}{2}\right]$ vérifie $\Delta(x) = |x|$. Alors,

$$f : x \mapsto \sum_{p=0}^{+\infty} \frac{1}{2^p} \Delta(2^p x)$$

p. 86

est bien définie, continue sur $\mathbb{R}$, mais dérivable en aucun point de $\mathbb{R}$.

Remarque 16. La fonction dérivée $f' : x \mapsto f'(x)$ n'est pas forcément continue là où elle est définie.

p. 72

Exemple 17. La fonction $x \mapsto \begin{cases} x^2 \sin\left(\frac{1}{x}\right) \text{ si x } \neq 0 \\ 0 \text{ sinon} \end{cases}$ définie sur $\mathbb{R}$ est dérivable, de dérivée $x \mapsto \begin{cases} 2x \sin\left(\frac{1}{x}\right) - \cos\left(\frac{1}{x}\right) \text{ si x } \neq 0 \\ 0 \text{ sinon} \end{cases}$ définie sur $\mathbb{R}$ mais non continue en 0.

Proposition 18. Si f et g sont deux fonctions définies sur I à valeurs réelles et dérivables en $a \in I$. Alors :

(i) $\forall \lambda, \mu \in \mathbb{R}$, $\lambda f + \mu g$ est dérivable en a et $(\lambda f + \mu g)'(a) = \lambda f'(a) + \mu g'(a)$.

(ii) fg est dérivable en a et $(fg)'(a) = f'(a)g(a) + f(a)g'(a)$.

(iii) Si $g(a) \neq 0$, alors $\frac{f}{g}$ est dérivable en a et $\left(\frac{f}{g}\right)'(a) = \frac{f'(a)g(a) - f(a)g'(a)}{g(a)^2}$.

Définition 19. On dit que f est **de classe $\mathscr{C}^n$ sur** I si $\forall k \in [\![0, n]\!]$, $f^{(k)}$ (la dérivée k-ième de f) existe et continue.

Proposition 20 (Formule de Leibniz)**.** Soit $a \in I$. Si f et g sont deux fonctions définies sur I à valeurs réelles et qui admettent une dérivée n-ième en a,

$$(fg)^{(n)}(a) = \sum_{k=0}^{n} \binom{n}{k} f^{(k)}(a) g^{(n-k)}(a)$$

Proposition 21. Soit J un intervalle de $\mathbb{R}$. Si $f : I \to \mathbb{R}$ et $g : J \to I$ sont deux fonctions, alors, en supposant f dérivable en a et g dérivable en $f(a)$, $(f \circ g)$ est dérivable en a et,

$$(f \circ g)'(a) = g'(a)(f' \circ g)(a)$$

Corollaire 22. Soient J un intervalle de $\mathbb{R}$ et $h : I \to J$ une bijection dérivable en $a \in I$. Alors, h^{-1} est dérivable en $b = h(a)$ si et seulement si $h'(a) \neq 0$, et on a,

$$(h^{-1})'(b) = \frac{1}{h'(a)} = \frac{1}{h'(h^{-1}(b))}$$

Corollaire 23. La composée de deux applications de classe $\mathscr{C}^n$ est de classe $\mathscr{C}^n$.

II - Fonctions particulières qui sont dérivables ou continues

1. Fonctions convexes

Définition 24. f est **convexe** si

$$\forall x, y \in I,\ \forall t \in [0,1],\ f((1-t)x + ty) \leq (1-t)f(x) + tf(y)$$

[ROM19-1] p. 225

Exemple 25.
— $x \mapsto |x|$ est convexe sur $\mathbb{R}$.
— exp est convexe sur $\mathbb{R}$.

Proposition 26. Si f est convexe, elle possède en tout point de $\mathring{I}$ une dérivée à droite et une dérivée à gauche. Elle est donc continue sur $\mathring{I}$. De plus les applications dérivées à gauche f'_g et à droite f'_d sont croissantes avec $f'_g(x) \leq f'_d(x)$ pour tout $x \in \mathring{I}$.

[GOU20] p. 96

Proposition 27. On suppose f deux fois dérivable. Alors, f est convexe si et seulement si $f''(x) \geq 0$ pour tout $x \in I$.

[DEV]

Application 28 (Méthode de Newton)**.** Soit $g : [c,d] \to \mathbb{R}$ une fonction de classe $\mathscr{C}^2$ strictement croissante sur $[c,d]$. On considère la fonction

$$\varphi : \begin{array}{ccc} [c,d] & \to & \mathbb{R} \\ x & \mapsto & x - \frac{g(x)}{g'(x)} \end{array}$$

(qui est bien définie car $g' > 0$). Alors :

(i) $\exists! a \in [c,d]$ tel que $g(a) = 0$.

(ii) $\exists \alpha > 0$ tel que $I = [a-\alpha, a+\alpha]$ est stable par φ.

(iii) La suite (x_n) des itérés (définie par récurrence par $x_{n+1} = \varphi(x_n)$ pour tout $n \geq 0$) converge quadratiquement vers a pour tout $x_0 \in I$.

[ROU] p. 152

Corollaire 29. En reprenant les hypothèses et notations du théorème précédent, et en supposant de plus g strictement convexe sur $[c,d]$, le résultat du théorème est vrai sur $I = [a,d]$. De plus :

(i) (x_n) est strictement décroissante (ou constante).

(ii) $x_{n+1} - a \sim \frac{f''(a)}{2f'(a)}(x_n - a)^2$ pour $x_0 > a$.

Exemple 30. — On fixe $y > 0$. En itérant la fonction $F : x \mapsto \frac{1}{2}\left(x + \frac{y}{x}\right)$ pour un nombre de départ compris entre c et d où $0 < c < d$ et $c^2 < 0 < d^2$, on peut obtenir une approximation du nombre $\sqrt{y}$.

— En itérant la fonction $F : x \mapsto \frac{x^2+1}{2x-1}$ pour un nombre de départ supérieur à 2, on peut obtenir une approximation du nombre d'or $\varphi = \frac{1+\sqrt{5}}{2}$.

2. Fonction monotones

Définition 31. — On dit que f est **croissante** si $\forall x, y \in I,\ x \leq y \implies f(x) \leq f(y)$.

— On dit que f est **décroissante** si $\forall x, y \in I,\ x \leq y \implies f(x) \geq f(y)$.

— On dit que f est **monotone** si f est croissante ou décroissante.

[R-R] p. 31

Définition 32. Si $a \in \mathring{I}$, et si f est discontinue en a avec des limites à gauche et à droite en ce point, on dit que f a une **discontinuité de première espèce** en a.

[ROM19-1] p. 163

Proposition 33. Une fonction monotone de I dans $\mathbb{R}$ ne peut avoir que des discontinuités de première espèce.

Théorème 34. On suppose que I est un intervalle ouvert. Si f est une fonction monotone, alors l'ensemble des points de discontinuités de f est dénombrable.

Exemple 35. La fonction f définie sur $[0,1]$ par $f(0) = 0$ et $f(x) = \frac{1}{\lfloor \frac{1}{x} \rfloor}$ est croissante avec une infinité de points de discontinuité.

Proposition 36. Si f est une fonction monotone telle que $f(I)$ est un intervalle, elle est alors continue sur I.

p. 175

Théorème 37 (Bijection)**.** Si f est une application continue et strictement monotone sur I, alors :

(i) $f(I)$ est un intervalle.

(ii) f^{-1} est continue.

(iii) f^{-1} est strictement monotone de même sens de variation que f.

Exemple 38. La fonction $\exp : x \mapsto e^x$ est une bijection de $\mathbb{R}$ dans $\mathbb{R}_*^+$ qui admet donc une bijection réciproque ln qui est strictement croissante.

Théorème 39 (Lebesgue)**.** Une application monotone est dérivable presque partout. [D-L] p. 405

III - Propriétés importantes

1. Théorème des valeurs intermédiaires

Théorème 40 (Des valeurs intermédiaires)**.** On suppose f continue sur I. Alors $f(I)$ est un intervalle. [GOU20] p. 41

Remarque 41. Une autre manière d'écrire ce résultat est la suivante. Si $f(a) \leq f(b)$ (resp. $f(a) \geq f(b)$) avec $a < b$, alors pour tout $f(a) \leq \gamma \leq f(b)$ (resp. $f(b) \leq \gamma \leq f(a)$), il existe $c \in [a,b]$ tel que $f(c) = \gamma$.

Corollaire 42. L'image d'un segment de $\mathbb{R}$ par f est un segment de $\mathbb{R}$.

2. Théorème de Rolle

Dans cette partie, I désigne un segment $[a,b]$ de $\mathbb{R}$ non réduit à un point.

Théorème 43 (Rolle)**.** On suppose f continue sur $[a,b]$, dérivable sur $]a,b[$ et telle que $f(a) = f(b)$. Alors,

$$\exists c \in]a,b[\text{ tel que } f'(c) = 0$$

Théorème 44 (Des accroissements finis)**.** On suppose f continue sur $[a,b]$ et dérivable sur $]a,b[$. Alors,

$$\exists c \in]a,b[\text{ tel que } f'(c) = \frac{f(b)-f(a)}{b-a}$$

Corollaire 45. On suppose f continue sur $[a,b]$ et dérivable sur $]a,b[$. Alors, f est croissante si et seulement si $f'(x) \geq 0$ pour tout $x \in]a,b[$, avec égalité si et seulement si f est constante.

Corollaire 46. On suppose f continue sur $[a,b[$ et dérivable sur $]a,b[$ et telle que $\ell = \lim_{\substack{t \to a \\ t>a}} f'(t)$ existe. Alors, f est dérivable en a et $f'(a) = \ell$.

Théorème 47 (Darboux)**.** On suppose f dérivable sur I. Alors $f'(I)$ est un intervalle. p. 80

3. Formules de Taylor

Dans cette partie, I désigne encore un segment $[a,b]$ de $\mathbb{R}$ non réduit à un point.

p. 75

Théorème 48 (Formule de Taylor-Lagrange)**.** On suppose f de classe $\mathscr{C}^n$ sur $[a,b]$ telle que $f^{(n+1)}$ existe sur $]a,b[$. Alors,

$$\exists c \in]a,b[\text{ tel que } f(b) = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(b-a)^k + \frac{f^{(n+1)}(c)}{(n+1)!}(b-a)^{n+1}$$

Application 49.
— $\forall x \in \mathbb{R}^+,\ x - \frac{x^2}{2} \leq \ln(1+x) \leq x - \frac{x^2}{2} + \frac{x^3}{3}$.
— $\forall x \in \mathbb{R}^+,\ x - \frac{x^3}{6} \leq \sin(x) \leq x - \frac{x^3}{6} + \frac{x^5}{120}$.
— $\forall x \in \mathbb{R},\ 1 - \frac{x^2}{2} \leq \cos(x) \leq 1 - \frac{x^2}{2} + \frac{x^4}{24}$.

4. Continuité sur un compact

p. 31

Théorème 50 (des bornes)**.** Une fonction continue sur un compact est bornée et atteint ses bornes.

Théorème 51 (Heine)**.** Une fonction continue sur un compact y est uniformément continue.

p. 242

Théorème 52 (Bernstein)**.** On suppose $I = [0,1]$ et f continue sur $[0,1]$. On note

$$B_n(f) : x \mapsto \sum_{k=0}^{n} f\left(\frac{k}{n}\right)\binom{n}{k} x^k (1-x)^{n-k}$$

Alors,

$$\|B_n(f) - f\|_\infty \longrightarrow_{n\to+\infty} 0$$

[DEV]

p. 304

Théorème 53 (Weierstrass)**.** Toute fonction continue sur un compact est limite uniforme de fonctions polynômiales.

IV - Régularité des fonctions limites

1. Suites et séries de fonctions

Proposition 54. Si une suite de fonctions est continue en un point a et converge uniformément vers une fonction limite, alors celle-ci est continue en a.

p. 233

Contre-exemple 55. La suite de fonctions (g_n) définie pour tout $n \in \mathbb{N}$ et pour tout $x \in [0,1]$ par $g_n(x) = x^n$ converge vers une fonction non continue.

Proposition 56. On suppose que I est un segment $[a,b]$ de $\mathbb{R}$ non réduit à un point. Soit (f_n) une suite de fonctions de I dans $\mathbb{R}$. On suppose que :

(i) Il existe $x_0 \in [a,b]$ tel que $(f_n(x_0))$ converge.

(ii) La suite (f_n') converge uniformément sur $[a,b]$ vers une fonction g.

Alors (f_n) converge uniformément vers une fonction f de classe $\mathscr{C}^1$ sur $[a,b]$ et telle que $f' = g$.

Exemple 57. La fonction $\zeta : s \mapsto \sum_{n=1}^{+\infty} \frac{1}{n^s}$ est $\mathscr{C}^\infty$ sur $]1,+\infty[$.

p. 302

2. Fonctions définies par une intégrale

Soient $(X, \mathscr{A}, \mu)$ un espace mesuré et $g : E \times X \to \mathbb{C}$ où (E,d) est un espace métrique. On pose $G : t \mapsto \int_X g(t,x)\,\mathrm{d}\mu(x)$.

[Z-Q] p. 312

Théorème 58 (Continuité sous le signe intégral)**.** On suppose :

(i) $\forall t \in E$, $x \mapsto g(t,x)$ est mesurable.

(ii) pp. en $x \in X$, $t \mapsto g(t,x)$ est continue en $t_0 \in E$.

(iii) $\exists h \in L_1(X)$ positive telle que

$$|g(t,x)| \leq h(x) \quad \forall t \in E, \text{pp. en } x \in X$$

Alors G est continue en t_0.

Théorème 59 (Dérivation sous le signe intégral)**.** On suppose :

(i) $\forall t \in I$, $x \mapsto g(t,x) \in L_1(X)$.

(ii) pp. en $x \in X$, $t \mapsto g(t,x)$ est dérivable sur I. On notera $\frac{\partial g}{\partial t}$ cette dérivée définie presque partout.

(iii) $\forall K \subseteq I$ compact, $\exists h_K \in L_1(X)$ positive telle que

$$\left|\frac{\partial g}{\partial t}(x,t)\right| \leq h_K(x) \quad \forall t \in I, \text{pp. en } x$$

Alors $\forall t \in I$, $x \mapsto \frac{\partial g}{\partial t}(x,t) \in L_1(X)$ et G est dérivable sur I avec

$$\forall t \in I, G'(t) = \int_X \frac{\partial g}{\partial t}(x,t)\,\mathrm{d}\mu(x)$$

Application 60 (Intégrale de Dirichlet)**.** On pose $\forall x \geq 0$,

[G-K] p. 107

$$F(x) = \int_0^{+\infty} \frac{\sin(t)}{t} e^{-xt}\,\mathrm{d}t$$

alors :

(i) F est bien définie et est continue sur $\mathbb{R}^+$.

(ii) F est dérivable sur $\mathbb{R}_*^+$ et $\forall x \in \mathbb{R}_*^+$, $F'(x) = -\frac{1}{1+x^2}$.

(iii) $F(0) = \int_0^{+\infty} \frac{\sin(t)}{t}\,\mathrm{d}t = \frac{\pi}{2}$.

Annexes

[GOU20] p. 73

Valeur de $f(x)$	**Valeur de** $f'(x)$
x^r $(r \in \mathbb{R})$	rx^{r-1}
$\ln(x)$	$\frac{1}{x}$
$\sin(x)$	$\cos(x)$
$\cos(x)$	$-\sin(x)$
$\tan(x)$	$\frac{1}{\cos(x)^2}$
e^x	e^x
$\arctan(x)$	$\frac{1}{1+x^2}$
$\arcsin(x)$	$\frac{1}{\sqrt{1-x^2}}$
$\arccos(x)$	$-\frac{1}{\sqrt{1-x^2}}$

FIGURE I.26 – Dérivées de fonctions usuelles.

229 Fonctions monotones. Fonctions convexes. Exemples et applications.

I - Fonctions monotones

1. Définition et première propriétés

Définition 1. Soient X une partie de $\mathbb{R}$ et $f : X \to \mathbb{R}$.

— On dit que f est **croissante** si $\forall x, y \in X,\ x \leq y \implies f(x) \leq f(y)$.

— On dit que f est **décroissante** si $\forall x, y \in X,\ x \leq y \implies f(x) \geq f(y)$.

— On dit que f est **monotone** si f est croissante ou décroissante.

[R-R] p. 31

Remarque 2. Les définitions de f **strictement croissante** et f **strictement décroissante** s'obtiennent en remplaçant les inégalités larges par des inégalités strictes dans la définition précédente.

Par conséquent, f est décroissante si et seulement si $-f$ est croissante. Pour cette raison, nous pouvons nous limiter à l'étude des fonctions croissantes.

Exemple 3. $x \mapsto \lfloor x \rfloor$ est une fonction monotone.

Proposition 4. L'ensemble des fonctions croissantes est stable par addition, par multiplication par un scalaire positif et par composition.

[D-L] p. 405

Proposition 5. Soient $I \subseteq \mathbb{R}$ un intervalle non réduit à un point et $f : I \to \mathbb{R}$. On suppose f dérivable sur $\mathring{I}$. Alors f est croissante si et seulement si $f'(x) \geq 0$ pour tout $x \in I$.

[ROM19-1] p. 205

2. Régularité

Soit $I \subseteq \mathbb{R}$ un intervalle non réduit à un point.

p. 162

Définition 6. On dit que $f : I \to \mathbb{R}$ a pour **limite à gauche** (resp. **à droite**) ℓ en $\alpha \in \bar{I}$ si :

$$\forall \epsilon > 0,\ \exists \eta > 0, \text{ tel que } \forall x \in I \cap]\alpha - \eta, \alpha[,\ |f(x) - \ell| < \epsilon$$

(resp. $\forall \epsilon > 0,\ \exists \eta > 0$, tel que $\forall x \in I \cap]\alpha, \alpha + \eta[,\ |f(x) - \ell| < \epsilon$).

Théorème 7. On suppose que I est un intervalle ouvert. Si $f : I \to \mathbb{R}$ est une fonction monotone, elle admet alors une limite à gauche et à droite en tout point. Dans le cas où f est croissante, on a

$$\forall x \in I, \quad f(x^-) = \sup_{\substack{t\in I \\ t<x}} f(t) \leq f(x) \leq f(x^+) = \inf_{\substack{t\in I \\ t>x}} f(t)$$

Définition 8. Si $\alpha \in \mathring{I}$, et si $f : I \to \mathbb{R}$ est discontinue en α avec des limites à gauche et à droite en ce point, on dit que f a une **discontinuité de première espèce** en α.

Proposition 9. Une fonction monotone de I dans $\mathbb{R}$ ne peut avoir que des discontinuités de première espèce.

Théorème 10. On suppose que I est un intervalle ouvert. Si $f : I \to \mathbb{R}$ est une fonction monotone, alors l'ensemble des points de discontinuités de f est dénombrable.

Exemple 11. La fonction f définie sur $[0,1]$ par $f(0) = 0$ et $f(x) = \frac{1}{\lfloor \frac{1}{x} \rfloor}$ est croissante avec une infinité de points de discontinuité.

Proposition 12. Si $f : I \to \mathbb{R}$ est une fonction monotone telle que $f(I)$ est un intervalle, elle est alors continue sur I. p. 175

Théorème 13 (Bijection)**.** Si $f : I \to \mathbb{R}$ est une application continue et strictement monotone, alors :

(i) $f(I)$ est un intervalle.

(ii) f^{-1} est continue.

(iii) f^{-1} est strictement monotone de même sens de variation que f.

Exemple 14. La fonction $\exp : x \mapsto e^x$ est une bijection de $\mathbb{R}$ dans $\mathbb{R}_*^+$ qui admet donc une bijection réciproque ln qui est strictement croissante.

Proposition 15. Soit $f : I \to \mathbb{R}$. Cette fonction f est injective si et seulement si elle est strictement monotone.

Théorème 16 (Lebesgue)**.** Une application monotone est dérivable presque partout. **[D-L]** p. 405

3. Suites et séries

Lemme 17. Une limite simple d'une suite de fonctions croissantes est croissante.

[GOU20] p. 238

Théorème 18 (Second théorème de Dini)**.** Soit (f_n) une suite de fonctions croissantes réelles continues définies sur un segment I de $\mathbb{R}$. Si (f_n) converge simplement vers une fonction continue sur I, alors la convergence est uniforme.

Proposition 19 (Comparaison série - intégrale)**.** Soit $f : \mathbb{R}^+ \to \mathbb{R}^+$ une fonction positive, continue par morceaux et décroissante sur $\mathbb{R}^+$. Alors la suite (U_n) définie par

$$\forall n \in \mathbb{N},\ \sum_{k=0}^{n} f(k) - \int_0^n f(t)\,\mathrm{d}t$$

est convergente. En particulier, la série $\sum f(n)$ et l'intégrale $\int_0^{+\infty} f(t)\,\mathrm{d}t$ sont de même nature.

p. 212

Application 20 (Développement asymptotique de la série harmonique)**.**

$$\sum_{k=1}^{n} \frac{1}{k} = \ln(n) + \gamma + o(1)$$

où γ désigne la constante d'Euler.

II - Fonctions convexes

Soit I une partie convexe d'un espace vectoriel normé $(E, \|.\|)$ non réduite à un point.

1. Définitions

Définition 21.
— I est **convexe** si $\forall a, b \in I,\ [a,b] \subseteq I$.
— Une fonction $f : I \to \mathbb{R}$ est **convexe** si

$$\forall x, y \in I,\ \forall t \in [0,1],\ f((1-t)x + ty) \leq (1-t)f(x) + tf(y)$$

— Une fonction $f : I \to \mathbb{R}$ est **concave** si $-f$ est convexe.

[ROM19-1] p. 225

Remarque 22. Les définitions de f **strictement convexe** et f **strictement concave** s'obtiennent en remplaçant les inégalités larges par des inégalités strictes dans la définition précédente.

Exemple 23. — $x \mapsto \|x\|$ est convexe sur E.
— exp est convexe sur $\mathbb{R}$.

Proposition 24. Une fonction $f : I \to \mathbb{R}$ est convexe si et seulement si son épigraphe est convexe dans $E \times \mathbb{R}$.

Théorème 25. Une fonction $f : I \to \mathbb{R}$ est convexe si et seulement si $\forall x, y \in I$, $t \mapsto f((1-t)x + ty)$ est convexe sur $[0,1]$.

Ce dernier théorème justifie que l'étude des fonctions convexes se ramène à l'étude des fonctions convexes sur un intervalle réel.

Proposition 26. — Une combinaison linéaire à coefficients positifs de fonctions convexes est convexe.
— La composée $\varphi \circ g$ d'une fonction convexe croissante $\varphi : J \to \mathbb{R}$ avec une fonction fonction convexe $g : I \to J$ est croissante.
— Une limite simple d'une suite de fonctions convexes est convexe.

À partir de maintenant, on supposera que I est un intervalle réel non réduit à un point.

2. Propriétés sur $\mathbb{R}$

Remarque 27. Dans le cadre réel, la Théorème 21 revient à dire que les cordes $[(a, f(a)), (b, f(b))]$ sont au-dessus du graphe de f pour tout $a, b \in I$ avec $a < b$. **[GOU20]** p. 95

Proposition 28. Une fonction $f : I \to \mathbb{R}$ est convexe si et seulement si $\forall x_0 \in I$, l'application

$$\begin{array}{ccc} I \setminus \{x_0\} & \to & \mathbb{R} \\ x & \mapsto & \frac{f(x)-f(x_0)}{x-x_0} \end{array}$$

est croissante.

Corollaire 29 (Inégalité des trois pentes)**.** Soient fonction $f : I \to \mathbb{R}$ convexe et $a, b, c \in I$ tels que $a < b < c$. Alors,

$$\frac{f(b)-f(a)}{b-a} < \frac{f(c)-f(a)}{c-a} < \frac{f(c)-f(b)}{c-b}$$

Définition 30. On dit que $f : I \to \mathbb{R}$ est **dérivable à gauche** (resp. **à droite**) en $\alpha \in I$ si la p. 71

limite

$$\lim_{\substack{t\to a^-\\ t\in I}} \frac{f(t)-f(a)}{t-a}$$

(resp. $\lim_{\substack{t\to a^+\\ t\in I}} \frac{f(t)-f(a)}{t-a}$) existe.

Proposition 31. Une fonction $f : I \to \mathbb{R}$ convexe possède en tout point de $\mathring{I}$ une dérivée à droite et une dérivée à gauche. Elle est donc continue sur $\mathring{I}$. De plus les applications dérivées à gauche f'_g et à droite f'_d sont croissantes avec $f'_g(x) \leq f'_d(x)$ pour tout $x \in \mathring{I}$.

p. 96

Théorème 32. Soit $f : I \to \mathbb{R}$ une fonction dérivable sur I. Alors, les assertions suivantes sont équivalentes :

(i) f est convexe.

(ii) f' est croissante.

(iii) La courbe représentative de f est au-dessus de ses tangentes.

Proposition 33. Une fonction $f : I \to \mathbb{R}$ deux fois dérivable est convexe si et seulement si $f''(x) \geq 0$ pour tout $x \in I$.

3. Fonctions log-convexes

Définition 34. On dit qu'une fonction $f : I \to \mathbb{R}_*^+$ est **log-convexe** si $\ln \circ f$ est convexe sur I.

[ROM19-1] p. 228

Proposition 35. Une fonction log-convexe est convexe.

Contre-exemple 36. $x \mapsto x$ est convexe mais non log-convexe.

Théorème 37. Pour une fonction $f : I \to \mathbb{R}_*^+$, les assertions suivantes sont équivalentes :

(i) f est log-convexe.

(ii) $\forall \alpha > 0$, $x \mapsto \alpha^x f(x)$ est convexe.

(iii) $\forall x, y \in I$, $\forall t \in [0,1]$, $f((1-t)x+ty) \leq (f(x))^{1-t}(f(y))^t$.

(iv) $\forall \alpha > 0$, f^α est convexe.

Lemme 38. La fonction Γ définie pour tout $x > 0$ par $\Gamma(x) = \int_0^{+\infty} t^{x-1}e^{-t}\,\mathrm{d}t$ vérifie :

(i) $\forall x \in \mathbb{R}_*^+$, $\Gamma(x+1) = x\Gamma(x)$.

p. 364

(ii) $\Gamma(1) = 1$.

(iii) Γ est log-convexe sur $\mathbb{R}_*^+$.

[DEV] p. 364

Théorème 39 (Bohr-Mollerup)**.** Soit $f : \mathbb{R}_*^+ \to \mathbb{R}^+$ vérifiant le Point (i), Point (ii) et Point (iii) du Théorème 38. Alors $f = \Gamma$.

Remarque 40. À la fin de la preuve, on obtient une formule due à Gauss :

$$\forall x \in]0,1], \Gamma(x) = \lim_{n\to+\infty} \frac{n^x n!}{(x+n)\dots(x+1)x}$$

que l'on peut aisément étendre à $\mathbb{R}_*^+$ entier.

III - Applications

1. Inégalités

Proposition 41 (Inégalité de Hölder)**.** Soient $p, q > 0$ tels que $\frac{1}{p} + \frac{1}{q} = 1$. Alors,

[GOU20] p. 97

$$\forall a_1, \dots, a_n, b_1, \dots, b_n \geq 0, \sum_{i=1}^n a_i b_i \leq \left(\sum_{i=1}^n a_i^p\right)^{\frac{1}{p}} \left(\sum_{i=1}^n b_i^q\right)^{\frac{1}{q}}$$

Proposition 42 (Inégalité de Minkowski)**.** Soit $p \geq 1$. Alors,

$$\forall x_1, \dots, x_n, y_1, \dots, y_n \geq 0, \left(\sum_{i=1}^n |x_i + y_i|^p\right)^{\frac{1}{p}} \leq \left(\sum_{i=1}^n x_i^p\right)^{\frac{1}{p}} \left(\sum_{i=1}^n y_i^p\right)^{\frac{1}{p}}$$

Proposition 43 (Inégalité de Jensen)**.** Si $f : \mathbb{R} \to \mathbb{R}$ est convexe, alors pour toute fonction u continue sur un intervalle $[a, b]$, on a :

[ROM19-1] p. 241

$$f\left(\frac{1}{b-a}\int_a^b u(t)\,\mathrm{d}t\right) \leq \frac{1}{b-a}\int_a^b f \circ u(t)\,\mathrm{d}t$$

Proposition 44 (Comparaison des moyennes harmonique, géométrique et arithmétique)**.** Pour toute suite finie $x = (x_i)$ de n réels strictement positifs, on a :

$$\frac{n}{\sum_{i=1}^n \frac{1}{x_i}} \leq \left(\prod_{i=1}^n x_i\right)^{\frac{1}{n}} \leq \frac{1}{n}\sum_{i=1}^n x_i$$

2. Recherche d'extrema

Proposition 45. Une fonction $f : \mathbb{R} \to \mathbb{R}$ est constante si et seulement si elle est convexe et majorée.

p. 234

Contre-exemple 46. La fonction f définie sur $\mathbb{R}^+$ par $f(x) = \frac{1}{1+x}$ est convexe, majorée, mais non constante.

Proposition 47. Si $f : I \to \mathbb{R}$ est convexe et est dérivable en un point $\alpha \in \mathring{I}$ tel que $f'(\alpha) = 0$, alors f admet un minimum global en α.

Proposition 48. Si $f : I \to \mathbb{R}$ est convexe et admet un minimum local, alors ce minimum est global.

3. Méthode de Newton

[DEV]

Théorème 49 (Méthode de Newton)**.** Soit $f : [c,d] \to \mathbb{R}$ une fonction de classe $\mathscr{C}^2$ strictement croissante sur $[c,d]$. On considère la fonction

$$\varphi : \begin{array}{ccc} [c,d] & \to & \mathbb{R} \\ x & \mapsto & x - \frac{f(x)}{f'(x)} \end{array}$$

(qui est bien définie car $f' > 0$). Alors :

(i) $\exists! a \in [c,d]$ tel que $f(a) = 0$.

(ii) $\exists \alpha > 0$ tel que $I = [a-\alpha, a+\alpha]$ est stable par φ.

(iii) La suite (x_n) des itérés (définie par récurrence par $x_{n+1} = \varphi(x_n)$ pour tout $n \geq 0$) converge quadratiquement vers a pour tout $x_0 \in I$.

[ROU] p. 152

Corollaire 50. En reprenant les hypothèses et notations du théorème précédent, et en supposant de plus f strictement convexe sur $[c,d]$, le résultat du théorème est vrai sur $I = [a,d]$. De plus :

(i) (x_n) est strictement décroissante (ou constante).

(ii) $x_{n+1} - a \sim \frac{f''(a)}{2f'(a)}(x_n - a)^2$ pour $x_0 > a$.

Exemple 51. — On fixe $y > 0$. En itérant la fonction $F : x \mapsto \frac{1}{2}\left(x + \frac{y}{x}\right)$ pour un nombre de départ compris entre c et d où $0 < c < d$ et $c^2 < 0 < d^2$, on peut obtenir une approximation du nombre $\sqrt{y}$.

— En itérant la fonction $F : x \mapsto \frac{x^2+1}{2x-1}$ pour un nombre de départ supérieur à 2, on peut obtenir une approximation du nombre d'or $\varphi = \frac{1+\sqrt{5}}{2}$.

230 Séries de nombres réels ou complexes. Comportement des restes ou des sommes partielles des séries numériques. Exemples.

I - Séries réelles et complexes

1. Notion de série et convergence

Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Muni de sa norme usuelle $|.|$, $\mathbb{K}$ est un espace de Banach.

Définition 1. Soit (u_n) une suite à valeurs dans $\mathbb{K}$. [GOU20] p. 208

— On appelle **série** de terme général u_n la suite (S_n) définie par

$$\forall n \in \mathbb{N},\ S_n = u_0 + \cdots + u_n$$

On note cette série $\sum u_n$.

— u_n s'appelle le **terme** d'indice n.

— S_n s'appelle la **somme partielle** d'indice n.

Définition 2. En reprenant les notations précédentes, on dit que $\sum u_n$ **converge** si la suite (S_n) converge. Dans ce cas, la limite s'appelle la **somme** de la série, et on la note $\sum_{n=0}^{+\infty} u_n$.

Définition 3. On appelle **reste** d'ordre n d'une série convergente $\sum u_n$ l'élément R_n défini par

$$R_n = \sum_{k=0}^{+\infty} u_k - \sum_{k=0}^{n} u_k = \sum_{k=n+1}^{+\infty} u_k$$

Exemple 4. Soit $q \in \mathbb{C}$. Alors $\sum q^n$ converge $\iff |q| < 1$. Dans ce cas :

— La somme partielle d'indice n est égale à $\frac{1-q^{n+1}}{1-q}$.

— La somme de la série est égale à $\frac{1}{1-q}$.

— Le reste d'ordre n de $\sum q^n$ est égal à $\frac{q^n}{1-q}$.

Proposition 5. Si $\sum u_n$ converge, alors $\lim_{n\to+\infty} u_n = 0$. [AMR11] p. 81

Contre-exemple 6. La réciproque est fausse, par exemple en considérant la suite (u_n) définie pour tout $n \in \mathbb{N}$ par $u_n = \ln(1 + \frac{1}{n})$, on a $\sum_{k=1}^{n} u_k = \ln(n+1) \longrightarrow_{n\to+\infty} +\infty$.

Proposition 7. Muni des opérations :

— $\forall (u_n), (v_n) \in \mathbb{K}^{\mathbb{N}}, \sum u_n + \sum v_n = \sum (u_n + v_n)$,

— $\forall \lambda \in \mathbb{K}, \forall (u_n) \in \mathbb{K}^{\mathbb{N}}, \lambda \sum u_n = \sum (\lambda u_n)$,

l'ensemble des séries numériques est un espace vectoriel sur $\mathbb{K}$ dont l'ensemble des séries convergentes est un sous-espace vectoriel.

Proposition 8 (Critère de Cauchy pour les séries)**.** Une série $\sum u_n$ converge si et seulement si

$$\forall \epsilon > 0, \exists N \in \mathbb{N}, \forall n \geq N, \forall p \in \mathbb{N}, \left| \sum_{k=0}^{p} u_{n+k} \right| < \epsilon$$

[GOU20] p. 209

Définition 9. On dit que $\sum u_n$ est **absolument convergente** si $\sum |u_n|$ est convergente.

Théorème 10. Tout série à valeurs dans $\mathbb{K}$ absolument convergente est convergente.

Ce dernier théorème justifie de s'intéresser plus particulièrement aux séries à termes positifs.

2. Séries à termes positifs

a. Comparaison

Proposition 11. Une série à termes positifs converge si et seulement si la suite des sommes partielles est majorée.

Corollaire 12. On considère deux séries réelles $\sum u_n$ et $\sum v_n$ telles que $\forall n \in \mathbb{N}, 0 \leq u_n \leq v_n$. Alors :

(i) Si $\sum v_n$ converge, $\sum u_n$ converge.

(ii) Si $\sum u_n$ diverge, $\sum v_n$ diverge.

Proposition 13. On considère deux séries $\sum u_n$ et $\sum v_n$ à termes positifs.

(i) Si $v_n = O(u_n)$ et si $\sum u_n$ converge, alors $\sum v_n$ converge.

(ii) Si $u_n \sim v_n$, alors les séries $\sum u_n$ et $\sum v_n$ sont de même nature.

— En cas de convergence, les restes vérifient $\sum_{k=n}^{+\infty} u_k \sim \sum_{k=n}^{+\infty} v_k$.

— En cas de divergence, les sommes partielles vérifient $\sum_{k=0}^{n} u_k \sim \sum_{k=0}^{n} v_k$.

p. 219

Application 14 (Formule de Stirling)**.**

$$\exists k > 0 \text{ tel que } n! \sim k\sqrt{n}\left(\frac{n}{e}\right)^n$$

Application 15 (Développement asymptotique de la suite des sinus itérés)**.** Soit (u_n) une suite vérifiant

$$u_0 \in \left]0, \frac{\pi}{2}\right], \quad \text{et} \quad \forall n \in \mathbb{N}, u_{n+1} = \sin(u_n)$$

Alors

$$u_n = \sqrt{\frac{3}{n}} - \frac{3\sqrt{3}}{10}\frac{\ln(n)}{n\sqrt{n}} + o\left(\frac{\ln(n)}{n\sqrt{n}}\right)$$

p. 228

Proposition 16 (Comparaison série - intégrale)**.** Soit $f : \mathbb{R}^+ \to \mathbb{R}^+$ une fonction positive, continue par morceaux et décroissante sur $\mathbb{R}^+$. Alors la suite (U_n) définie par

$$\forall n \in \mathbb{N}, \sum_{k=0}^{n} f(k) - \int_0^n f(t)\,\mathrm{d}t$$

est convergente. En particulier, la série $\sum f(n)$ et l'intégrale $\int_0^{+\infty} f(t)\,\mathrm{d}t$ sont de même nature.

p. 211

Exemple 17. La série de Riemann $\sum \frac{1}{n^\alpha}$ converge si et seulement si $\alpha > 1$.

Exemple 18. La série de Bertrand $\sum \frac{1}{n^\alpha \ln(n)^\beta}$ converge si et seulement si $\alpha > 1$ ou si $\alpha = 1$ et $\beta > 1$.

Lemme 19. Soit $\alpha > 1$. Lorsque n tend vers $+\infty$, on a

$$\sum_{k=n+1}^{+\infty} \frac{1}{n^\alpha} \sim \frac{1}{\alpha - 1}\frac{1}{n^{\alpha-1}}$$

[I-P] p. 380

[DEV]

Application 20 (Développement asymptotique de la série harmonique)**.** On note $\forall n \in \mathbb{N}^*, H_n = \sum_{k=1}^n \frac{1}{k}$. Alors, quand n tend vers $+\infty$,

$$H_n = \ln(n) + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + o\left(\frac{1}{n^2}\right)$$

Proposition 21. Soit $\sum f(n)$ une série relevant d'une comparaison série - intégrale. On note

[AMR11] p. 109

R_n le reste d'ordre n de cette série. Alors,

$$\forall n \geq 1, \int_{n+1}^{+\infty} f(t)\,\mathrm{d}t \leq |R_n| \leq \int_{n}^{+\infty} f(t)\,\mathrm{d}t$$

Exemple 22. La somme $\sum_{n=1}^{20} \frac{1}{n^3}$ donne une approximation de $\zeta(3) = \sum_{n=1}^{+\infty} \frac{1}{n^3}$ à moins de 125×10^{-5} près.

Proposition 23. Soient deux séries réelles $\sum u_n$ et $\sum v_n$ à termes strictement positifs telles que $\frac{u_{n+1}}{u_n} \geq \frac{v_{n+1}}{v_n}$ à partir d'un certain rang. Alors : [GOU20] p. 213

(i) Si $\sum u_n$ converge, $\sum v_n$ converge.

(ii) Si $\sum v_n$ diverge, $\sum u_n$ diverge.

b. Critères

Proposition 24 (Règle de d'Alembert)**.** Soit $\sum u_n$ une série à termes strictement positifs telle que

$$\lim_{n\to+\infty} \frac{u_{n+1}}{u_n} = \lambda \in [0, +\infty]$$

Alors :

(i) Si $\lambda < 1$, $\sum u_n$ converge.

(ii) Si $\lambda > 1$, $\sum u_n$ diverge.

Exemple 25. $\sum \left(1 - \frac{1}{n}\right)^{n^2}$ converge. [AMR11] p. 94

Proposition 26. Soit $\sum u_n$ une série relevant de la règle de D'Alembert. On note R_n le reste d'ordre n de cette série. Alors il existe $N \in \mathbb{N}$ et $\alpha \in]0,1[$ tels que p. 108

$$\forall n \geq N, |R_n| \leq \frac{\alpha}{1-\alpha}$$

Exemple 27. $\sum_{k=0}^{10} \frac{1}{n!}$ donne une valeur approchée de e à moins de 3×10^{-8} près par défaut.

Proposition 28 (Règle de Cauchy)**.** Soit $\sum u_n$ une série à termes strictement positifs telle que [GOU20] p. 214

$$\lim_{n\to+\infty} \sqrt[n]{u_n} = \lambda \in [0, +\infty]$$

Alors :

(i) Si $\lambda < 1$, $\sum u_n$ converge.

(ii) Si $\lambda > 1$, $\sum u_n$ diverge.

Exemple 29. $\sum \left(\frac{4n+1}{3n+2}\right)^n$ converge. [AMR11] p. 112

Proposition 30. Soit $\sum u_n$ une série relevant de la règle de Cauchy. On note R_n le reste d'ordre n de cette série. Alors il existe $N \in \mathbb{N}$ et $\alpha \in]0,1[$ tels que p. 107

$$\forall n \geq N,\ |R_n| \leq \frac{\alpha^{n+1}}{1-\alpha}$$

Exemple 31. En reprenant les notations précédentes, pour $u_n = n^{-n}$, on a $R_4 < 0,00035$.

3. Séries semi-convergentes

Définition 32. On appelle **séries semi-convergentes** les séries convergentes mais non absolument convergentes. p. 214

Théorème 33 (Critère de Leibniz)**.** Soit (a_n) une suite à termes positifs, décroissantes, tendant vers 0. Alors

$$\sum (-1)^n a_n \text{ converge} \quad \text{et} \quad \forall n \in \mathbb{N},\ |R_n| = \left| \sum_{k=n+1}^{+\infty} (-1)^k a_k \right| \leq a_{n+1}$$

Exemple 34. La série $\sum (-1)^{n-1} n^{-\alpha}$ est convergente pour $\alpha > 0$. De plus, les restes R_n vérifient p. 97

$$|R_n| \leq \frac{1}{(n+1)^\alpha}$$

Proposition 35 (Transformation d'Abel)**.** Soit une série $\sum u_n$ où $\forall n \in \mathbb{N}$, $u_n = \alpha_n v_n$. On note $\forall n \in \mathbb{N}$, $S_n = \sum_{k=0}^{n} v_k$. Alors, [GOU20] p. 215

$$\sum_{k=0}^{n} u_k = \alpha_n S_n + \sum_{k=0}^{n-1} (\alpha_k - \alpha_{k+1}) S_k$$

Corollaire 36 (Critère d'Abel)**.** Soit une série $\sum u_n$ où $\forall n \in \mathbb{N}$, $u_n = \alpha_n v_n$. On suppose : [AMR11] p. 99

— (α_n) est une suite réelle positive, décroissante et qui tend vers 0.

— La série $\sum v_n$ est bornée par une constante M.

Alors $\sum u_n$ est convergente, et les restes R_n vérifient $\forall n \in \mathbb{N}, |R_n| \leq M a_{n+1}$.

Remarque 37. En reprenant les notations précédentes, avec $v_n = (-1)^n$, on retrouve le critère de Leibniz. [GOU20] p. 216

Exemple 38. La série $\sum \frac{e^{ni\theta}}{n^\alpha}$ converge pour tout $\alpha > 0, \theta \in \mathbb{R} \setminus 2\pi\mathbb{Z}$.

II - Calcul de sommes

1. Séries de Fourier

Définition 39. Soit $f : \mathbb{R} \to \mathbb{C}$ une application 2π-périodique et continue par morceaux sur $\mathbb{R}$. On appelle **coefficients de Fourier** de f les nombres complexes définis par p. 267

$$\forall n \in \mathbb{Z}, c_n(f) = \int_0^{2\pi} f(t) e^{-int} \, \mathrm{d}t$$

La **série de Fourier** associée à f est

$$\sum_{n \in \mathbb{Z}} c_n(f) e^{inx}$$

Théorème 40 (Parseval)**.** Soit $f : \mathbb{R} \to \mathbb{C}$ une application 2π-périodique et continue par morceaux sur $\mathbb{R}$. Alors la série de Fourier de f est convergente et,

$$\sum_{n=-\infty}^{+\infty} |c_n(f)|^2 = \frac{1}{2\pi} \int_0^{2\pi} |f(t)| \, \mathrm{d}t$$

Exemple 41. Avec $f : x \mapsto 1 - \frac{x^2}{\pi^2}$, on obtient $\sum_{n=1}^{+\infty} \frac{1}{n^4} = \frac{\pi^4}{90}$.

Théorème 42 (Jordan-Dirichlet)**.** Soit $f : \mathbb{R} \to \mathbb{C}$ une application 2π-périodique et $\mathscr{C}^1$ par morceaux sur $\mathbb{R}$. Alors la série de Fourier de f est convergente en tout point $x \in \mathbb{R}$ et sa somme en ce point vaut

$$\frac{f(x^+) + f(x^-)}{2}$$

Exemple 43. Toujours avec $f : x \mapsto 1 - \frac{x^2}{\pi^2}$, on obtient $\sum_{n=1}^{+\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$.

2. Séries entières

Définition 44. On appelle **série entière** toute série de fonctions de la forme $\sum a_n z^n$ où z est une variable complexe et où (a_n) est une suite complexe.

p. 247

Lemme 45 (Abel)**.** Soient $\sum a_n z^n$ une série entière et $z_0 \in \mathbb{C}$ tels que $(a_n z_0^n)$ soit bornée. Alors :

(i) $\forall z \in \mathbb{C}$ tel que $|z| < |z_0|$, $\sum a_n z^n$ converge absolument.

(ii) $\forall r \in]0, |z_0|[$, $\sum a_n z^n$ converge normalement dans $\overline{D}(0,r) = \{z \in \mathbb{C} \mid |z| \leq r\}$.

Définition 46. Soit $\sum a_n z^n$ une série entière. Le nombre

$$R = \sup\{r \geq 0 \mid (|a_n| r^n) \text{ est bornée}\}$$

est le **rayon de convergence** de $\sum a_n z^n$. On a :

— $\forall z \in \mathbb{C}$ tel que $|z| < R$, $\sum a_n z^n$ converge absolument.

— $\forall z \in \mathbb{C}$ tel que $|z| > R$, $\sum a_n z^n$ diverge.

— $\forall r \in [0, R[$, $\sum a_n z^n$ converge normalement sur $\overline{D}(0,r)$.

Le disque $D(0,R)$ est le **disque de convergence** de la série, le cercle $C(0,R)$ est le **cercle d'incertitude**.

Exemple 47. $\sum \frac{z^n}{n!}$ est une série entière de rayon de convergence infini.

[DEV]

Théorème 48 (Nombres de Bell)**.** Pour tout $n \in \mathbb{N}^*$, on note B_n le nombre de partitions de $[\![1, n]\!]$. Par convention on pose $B_0 = 1$. Alors,

$$\forall k \in \mathbb{N}^*, B_k = \frac{1}{e} \sum_{n=0}^{+\infty} \frac{n^k}{n!}$$

[GOU21] p. 314

Théorème 49 (Abel angulaire)**.** Soit $\sum a_n z^n$ une série entière de rayon de convergence supérieur ou égal à 1 telle que $\sum a_n$ converge. On note f la somme de cette série sur le disque unité D de $\mathbb{C}$. On fixe $\theta_0 \in \left[0, \frac{\pi}{2}\right[$ et on pose $\Delta_{\theta_0} = \{z \in D \mid \exists \rho > 0 \text{ et } \exists \theta \in [-\theta_0, \theta_0] \text{ tels que } z = 1 - \rho e^{i\theta}\}$.

Alors $\lim\limits_{\substack{z \to 1 \\ z \in \Delta_{\theta_0}}} f(z) = \sum_{n=0}^{+\infty} a_n$.

[GOU20] p. 263

Application 50.

$$\sum_{n=0}^{+\infty} \frac{(-1)^n}{(2n+1)} = \frac{\pi}{4}$$

Application 51.

$$\sum_{n=0}^{+\infty} \frac{(-1)^{n-1}}{n} = \ln(2)$$

Contre-exemple 52. La réciproque est fausse :

$$\lim_{\substack{z\to 1\\ |z|<1}} (-1)^n z^n = \lim_{\substack{z\to 1\\ |z|<1}} \frac{1}{1+z} = \frac{1}{2}$$

Théorème 53 (Taubérien faible)**.** Soit $\sum a_n z^n$ une série entière de rayon de convergence 1. On note f la somme de cette série sur $D(0,1)$. On suppose que

$$\exists S \in \mathbb{C} \text{ tel que } \lim_{\substack{x\to 1\\ x<1}} f(x) = S$$

Si $a_n = o\left(\frac{1}{n}\right)$, alors $\sum a_n$ converge et $\sum_{n=0}^{+\infty} a_n = S$.

Remarque 54. Ce dernier résultat est une réciproque partielle du Théorème 49. Il reste vrai en supposant $a_n = O\left(\frac{1}{n}\right)$ (c'est le théorème Taubérien fort).

Annexes

[GOU20]
p. 263

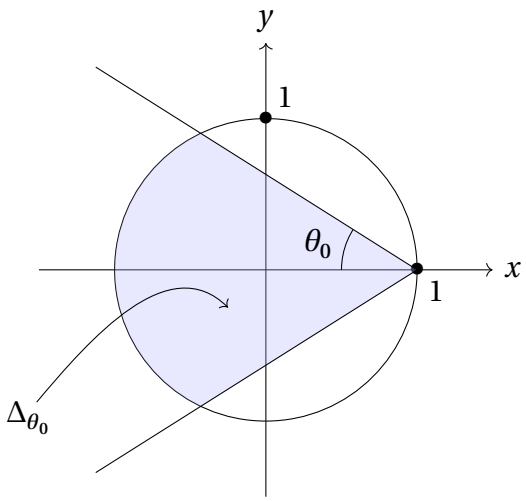


FIGURE I.27 – Illustration du théorème d'Abel angulaire.

234 Fonctions et espaces de fonctions Lebesgue-intégrable

On se place dans un espace mesuré $(X, \mathscr{A}, \mu)$. Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, que l'on munit de sa tribu borélienne $\mathscr{B}(\mathbb{K})$.

I - L'intégrale de Lebesgue

1. Définition abstraite

Définition 1. Soit f une fonction étagée positive sur $(X, \mathscr{A})$. **L'intégrale** de f sur X par rapport à la mesure μ est définie par

$$\int_X f \, \mathrm{d}\mu = \sum_{\alpha \in f(X)} \alpha \mu(\{f = \alpha\}) \in \overline{\mathbb{R}^+}$$

[B-P] p. 120

Proposition 2. Soit f une fonction étagée. Pour toute décomposition de la forme $f = \sum_{i \in I} \alpha_i \mathbb{1}_{A_i}$ (où $(A_i)_{i \in I}$ désigne une partition $\mathscr{A}$-mesurable finie de X), on a :

$$\int_X f \, \mathrm{d}\mu = \sum_{i \in I} \alpha_i \mu(A_i)$$

Exemple 3. Soit $f : X \to \mathbb{R}^+$ une fonction ne prenant qu'un nombre fini de valeurs.

— On se place dans le cas où $\mu = \delta_a$, la mesure de Dirac en un point $a \in X$. Alors,

$$\int_X f \, \mathrm{d}\mu = f(a)$$

— On se place dans le cas où $\mu = m$, la mesure de comptage sur $(X, \mathscr{P}(X))$. Alors,

$$\int_X f \, \mathrm{d}m = \sum_{\alpha \in f(X)} \alpha |\{f = \alpha\}|$$

Définition 4. Soit f une fonction mesurable positive (finie ou non) sur $(X, \mathscr{A})$. On pose

$$\int_X f \, \mathrm{d}\mu = \sup \left\{ \int_X \varphi \, \mathrm{d}\mu \mid \varphi \text{ étagée positive telle que } \varphi \leq f \right\}$$

on dit que f est μ-**intégrable** si $\int_X f \, \mathrm{d}\mu < +\infty$.

2. Propriétés

Théorème 5 (Convergence monotone)**.** Soit (f_n) une suite croissante de fonctions mesurables positives. Alors, la limite f de cette suite est mesurable positive, et,

$$\int_X f \,\mathrm{d}\mu = \lim_{n\to+\infty} \int_X f_n \,\mathrm{d}\mu$$

Corollaire 6. Soient f, g deux fonctions mesurables positives.

(i) $f \leq g \implies \int_X f \,\mathrm{d}\mu \leq \int_X g \,\mathrm{d}\mu$ (l'intégrale est croissante).

(ii) $\int_X (f+g)\,\mathrm{d}\mu = \int_X f \,\mathrm{d}\mu + \int_X g \,\mathrm{d}\mu$ (l'intégrale est additive).

(iii) $\forall \lambda \geq 0$, $\int_X \lambda f \,\mathrm{d}\mu = \lambda \int_X f \,\mathrm{d}\mu$ (l'intégrale est positivement homogène).

(iv) Si $f = g$ pp., alors $\int_X f \,\mathrm{d}\mu = \int_X g \,\mathrm{d}\mu$.

Au vu de la linéarité de l'intégrale, on peut maintenant donner la définition suivante.

Définition 7. Soit $f : X \to \mathbb{K}$ mesurable. p. 128

— f est dite **μ-intégrable** si $|f|$ est μ-intégrable.

— Dans ce cas, si $\mathbb{K} = \mathbb{R}$, en notant f^+ et f^- les parties positives et négatives de f, on définit

$$\int_X f \,\mathrm{d}\mu = \int_X f^+ \,\mathrm{d}\mu - \int_X f^- \,\mathrm{d}\mu$$

— Si $\mathbb{K} = \mathbb{C}$, en reprenant le point précédent, on définit

$$\int_X f \,\mathrm{d}\mu = \int_X \mathrm{Re}(f)\,\mathrm{d}\mu + i \int_X \mathrm{Im}(f)\,\mathrm{d}\mu$$

Proposition 8. Soit $f : X \to \mathbb{K}$ intégrable. Alors,

$$\left| \int_X f \,\mathrm{d}\mu \right| \leq \int_X |f| \,\mathrm{d}\mu$$

avec égalité,

— si $\mathbb{K} = \mathbb{R}$, si f est de signe constant pp.

— si $\mathbb{K} = \mathbb{C}$, si $f = \alpha |f|$ pp. pour $\alpha \in C(0,1)$.

3. Lien avec l'intégrale de Riemann

Proposition 9. Soit $[a,b]$ un intervalle de $\mathbb{R}$. Soit f une fonction intégrable au sens de Riemann sur $[a,b]$.

(i) Il existe une fonction g λ-intégrable sur $[a,b]$ telle que $f = g$ pp. De plus,

$$\int_a^b f = \int_{[a,b]} g \, \mathrm{d}\lambda$$

(ii) En particulier, si f est borélienne,

$$\int_a^b f = \int_{[a,b]} f \, \mathrm{d}\lambda$$

Contre-exemple 10. La réciproque est fausse. Par exemple, $\mathbb{1}_{\mathbb{Q}\cap[0,1]}$ est intégrable au sens de Lebesgue, mais pas au sens de Riemann.

II - Construction des espaces L_p

1. L'espace vectoriel $\mathscr{L}_1$

Définition 11. On note

$$\mathscr{L}_1(X,\mathscr{A},\mu) = \{f : X \to \mathbb{K} \mid f \text{ est } \mu\text{-intégrable}\}$$

l'ensemble des fonctions μ-intégrables. En l'absence d'ambiguïté, on notera simplement $\mathscr{L}_1(\mu)$ ou $\mathscr{L}_1$. Cette définition s'étend aux ensembles de fonctions intégrables à valeurs dans $\mathbb{R}^+$, $\overline{\mathbb{R}}$, etc.

Exemple 12. Si μ est la mesure de comptage sur $(\mathscr{P}(\mathbb{N}),\mathbb{N})$, alors

$$\mathscr{L}_1 = \ell_1 = \left\{(u_n) \in \mathbb{R}^n \mid \sum_{n\geq 0} |u_n| < +\infty\right\}$$

Théorème 13. (i) $f \mapsto \int_X f \, \mathrm{d}\mu$ est une forme linéaire positive (au sens où $f \geq 0 \implies \int_X f \, \mathrm{d}\mu \geq 0$) et croissante sur $\mathscr{L}_1$.

(ii) $\mathscr{L}_1$ est un espace vectoriel sur $\mathbb{K}$.

(iii) $\|.\|_1 : f \mapsto \int_X |f| \, \mathrm{d}\mu$ est une semi-norme sur $\mathscr{L}_1$.

p. 137

Théorème 14 (Lemme de Fatou)**.** Soit (f_n) une suite de fonctions mesurables positives. Alors,

$$0 \leq \int_X \liminf f_n \, \mathrm{d}\mu \leq \liminf \int_X f_n \, \mathrm{d}\mu \leq +\infty$$

Exemple 15. Soit f croissante sur $[0,1]$, continue en 0 et dérivable en 1 et dérivable pp. dans $[0,1]$. Alors,

$$\int_0^1 f'(x)\,\mathrm{d}x \leq f(1) - f(0)$$

Théorème 16 (Convergence dominée)**.** Soit (f_n) une suite d'éléments de $\mathscr{L}_1$ telle que :

(i) pp. en x, $(f_n(x))$ converge dans $\mathbb{K}$ vers $f(x)$.

(ii) $\exists g \in \mathscr{L}_1$ positive telle que

$$\forall n \in \mathbb{N}, \text{ pp. en } x, \ |f_n(x)| \leq g(x)$$

Alors,

$$\int_X f \, \mathrm{d}\mu = \lim_{n\to+\infty} \int_X f_n \, \mathrm{d}\mu \text{ et } \lim_{n\to+\infty} \int_X |f_n - f| \, \mathrm{d}\mu = 0$$

Exemple 17.
— On reprend l'Théorème 15 et on suppose f partout dérivable sur $[0,1]$ de dérivée bornée. Alors l'inégalité est une égalité.

— Soit $\alpha > 1$. On pose $\forall n \geq 1$, $I_n(\alpha) = \int_0^n \left(1 + \frac{x}{n}\right)^n e^{-\alpha x}\,\mathrm{d}x$. Alors,

$$\lim_{n\to+\infty} I_n(\alpha) = \int_0^{+\infty} e^{(1-\alpha)x}\,\mathrm{d}x = \frac{1}{\alpha - 1}$$

Application 18 (Lemme de Borel-Cantelli)**.** Soit (A_n) une famille de parties de $\mathscr{A}$. Alors,

$$\sum_{n=1}^{+\infty} \mu(A_n) < +\infty \implies \mu\left(\limsup_{n\to+\infty} A_n\right) = 0$$

2. Les espaces vectoriels $\mathscr{L}_p$

Définition 19. Pour tout réel $p > 0$, on définit

$$\mathscr{L}_p(X, \mathscr{A}, \mu) = \{f : X \to \mathbb{K} \mid |f|^p \in \mathscr{L}_1(X, \mathscr{A}, \mu)\}$$

on a les mêmes remarques qu'à la Théorème 11.

p. 163

Proposition 20. $\mathscr{L}_p$ est un espace vectoriel.

Proposition 21. (i) Si $\mu(X) < +\infty$, alors

$$0 < p \leq q \implies \mathscr{L}_q \subseteq \mathscr{L}_p$$

(ii) Si $\mu = m$ est la mesure de comptage sur $\mathbb{N}$, alors

$$0 < p \leq q \implies \underbrace{\mathscr{L}_p(m)}_{\ell_p} \subseteq \underbrace{\mathscr{L}_q(m)}_{\ell_q}$$

Définition 22. Pour tout $p > 0$, on définit

$$\|.\|_p : f \mapsto \left(\int_X |f|^p \, \mathrm{d}\mu\right)^{\frac{1}{p}}$$

Théorème 23 (Inégalité de Hölder)**.** Soient $p, q \in]1, +\infty[$ tels que $\frac{1}{p} + \frac{1}{q} = 1$, $f \in \mathscr{L}_p$ et $g \in \mathscr{L}_q$. Alors $fg \in \mathscr{L}_1$ et

$$\|fg\|_1 \leq \|f\|_p \|g\|_q$$

Théorème 24 (Inégalité de Minkowski)**.**

$$\forall f, g \in \mathscr{L}_p, \ \|f + g\|_p \leq \|f\|_p + \|g\|_p$$

3. Les espaces vectoriels normés L_p

p. 171

Définition 25. On définit pour tout $p > 0$,

$$L_p = \mathscr{L}_p / V$$

où $V = \{v \in \mathscr{L}_p \mid v = 0 \text{ pp.}\}$.

Théorème 26. Pour tout $p \in [1, +\infty]$, (L_p), $\|.\|_p$ est un espace vectoriel normé.

Théorème 27 (Riesz-Fischer)**.** Pour tout $p \in [1, +\infty]$, L_p est complet pour la norme $\|.\|_p$.

Théorème 28. Soit (f_n) une suite d'éléments de L_p qui converge vers f pour la norme $\|.\|_p$. Alors, il existe une sous-suite de (f_n) qui converge pp. vers f.

Proposition 29. Pour tout $p \in [1, +\infty[$, l'ensemble des fonctions étagées intégrables est dense dans L_p. p. 176

Théorème 30. On se place sur $(\mathbb{R}, \mathscr{B}(\mathbb{R}), \lambda)$. Alors :

(i) L'ensemble des fonctions en escalier à support compact est dense dans L_p pour tout $p \in [1, +\infty[$.

(ii) L'ensemble des fonctions continues à support compact est dense dans L_p pour tout $p \in [1, +\infty[$.

4. L'espace L_∞

Définition 31. — Soit $f : X \to \mathbb{K}$. On définit $\|f\|_\infty$ comme le supremum essentiel de la fonction $|f|$ et $\mathscr{L}_\infty(\mu)$ (noté $\mathscr{L}_\infty$ en l'absence d'ambiguïté) l'ensemble des fonctions μ-essentiellement bornées. p. 180

— On définit

$$L_\infty = \mathscr{L}_\infty / V$$

où $V = \{v \in \mathscr{L}_\infty \mid v = 0 \text{ pp.}\}$.

Théorème 32. L_∞, muni de $\|.\|_\infty$, est un espace vectoriel normé complet.

Remarque 33. L'inégalité de Hölder est encore vraie pour $q = +\infty$.

III - Grands théorèmes d'intégration

1. Régularité sous l'intégrale

Soit $f : E \times X \to \mathbb{C}$ où (E, d) est un espace métrique. On pose $F : t \mapsto \int_X f(t,x)\,\mathrm{d}\mu(x)$. **[Z-Q]** p. 312

a. Continuité

Théorème 34 (Continuité sous le signe intégral)**.** On suppose :

(i) $\forall t \in E$, $x \mapsto f(t,x)$ est mesurable.

(ii) pp. en $x \in X$, $t \mapsto f(t,x)$ est continue en $t_0 \in E$.

(iii) $\exists g \in L_1(X)$ positive telle que

$$|f(t,x)| \leq g(x) \quad \forall t \in E, \text{pp. en } x \in X$$

Alors F est continue en t_0.

Corollaire 35. On suppose :

(i) $\forall t \in E$, $x \mapsto f(t,x)$ est mesurable.

(ii) pp. en $x \in X$, $t \mapsto f(t,x)$ est continue sur E.

(iii) $\forall K \subseteq E$, $\exists g_K \in L_1(X)$ positive telle que

$$|f(t,x)| \leq g_K(x) \quad \forall t \in E, \text{pp. en } x$$

Alors F est continue sur E.

Exemple 36. La fonction

$$\Gamma : \begin{array}{ccc} \mathbb{R}_*^+ & \to & \mathbb{R}_*^+ \\ t & \mapsto & \int_0^{+\infty} t^{x-1} e^{-t} \, \mathrm{d}t \end{array}$$

est bien définie et continue sur $\mathbb{R}_*^+$.

p. 318

Exemple 37. Soit $f : \mathbb{R}^+ \to \mathbb{C}$ intégrable. Alors,

$$\lambda \mapsto \int_0^{+\infty} e^{-\lambda t} f(t) \, \mathrm{d}t$$

est bien définie et est continue sur $\mathbb{R}^+$.

[G-K] p. 104

b. Dérivabilité

On suppose ici que E est un intervalle I ouvert de $\mathbb{R}$.

[Z-Q] p. 313

Théorème 38 (Dérivation sous le signe intégral)**.** On suppose :

(i) $\forall t \in I$, $x \mapsto f(t,x) \in L_1(X)$.

(ii) pp. en $x \in X$, $t \mapsto f(t,x)$ est dérivable sur I. On notera $\frac{\partial f}{\partial t}$ cette dérivée définie presque partout.

(iii) $\forall K \subseteq I$ compact, $\exists g_K \in L_1(X)$ positive telle que

$$\left|\frac{\partial f}{\partial t}(x,t)\right| \leq g_K(x) \quad \forall t \in I, \text{pp. en } x$$

Alors $\forall t \in I, x \mapsto \frac{\partial f}{\partial t}(x,t) \in L_1(X)$ et F est dérivable sur I avec

$$\forall t \in I, F'(t) = \int_X \frac{\partial f}{\partial t}(x,t)\,\mathrm{d}\mu(x)$$

Remarque 39. — Si dans le Théorème 38, hypothèse (i), on remplace "dérivable" par "$\mathscr{C}^1$", alors la fonction F est de classe $\mathscr{C}^1$.

— On a un résultat analogue pour les dérivées d'ordre supérieur.

Théorème 40 (k-ième dérivée sous le signe intégral)**.** On suppose :

(i) $\forall t \in I, x \mapsto f(t,x) \in L_1(X)$.

(ii) pp. en $x \in X$, $t \mapsto f(t,x) \in \mathscr{C}^k(I)$. On notera $\left(\frac{\partial}{\partial t}\right)^j f$ la j-ième dérivée définie presque partout pour $j \in [\![0,k]\!]$.

(iii) $\forall j \in [\![0,k]\!]$, $\forall K \subseteq I$ compact, $\exists g_{j,K} \in L_1(X)$ positive telle que

$$\left|\left(\frac{\partial}{\partial t}\right)^j f(x,t)\right| \leq g_{j,K}(x) \quad \forall t \in K, \text{pp. en } x$$

Alors $\forall j \in [\![0,k]\!]$, $\forall t \in I$, $x \mapsto \left(\frac{\partial}{\partial t}\right)^j f(x,t) \in L_1(X)$ et $F \in \mathscr{C}^k(I)$ avec

$$\forall j \in [\![0,k]\!],\ \forall t \in I,\ F^{(j)}(t) = \int_X \left(\frac{\partial}{\partial t}\right)^j f(x,t)\,\mathrm{d}\mu(x)$$

Exemple 41. La fonction Γ de l'Théorème 36 est $\mathscr{C}^\infty$ sur $\mathbb{R}_*^+$. p. 318

Exemple 42. On se place dans l'espace mesuré $(\mathbb{N}, \mathscr{P}(\mathbb{N}), \mathrm{card})$ et on considère (f_n) une suite de fonctions dérivables sur I telle que **[B-P]** p. 149

$$\forall x \in \mathbb{R},\ \sum_{n\in\mathbb{N}} |f_n(x)| + \sup_{x\in I} |f_n'(t)| < +\infty$$

Alors $x \mapsto \sum_{n\in\mathbb{N}} f_n(x)$ est dérivable sur I de dérivée $x \mapsto \sum_{n\in\mathbb{N}} f_n'(x)$.

Application 43 (Transformée de Fourier d'une Gaussienne)**.** En résolvant une équation différentielle linéaire, on a **[GOU20]** p. 169

$$\forall \alpha > 0,\ \forall x \in \mathbb{R},\ \int_{\mathbb{R}} e^{-\alpha t^2} e^{-itx}\,\mathrm{d}t = \sqrt{\frac{\pi}{\alpha}} e^{-\frac{x^2}{\pi\alpha}}$$

[G-K] p. 107

Application 44 (Intégrale de Dirichlet)**.** On pose $\forall x \geq 0$,

$$F(x) = \int_0^{+\infty} \frac{\sin(t)}{t} e^{-xt} \, \mathrm{d}t$$

alors :

(i) F est bien définie et est continue sur $\mathbb{R}^+$.

(ii) F est dérivable sur $\mathbb{R}_*^+$ et $\forall x \in \mathbb{R}_*^+, F'(x) = -\frac{1}{1+x^2}$.

(iii) $F(0) = \int_0^{+\infty} \frac{\sin(t)}{t} \, \mathrm{d}t = \frac{\pi}{2}$.

c. Holomorphie

On suppose ici que E est un ouvert Ω de $\mathbb{C}$.

[Z-Q] p. 314

Théorème 45 (Holomorphie sous le signe intégral)**.** On suppose :

(i) $\forall z \in \Omega$, $x \mapsto f(z,x) \in L_1(X)$.

(ii) pp. en $x \in X$, $z \mapsto f(z,x)$ est holomorphe dans Ω. On notera $\frac{\partial f}{\partial z}$ cette dérivée définie presque partout.

(iii) $\forall K \subseteq \Omega$ compact, $\exists g_K \in L_1(X)$ positive telle que

$$|f(x,z)| \leq g_K(x) \quad \forall z \in K, \text{pp. en } x$$

Alors F est holomorphe dans Ω avec

$$\forall z \in \Omega, F'(z) = \int_X \frac{\partial f}{\partial z}(z,t) \, \mathrm{d}\mu(z)$$

Exemple 46. La fonction Γ de l'Théorème 36 est holomorphe dans l'ouvert $\{z \in \mathbb{C} \mid \mathrm{Re}(z) > 0\}$.

p. 318

2. Intégration sur un espace produit

[B-P] p. 237

Théorème 47 (Fubini-Tonelli)**.** Soient $(Y, \mathscr{B}, \nu)$ un autre espace mesuré et $f : (X \times Y) \to \overline{\mathbb{R}^+}$. On suppose μ et ν σ-finies. Alors :

(i) $x \mapsto \int_Y f(x,y) \, \mathrm{d}\nu(y)$ et $y \mapsto \int_X f(x,y) \, \mathrm{d}\mu(x)$ sont mesurables.

(ii) Dans $\overline{\mathbb{R}^+}$,

$$\int_{X \times Y} f \, \mathrm{d}(\mu \otimes \nu) = \int_X \left(\int_Y f(x,y) \, \mathrm{d}\nu(y) \right) = \int_Y \left(\int_X f(x,y) \, \mathrm{d}\mu(x) \right)$$

Théorème 48 (Fubini-Lebesgue)**.** Soient $(Y, \mathcal{B}, \nu)$ un autre espace mesuré et $f \in \mathcal{L}_1(\mu \otimes \nu)$. Alors :

(i) Pour tout $y \in Y$, $x \mapsto f(x,y)$ et pour tout $x \in X$, $y \mapsto f(x,y)$ sont intégrables.

(ii) $x \mapsto \int_Y f(x,y)\,\mathrm{d}\nu(y)$ et $y \mapsto \int_X f(x,y)\,\mathrm{d}\mu(x)$ sont intégrables, les fonctions étant définies pp.

(iii) On a :
$$\int_{X\times Y} f\,\mathrm{d}(\mu\otimes\nu) = \int_X \left(\int_Y f(x,y)\,\mathrm{d}\nu(y)\right) = \int_Y \left(\int_X f(x,y)\,\mathrm{d}\mu(x)\right)$$

Contre-exemple 49. On considère $f : (x,y) \mapsto 2e^{-2xy} - e^{-xy}$. Alors, $\int_{[0,1]} \left(\int_{\mathbb{R}^+} f(x,y)\,\mathrm{d}x\right)\mathrm{d}y = 0$, mais $\int_{\mathbb{R}^+} \left(\int_{[0,1]} f(x,y)\,\mathrm{d}y\right)\mathrm{d}x = \ln(2)$.

Exemple 50. Soient $f : (x,y) \mapsto xy$ et $D = \{(x,y) \in \mathbb{R}^2 \mid x,y \geq 0 \text{ et } x+y \leq 1\}$. Alors, [GOU20] p. 359

$$\int\int_D = f(x,y)\,\mathrm{d}x\mathrm{d}y = \int_0^1 x\frac{(1-x)^2}{2}\,\mathrm{d}x = \frac{1}{24}$$

IV - L'espace L_2

1. Aspect hilbertien

Définition 51. L'application [B-P] p. 185
$$\langle .,. \rangle : (f,g) \mapsto \int_X f\overline{g}\,\mathrm{d}\mu$$
définit un produit scalaire hermitien sur L_2. Muni de ce produit scalaire précédent, L_2 est un espace de Hilbert.

a. Conséquences

Théorème 52 (Projection orthogonale)**.** Soit F un sous-espace vectoriel fermé de L_2. Alors,
$$L_2 = F \oplus F^\perp$$

Corollaire 53 (Théorème de représentation de Riesz)**.** Soit $\varphi \in L_2'$ une forme linéaire continue. Alors,
$$\exists! g \in L_2 \text{ telle que } \forall f \in L_2,\ \varphi(f) = \int_X f\overline{g}\,\mathrm{d}\mu$$

[DEV] [Z-Q] p. 222

Application 54 (Dual de L_p)**.** Soit $(X,\mathscr{A},\mu)$ un espace mesuré de mesure finie. On note $\forall p\in]1,2[$, $L_p = L_p(X,\mathscr{A},\mu)$. L'application

$$\varphi : \begin{array}{ll} L_q & \to (L_p)' \\ g & \mapsto \left(\varphi_g : f \mapsto \int_X fg\,\mathrm{d}\mu\right) \end{array} \qquad \text{où } \frac{1}{p}+\frac{1}{q}=1$$

est une isométrie linéaire surjective. C'est donc un isomorphisme isométrique.

Remarque 55. Plus généralement, si l'on identifie g et φ_g :

— L_q est le dual topologique de L_p pour $p\in]1,+\infty[$.

— L_∞ est le dual topologique de L_1 si μ est σ-finie.

[LI] p. 140

b. Base hilbertienne de L_2

Soit I un intervalle de $\mathbb{R}$. On pose $\forall n\in\mathbb{N}$, $g_n : x\mapsto x^n$.

[BMP] p. 110

Définition 56. On appelle **fonction poids** une fonction $\rho : I\to\mathbb{R}$ mesurable, positive et telle que $\forall n\in\mathbb{N}, \rho g_n\in L_1(I)$.

Soit $\rho : I\to\mathbb{R}$ une fonction poids.

Notation 57. On note $L_2(I,\rho)$ l'espace des fonctions de carré intégrable pour la mesure de densité ρ par rapport à la mesure de Lebesgue.

Proposition 58. Muni de

$$\langle .,. \rangle : (f,g)\mapsto \int_I f(x)\overline{g(x)}\rho(x)\,\mathrm{d}x$$

$L_2(I,\rho)$ est un espace de Hilbert.

Théorème 59. Il existe une unique famille (P_n) de polynômes unitaires orthogonaux deux-à-deux telle que $\deg(P_n)=n$ pour tout entier n. C'est la famille de **polynômes orthogonaux** associée à ρ sur I.

Exemple 60 (Polynômes de Hermite)**.** Si $\forall x\in I$, $\rho(x)=e^{-x^2}$, alors

$$\forall n\in\mathbb{N},\ \forall x\in I,\ P_n(x) = \frac{(-1)^n}{2^n}e^{x^2}\frac{\partial}{\partial x^n}\left(e^{-x^2}\right)$$

p. 140

Lemme 61. On suppose que $\forall n \in \mathbb{N}$, $g_n \in L_1(I,\rho)$ et on considère (P_n) la famille des polynômes orthogonaux associée à ρ sur I. Alors $\forall n \in \mathbb{N}$, $g_n \in L_2(I,\rho)$. En particulier, l'algorithme de Gram-Schmidt a bien du sens et (P_n) est bien définie.

[DEV]

Application 62. On considère (P_n) la famille des polynômes orthogonaux associée à ρ sur I et on suppose qu'il existe $a > 0$ tel que

$$\int_I e^{a|x|}\rho(x)\,\mathrm{d}x < +\infty$$

alors (P_n) est une base hilbertienne de $L_2(I,\rho)$ pour la norme $\|.\|_2$.

Contre-exemple 63. On considère, sur $I = \mathbb{R}_*^+$, la fonction poids $\rho : x \mapsto x^{-\ln(x)}$. Alors, la famille des g_n n'est pas totale. La famille des polynômes orthogonaux associée à ce poids particulier n'est donc pas totale non plus : ce n'est pas une base hilbertienne.

2. Application aux séries de Fourier

Notation 64.
— Pour tout $p \in [1,+\infty]$, on note $L_p^{2\pi}$ l'espace des fonctions $f : \mathbb{R} \to \mathbb{C}$, 2π-périodiques et mesurables, telles que $\|f\|_p < +\infty$.
— Pour tout $n \in \mathbb{Z}$, on note e_n la fonction 2π-périodique définie pour tout $t \in \mathbb{R}$ par $e_n(t) = e^{int}$.

[Z-Q] p. 73

Proposition 65. $L_2^{2\pi}$ est un espace de Hilbert pour le produit scalaire

$$\langle .,. \rangle : (f,g) \mapsto \frac{1}{2\pi}\int_0^{2\pi} f(t)\overline{g(t)}\,\mathrm{d}t$$

Théorème 66. La famille $(e_n)_{n\in\mathbb{Z}}$ est une base hilbertienne de $L_2^{2\pi}$.

[BMP] p. 123

Corollaire 67 (Égalité de Parseval)**.**

$$\forall f \in L_2^{2\pi},\ f = \sum_{n=-\infty}^{+\infty} \langle f, e_n\rangle e_n$$

Exemple 68. On considère $f : x \mapsto 1 - \frac{x^2}{\pi^2}$ sur $[-\pi,\pi]$. Alors,

$$\frac{\pi^4}{90} = \|f\|_2 = \sum_{n=0}^{+\infty} \frac{1}{n^4}$$

[GOU20] p. 272

Remarque 69. L'égalité du Théorème 67 est valable dans $L^{2\pi}_2$, elle signifie donc que

$$\left\| \sum_{n=-N}^{N} \langle f, e_n \rangle e_n - f \right\|_2 \longrightarrow_{N \to +\infty} 0$$

[BMP] p. 124

235 Problèmes d'interversion de symboles en analyse.

I - Problèmes d'interversion avec les suites et séries de fonctions

1. Utilisation de la convergence uniforme

[AMR11] p. 146

Théorème 1 (de la double limite)**.** Soient X une partie non vide d'un espace vectoriel normé de dimension finie, E un espace de Banach, (f_n) une suite de fonctions de X dans E et $a \in \overline{X}$. On suppose :

(i) (f_n) converge uniformément sur X.

(ii) $\forall n \in \mathbb{N}$, $f_n(x)$ admet une limite quand x tend vers a.

Alors,

$$\lim_{n\to+\infty}\left(\lim_{x\to a} f_n(x)\right) = \lim_{x\to a}\left(\lim_{n\to+\infty} f_n(x)\right)$$

Théorème 2. Soient X une partie non vide d'un espace vectoriel normé de dimension finie, E un espace de Banach, (f_n) une suite de fonctions de X dans E et $a \in X$. On suppose :

(i) (f_n) converge uniformément sur X vers f.

(ii) $\forall n \in \mathbb{N}$, $f_n(x)$ est continue en a.

Alors f est continue en a.

Exemple 3. La suite (f_n) définie sur $\mathbb{R}^+$ pour tout $n \in \mathbb{N}$ par $f_n : x \mapsto e^{-nx}$ converge vers

$$f : \begin{array}{ccc} \mathbb{R}^+ & \to & \mathbb{R}^+ \\ x & \mapsto & \begin{cases} 1 & \text{si } x = 0 \\ 0 & \text{sinon} \end{cases} \end{array}$$

Les fonctions f_n sont continues, mais f ne l'est pas : on n'a pas convergence uniforme sur $\mathbb{R}^+$.

Théorème 4. Soient I un intervalle non vide de $\mathbb{R}$, E un espace vectoriel normé et (f_n) une suite de fonctions de I dans E. On suppose :

(i) $\forall n \in \mathbb{N}$, f_n est dérivable sur I.

(ii) (f_n) converge simplement sur I vers f.

(iii) (f_n') converge uniformément sur I.

Alors f est dérivable sur I et $\forall x \in I$, $f'(x) = \lim_{n\to+\infty} f_n'(x)$.

Contre-exemple 5. La suite (f_n) définie sur $\mathbb{R}$ pour tout $n \in \mathbb{N}$ par $f_n : x \mapsto \left(x^2 + \frac{1}{n^2}\right)^{\frac{1}{2}}$ converge vers $x \mapsto |x|$, qui n'est pas dérivable à l'origine bien que les f_n le soient.

Théorème 6. Soient $I = [a,b]$ un segment non vide de $\mathbb{R}$, E un espace de Banach et (f_n) une suite de fonctions de I dans E. On suppose :

(i) $\forall n \in \mathbb{N}$, f_n est de classe $\mathscr{C}^1$ sur I.

(ii) Il existe $x_0 \in I$ tel que $(f_n(x_0))$ converge.

(iii) (f_n') converge uniformément sur I vers g.

Alors (f_n) converge uniformément sur I vers f de classe $\mathscr{C}^1$ sur I et $f' = g$.

2. Séries de fonctions et limites

Théorème 7. Soient X une partie non vide d'un espace vectoriel normé, E un espace de Banach, $\sum f_n$ une série de fonctions de X dans E et $a \in \overline{X}$. On suppose : p. 195

(i) $\sum f_n$ converge uniformément sur X.

(ii) $\forall n \in \mathbb{N}$, $f_n(x)$ admet une limite ℓ_n quand x tend vers a.

Alors, $\sum \ell_n$ converge dans E et,

$$\lim_{x\to a} \sum_{n=0}^{+\infty} f_n(x) = \sum_{n=0}^{+\infty} \lim_{x\to a} f_n(x) = \sum_{n=0}^{+\infty} \ell_n$$

Théorème 8. Soient X une partie non vide d'un espace vectoriel normé, E un espace de Banach, $\sum f_n$ une série de fonctions de X dans E et $a \in X$. On suppose :

(i) $\sum f_n$ converge uniformément sur X.

(ii) $\forall n \in \mathbb{N}$, f_n est continue en a.

Alors, $\sum_{n=0}^{+\infty} f_n$ est continue en a.

Exemple 9. La fonction $x \mapsto \sum_{n=0}^{+\infty} \frac{e^{-n|x|}}{n^2}$ est continue sur $\mathbb{R}$.

Théorème 10. Soient I un intervalle non vide de $\mathbb{R}$, E un espace de Banach et $\sum f_n$ une série de fonctions de I dans E. On suppose :

(i) $\forall n \in \mathbb{N}$, f_n est dérivable sur I.

(ii) Il existe $x_0 \in I$ tel que $\sum f_n(x_0)$ converge.

(iii) $\sum f_n'$ converge uniformément sur I.

Alors $\sum f_n$ converge simplement sur I uniformément sur tout compact de I, et,

$$\left(\sum_{n=0}^{+\infty} f_n\right)' = \sum_{n=0}^{+\infty} f_n'$$

Exemple 11. La fonction $\zeta : s \mapsto \sum_{n=1}^{+\infty} \frac{1}{n^s}$ est $\mathscr{C}^\infty$ sur $]1,+\infty[$ et,

$$\forall k \in \mathbb{N},\ \forall s \in]1,+\infty[,\ \zeta^{(k)}(s) = (-1)^k \sum_{n=1}^{+\infty} \frac{(\ln(s))^k}{n^s}$$

3. Le cas des séries entières

Définition 12. On appelle **série entière** toute série de fonctions de la forme $\sum a_n z^n$ où z est une variable complexe et où (a_n) est une suite complexe.

[GOU20] p. 247

Lemme 13 (Abel)**.** Soient $\sum a_n z^n$ une série entière et $z_0 \in \mathbb{C}$ tels que $(a_n z_0^n)$ soit bornée. Alors :

(i) $\forall z \in \mathbb{C}$ tel que $|z| < |z_0|$, $\sum a_n z^n$ converge absolument.

(ii) $\forall r \in]0,|z_0|[$, $\sum a_n z^n$ converge normalement dans $\overline{D}(0,r) = \{z \in \mathbb{C} \mid |z| \leq r\}$.

Définition 14. En reprenant les notations précédentes, le nombre

$$R = \sup\{r \geq 0 \mid (|a_n| r^n) \text{ est bornée}\}$$

est le **rayon de convergence** de $\sum a_n z^n$.

Exemple 15.
— $\sum n^2 z^n$ a un rayon de convergence égal à 1.
— $\sum \frac{z^n}{n!}$ a un rayon de convergence infini. On note $z \mapsto e^z$ la fonction somme.

p. 255

Proposition 16. Soit $\sum a_n z^n$ une série entière de rayon de convergence $r \neq 0$. Alors $S \in \mathscr{H}(D(0,r))$ et,

$$S'(z) = \sum_{n=0}^{+\infty} n a_n z^{n-1}$$

pour tout $z \in D(0,r)$.

Plus précisément, pour tout $k \in \mathbb{N}$, S est k fois dérivable avec

$$S^{(k)}(z) = \sum_{n=k}^{+\infty} n(n-1)\dots(n-k+1) a_n z^{n-k}$$

[QUE] p. 57

[DEV]

Théorème 17 (Abel angulaire)**.** Soit $\sum a_n z^n$ une série entière de rayon de convergence supérieur ou égal à 1 telle que $\sum a_n$ converge. On note f la somme de cette série sur le disque unité D de $\mathbb{C}$. On fixe $\theta_0 \in \left[0, \frac{\pi}{2}\right[$ et on pose $\Delta_{\theta_0} = \{z \in D \mid \exists \rho > 0 \text{ et } \exists \theta \in [-\theta_0, \theta_0] \text{ tels que } z = 1 - \rho e^{i\theta}\}$.

Alors $\lim\limits_{\substack{z \to 1 \\ z \in \Delta_{\theta_0}}} f(z) = \sum_{n=0}^{+\infty} a_n$.

[GOU20] p. 263

Application 18.

$$\sum_{n=0}^{+\infty} \frac{(-1)^n}{(2n+1)} = \frac{\pi}{4}$$

Application 19.

$$\sum_{n=0}^{+\infty} \frac{(-1)^{n-1}}{n} = \ln(2)$$

Contre-exemple 20. La réciproque est fausse :

$$\lim_{\substack{z \to 1 \\ |z|<1}} (-1)^n z^n = \lim_{\substack{z \to 1 \\ |z|<1}} \frac{1}{1+z} = \frac{1}{2}$$

Théorème 21 (Taubérien faible)**.** Soit $\sum a_n z^n$ une série entière de rayon de convergence 1. On note f la somme de cette série sur $D(0,1)$. On suppose que

$$\exists S \in \mathbb{C} \text{ tel que } \lim_{\substack{x \to 1 \\ x<1}} f(x) = S$$

Si $a_n = o\left(\frac{1}{n}\right)$, alors $\sum a_n$ converge et $\sum_{n=0}^{+\infty} a_n = S$.

Remarque 22. Ce dernier résultat est une réciproque partielle du Théorème 17. Il reste vrai en supposant $a_n = O\left(\frac{1}{n}\right)$ (c'est le théorème Taubérien fort).

II - Problèmes d'interversion en intégration

On se place dans un espace mesuré $(X, \mathscr{A}, \mu)$.

1. Intégrale d'une suite de fonctions

Théorème 23 (Convergence monotone)**.** Soit (f_n) une suite croissante de fonctions mesurables positives. Alors, la limite f de cette suite est mesurable positive, et,

$$\int_X f \,\mathrm{d}\mu = \lim_{n\to+\infty} \int_X f_n \,\mathrm{d}\mu$$

[B-P] p. 124

Application 24. Soient f, g deux fonctions mesurables positives.

(i) $f \leq g \implies \int_X f \,\mathrm{d}\mu \leq \int_X g \,\mathrm{d}\mu$ (l'intégrale est croissante).

(ii) $\int_X (f+g)\,\mathrm{d}\mu = \int_X f \,\mathrm{d}\mu + \int_X g \,\mathrm{d}\mu$ (l'intégrale est additive).

(iii) $\forall \lambda \geq 0$, $\int_X \lambda f \,\mathrm{d}\mu = \lambda \int_X f \,\mathrm{d}\mu$ (l'intégrale est positivement homogène).

(iv) Si $f = g$ pp., alors $\int_X f \,\mathrm{d}\mu = \int_X g \,\mathrm{d}\mu$.

Théorème 25 (Lemme de Fatou)**.** Soit (f_n) une suite de fonctions mesurables positives. Alors,

$$0 \leq \int_X \liminf f_n \,\mathrm{d}\mu \leq \liminf \int_X f_n \,\mathrm{d}\mu \leq +\infty$$

p. 137

Exemple 26. Soit f croissante sur $[0,1]$, continue en 0 et dérivable en 1 et dérivable pp. dans $[0,1]$. Alors,

$$\int_0^1 f'(x)\,\mathrm{d}x \leq f(1) - f(0)$$

Théorème 27 (Convergence dominée)**.** Soit (f_n) une suite d'éléments de $\mathscr{L}_1$ telle que :

(i) pp. en x, $(f_n(x))$ converge dans $\mathbb{K}$ vers $f(x)$.

(ii) $\exists g \in \mathscr{L}_1$ positive telle que

$$\forall n \in \mathbb{N},\ \text{pp. en } x,\ |f_n(x)| \leq g(x)$$

Alors,

$$\int_X f \,\mathrm{d}\mu = \lim_{n\to+\infty} \int_X f_n \,\mathrm{d}\mu \text{ et } \lim_{n\to+\infty} \int_X |f_n - f| \,\mathrm{d}\mu = 0$$

Exemple 28. — On reprend l'Théorème 26 et on suppose f partout dérivable sur $[0,1]$ de dérivée bornée. Alors l'inégalité est une égalité.

— Soit $\alpha > 1$. On pose $\forall n \geq 1$, $I_n(\alpha) = \int_0^n \left(1 + \frac{x}{n}\right)^n e^{-\alpha x} \, \mathrm{d}x$. Alors,

$$\lim_{n \to +\infty} I_n(\alpha) = \int_0^{+\infty} e^{(1-\alpha)x} \, \mathrm{d}x = \frac{1}{\alpha - 1}$$

Exemple 29.

$$\lim_{n \to +\infty} \int_0^{+\infty} \frac{x^n}{x^{2n} + 1} \, \mathrm{d}x = 0$$

[AMR11] p. 156

Application 30 (Lemme de Borel-Cantelli)**.** Soit (A_n) une famille de parties de $\mathscr{A}$. Alors,

$$\sum_{n=1}^{+\infty} \mu(A_n) < +\infty \implies \mu\left(\limsup_{n \to +\infty} A_n\right) = 0$$

[B-P] p. 144

2. Intégrale à paramètre

Soit $f : E \times X \to \mathbb{C}$ où (E, d) est un espace métrique. On pose $F : t \mapsto \int_X f(t,x) \, \mathrm{d}\mu(x)$.

[Z-Q] p. 312

a. Continuité

Théorème 31 (Continuité sous le signe intégral)**.** On suppose :

(i) $\forall t \in E$, $x \mapsto f(t,x)$ est mesurable.

(ii) pp. en $x \in X$, $t \mapsto f(t,x)$ est continue en $t_0 \in E$.

(iii) $\exists g \in L_1(X)$ positive telle que

$$|f(t,x)| \leq g(x) \quad \forall t \in E, \text{pp. en } x \in X$$

Alors F est continue en t_0.

Corollaire 32. On suppose :

(i) $\forall t \in E$, $x \mapsto f(t,x)$ est mesurable.

(ii) pp. en $x \in X$, $t \mapsto f(t,x)$ est continue sur E.

(iii) $\forall K \subseteq E$, $\exists g_K \in L_1(X)$ positive telle que

$$|f(t,x)| \leq g_K(x) \quad \forall t \in E, \text{pp. en } x$$

Alors F est continue sur E.

p. 318

Exemple 33. La fonction

$$\Gamma : \begin{array}{ccc} \mathbb{R}_*^+ & \to & \mathbb{R}_*^+ \\ t & \mapsto & \int_0^{+\infty} t^{x-1} e^{-t}\,\mathrm{d}t \end{array}$$

est bien définie et continue sur $\mathbb{R}_*^+$.

Exemple 34. Soit $f : \mathbb{R}^+ \to \mathbb{C}$ intégrable. Alors, [G-K] p. 104

$$\lambda \mapsto \int_0^{+\infty} e^{-\lambda t} f(t)\,\mathrm{d}t$$

est bien définie et est continue sur $\mathbb{R}^+$.

b. Dérivabilité

On suppose ici que E est un intervalle I ouvert de $\mathbb{R}$.

[Z-Q] p. 313

Théorème 35 (Dérivation sous le signe intégral)**.** On suppose :

(i) $\forall t \in I, x \mapsto f(t,x) \in L_1(X)$.

(ii) pp. en $x \in X$, $t \mapsto f(t,x)$ est dérivable sur I. On notera $\frac{\partial f}{\partial t}$ cette dérivée définie presque partout.

(iii) $\forall K \subseteq I$ compact, $\exists g_K \in L_1(X)$ positive telle que

$$\left|\frac{\partial f}{\partial t}(x,t)\right| \leq g_K(x) \quad \forall t \in I, \text{pp. en } x$$

Alors $\forall t \in I, x \mapsto \frac{\partial f}{\partial t}(x,t) \in L_1(X)$ et F est dérivable sur I avec

$$\forall t \in I, F'(t) = \int_X \frac{\partial f}{\partial t}(x,t)\,\mathrm{d}\mu(x)$$

Remarque 36.
— Si dans le Théorème 35, hypothèse (i), on remplace "dérivable" par "$\mathscr{C}^1$", alors la fonction F est de classe $\mathscr{C}^1$.
— On a un résultat analogue pour les dérivées d'ordre supérieur.

Théorème 37 (k-ième dérivée sous le signe intégral)**.** On suppose :

(i) $\forall t \in I, x \mapsto f(t,x) \in L_1(X)$.

(ii) pp. en $x \in X$, $t \mapsto f(t,x) \in \mathscr{C}^k(I)$. On notera $\left(\frac{\partial}{\partial t}\right)^j f$ la j-ième dérivée définie presque partout pour $j \in [\![0,k]\!]$.

(iii) $\forall j \in [\![0,k]\!]$, $\forall K \subseteq I$ compact, $\exists g_{j,K} \in L_1(X)$ positive telle que

$$\left|\left(\frac{\partial}{\partial t}\right)^j f(x,t)\right| \leq g_{j,K}(x) \quad \forall t \in K, \text{pp. en } x$$

Alors $\forall j \in [\![0,k]\!]$, $\forall t \in I$, $x \mapsto \left(\frac{\partial}{\partial t}\right)^j f(x,t) \in L_1(X)$ et $F \in \mathscr{C}^k(I)$ avec

$$\forall j \in [\![0,k]\!],\ \forall t \in I,\ F^{(j)}(t) = \int_X \left(\frac{\partial}{\partial t}\right)^j f(x,t)\,\mathrm{d}\mu(x)$$

Exemple 38. La fonction Γ de l'Théorème 33 est $\mathscr{C}^\infty$ sur $\mathbb{R}_*^+$. p. 318

Exemple 39. On se place dans l'espace mesuré $(\mathbb{N}, \mathscr{P}(\mathbb{N}), \text{card})$ et on considère (f_n) une suite de fonctions dérivables sur I telle que [B-P] p. 149

$$\forall x \in \mathbb{R},\ \sum_{n\in\mathbb{N}} |f_n(x)| + \sup_{x\in I} |f_n'(t)| < +\infty$$

Alors $x \mapsto \sum_{n\in\mathbb{N}} f_n(x)$ est dérivable sur I de dérivée $x \mapsto \sum_{n\in\mathbb{N}} f_n'(x)$.

Application 40 (Transformée de Fourier d'une Gaussienne)**.** En résolvant une équation différentielle linéaire, on a [GOU20] p. 169

$$\forall \alpha > 0,\ \forall x \in \mathbb{R},\ \int_{\mathbb{R}} e^{-\alpha t^2} e^{-itx}\,\mathrm{d}t = \sqrt{\frac{\pi}{\alpha}} e^{-\frac{x^2}{\pi\alpha}}$$

[DEV]

Application 41 (Intégrale de Dirichlet)**.** On pose $\forall x \geq 0$, [G-K] p. 107

$$F(x) = \int_0^{+\infty} \frac{\sin(t)}{t} e^{-xt}\,\mathrm{d}t$$

alors :

(i) F est bien définie et est continue sur $\mathbb{R}^+$.

(ii) F est dérivable sur $\mathbb{R}_*^+$ et $\forall x \in \mathbb{R}_*^+$, $F'(x) = -\frac{1}{1+x^2}$.

(iii) $F(0) = \int_0^{+\infty} \frac{\sin(t)}{t}\,\mathrm{d}t = \frac{\pi}{2}$.

c. Holomorphie

On suppose ici que E est un ouvert Ω de $\mathbb{C}$.

[Z-Q] p. 314

Théorème 42 (Holomorphie sous le signe intégral)**.** On suppose :

(i) $\forall z \in \Omega,\ x \mapsto f(z,x) \in L_1(X)$.

(ii) pp. en $x \in X$, $z \mapsto f(z,x)$ est holomorphe dans Ω. On notera $\frac{\partial f}{\partial z}$ cette dérivée définie presque partout.

(iii) $\forall K \subseteq \Omega$ compact, $\exists g_K \in L_1(X)$ positive telle que

$$|f(x,z)| \leq g_K(x) \quad \forall z \in K, \text{pp. en } x$$

Alors F est holomorphe dans Ω avec

$$\forall z \in \Omega,\ F'(z) = \int_X \frac{\partial f}{\partial z}(z,t)\,\mathrm{d}\mu(z)$$

p. 318

Exemple 43. La fonction Γ de l'Théorème 33 est holomorphe dans l'ouvert $\{z \in \mathbb{C} \mid \mathrm{Re}(z) > 0\}$.

3. Intégrale sur un espace produit

[B-P] p. 237

Théorème 44 (Fubini-Tonelli)**.** Soient $(Y, \mathscr{B}, \nu)$ un autre espace mesuré et $f : (X \times Y) \to \overline{\mathbb{R}^+}$. On suppose μ et ν σ-finies. Alors :

(i) $x \mapsto \int_Y f(x,y)\,\mathrm{d}\nu(y)$ et $y \mapsto \int_X f(x,y)\,\mathrm{d}\mu(x)$ sont mesurables.

(ii) Dans $\overline{\mathbb{R}^+}$,

$$\int_{X\times Y} f\,\mathrm{d}(\mu\otimes\nu) = \int_X \left(\int_Y f(x,y)\,\mathrm{d}\nu(y)\right) = \int_Y \left(\int_X f(x,y)\,\mathrm{d}\mu(x)\right)$$

Théorème 45 (Fubini-Lebesgue)**.** Soient $(Y, \mathscr{B}, \nu)$ un autre espace mesuré et $f \in \mathscr{L}_1(\mu\otimes\nu)$. Alors :

(i) Pour tout $y \in Y$, $x \mapsto f(x,y)$ et pour tout $x \in X$, $y \mapsto f(x,y)$ sont intégrables.

(ii) $x \mapsto \int_Y f(x,y)\,\mathrm{d}\nu(y)$ et $y \mapsto \int_X f(x,y)\,\mathrm{d}\mu(x)$ sont intégrables, les fonctions étant définies pp.

(iii) On a :

$$\int_{X\times Y} f\,\mathrm{d}(\mu\otimes\nu) = \int_X \left(\int_Y f(x,y)\,\mathrm{d}\nu(y)\right) = \int_Y \left(\int_X f(x,y)\,\mathrm{d}\mu(x)\right)$$

Contre-exemple 46. On considère $f : (x,y) \mapsto 2e^{-2xy} - e^{-xy}$. Alors, $\int_{[0,1]} \left(\int_{\mathbb{R}^+} f(x,y)\,\mathrm{d}x \right) \mathrm{d}y = 0$, mais $\int_{\mathbb{R}^+} \left(\int_{[0,1]} f(x,y)\,\mathrm{d}y \right) \mathrm{d}x = \ln(2)$.

Exemple 47. Soient $f : (x,y) \mapsto xy$ et $D = \{(x,y) \in \mathbb{R}^2 \mid x,y \geq 0 \text{ et } x+y \leq 1\}$. Alors, [GOU20] p. 359

$$\int\int_D = f(x,y)\,\mathrm{d}x\mathrm{d}y = \int_0^1 x\frac{(1-x)^2}{2}\,\mathrm{d}x = \frac{1}{24}$$

III - Problèmes d'interversion en analyse de Fourier

1. Séries de Fourier

Définition 48. Soit $f : \mathbb{R} \to \mathbb{C}$ une application 2π-périodique et continue par morceaux sur $\mathbb{R}$. On appelle **coefficients de Fourier** de f les nombres complexes définis par p. 267

$$\forall n \in \mathbb{Z},\ c_n(f) = \int_0^{2\pi} f(t)e^{-int}\,\mathrm{d}t$$

La **série de Fourier** associée à f est

$$\sum_{n\in\mathbb{Z}} c_n(f)e^{inx}$$

Théorème 49 (Parseval)**.** Soit $f : \mathbb{R} \to \mathbb{C}$ une application 2π-périodique et continue par morceaux sur $\mathbb{R}$. Alors la série de Fourier de f est convergente et,

$$\sum_{n=-\infty}^{+\infty} |c_n(f)|^2 = \frac{1}{2\pi}\int_0^{2\pi} |f(t)|\,\mathrm{d}t$$

Exemple 50. Avec $f : x \mapsto 1 - \frac{x^2}{\pi^2}$, on obtient $\sum_{n=1}^{+\infty} \frac{1}{n^4} = \frac{\pi^4}{90}$.

Théorème 51 (Jordan-Dirichlet)**.** Soit $f : \mathbb{R} \to \mathbb{C}$ une application 2π-périodique et $\mathscr{C}^1$ par morceaux sur $\mathbb{R}$. Alors la série de Fourier de f est convergente en tout point $x \in \mathbb{R}$ et sa somme en ce point vaut

$$\frac{f(x^+) + f(x^-)}{2}$$

Exemple 52. Toujours avec $f : x \mapsto 1 - \frac{x^2}{\pi^2}$, on obtient $\sum_{n=1}^{+\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$.

2. Transformée de Fourier

[AMR08] p. 109

Définition 53. Soit $f : \mathbb{R}^d \to \mathbb{C}$ une fonction mesurable. On définit, lorsque cela a un sens, sa **transformée de Fourier**, notée $\widehat{f}$ par

$$\widehat{f} : \begin{array}{ccc} \mathbb{R}^d & \to & \mathbb{C} \\ \xi & \mapsto & \int_{\mathbb{R}^d} f(x) e^{-i\langle x,\xi\rangle} \, \mathrm{d}x \end{array}$$

Exemple 54 (Densité de Poisson)**.** On pose $\forall x \in \mathbb{R}$, $p(x) = \frac{1}{2} e^{-|x|}$. Alors $p \in L_1(\mathbb{R})$ et, $\forall \xi \in \mathbb{R}$, $\widehat{p}(\xi) = \frac{1}{1+\xi^2}$.

Lemme 55 (Riemann-Lebesgue)**.** Soit $f \in L_1(\mathbb{R}^d)$, $\widehat{f}$ existe et

$$\lim_{\|\xi\| \to +\infty} \widehat{f}(\xi)$$

Théorème 56. $\forall f \in L_1(\mathbb{R}^d)$, $\widehat{f}$ est continue, bornée par $\|f\|_1$. Donc la **transformation de Fourier**

$$\mathscr{F} : \begin{array}{ccc} L_1(\mathbb{R}^d) & \to & \mathscr{C}_0(\mathbb{R}^d) \\ f & \mapsto & \widehat{f} \end{array}$$

est bien définie.

Corollaire 57. La transformation de Fourier $\mathscr{F} : L_1(\mathbb{R}^d) \to \mathscr{C}_0(\mathbb{R}^d)$ est une application linéaire continue.

Exemple 58.

$$\forall \xi \in \mathbb{R}, \widehat{\mathbb{1}_{[-1,1]}}(\xi) = \begin{cases} \frac{2\sin(\xi)}{\xi} \text{ si } \xi \neq 0 \\ 2 \text{ sinon} \end{cases}$$

Remarquons ici que la transformée de Fourier n'est pas intégrable.

Théorème 59 (Formule de dualité)**.**

$$\forall f, g \in L_1(\mathbb{R}^d), \int_{\mathbb{R}^d} f(t)\widehat{g}(t) \, \mathrm{d}t = \int_{\mathbb{R}^d} \widehat{f}(t) g(t) \, \mathrm{d}t$$

Corollaire 60. La transformation de Fourier $\mathscr{F} : L_1(\mathbb{R}^d) \to \mathscr{C}_0(\mathbb{R}^d)$ est une application injective.

Théorème 61 (Formule d'inversion de Fourier)**.** Si $f \in L_1(\mathbb{R}^d)$ est telle que $\widehat{f} \in L_1(\mathbb{R}^d)$, alors

$$\widehat{\widehat{f}}(x) = (2\pi)^d f(x) \text{ pp. en } x \in \mathbb{R}^d$$

Théorème 62 (Formule sommatoire de Poisson)**.** Soit $f : \mathbb{R} \to \mathbb{C}$ une fonction de classe $\mathscr{C}^1$ telle que $f(x) = O\left(\frac{1}{x^2}\right)$ et $f'(x) = O\left(\frac{1}{x^2}\right)$ quand $|x| \longrightarrow +\infty$. Alors :

[GOU20] p. 284

$$\forall x \in \mathbb{R}, \sum_{n\in\mathbb{Z}} f(x+n) = \sum_{n\in\mathbb{Z}} \widehat{f}(2\pi n) e^{2i\pi nx}$$

Application 63 (Identité de Jacobi)**.**

$$\forall s > 0, \sum_{n=-\infty}^{+\infty} e^{-\pi n^2 s} = \frac{1}{\sqrt{s}} \sum_{n=-\infty}^{+\infty} e^{-\frac{\pi n^2}{s}}$$

236 Illustrer par des exemples quelques méthodes de calcul d'intégrales de fonctions d'une ou plusieurs variables.

I - Méthodes de base pour les fonction d'une variable

1. Primitives

Théorème 1 (Fondamental de l'analyse)**.** Soit $f : [a,b] \to E$ (où $[a,b] \subseteq \mathbb{R}$ est un segment et E un espace de Banach sur $\mathbb{R}$ ou $\mathbb{C}$). [GOU20] p. 127

(i) L'application

$$F : \begin{array}{ccc} [a,b] & \to & E \\ x & \mapsto & \int_a^x f(t)\,\mathrm{d}t \end{array}$$

est $\mathscr{C}^1$ par morceaux, continue, dérivable à gauche et à droite sur $[a,b]$ telle que

$$F'_g(x) = \lim_{\substack{t\to x \\ t<x}} f'(t) \text{ et } F'_d(x) = \lim_{\substack{t\to x \\ t>x}} f'(t)$$

(ii) Si f est continue sur $[a,b]$, F est de classe $\mathscr{C}^1$ sur $[a,b]$ avec $F'(x) = f(x)$ pour tout $x \in [a,b]$.

Corollaire 2. Soit $[a,b] \subseteq \mathbb{R}$ un segment. Toute application continue $f : [a,b] \to \mathbb{R}$ admet au moins une primitive, et pour toute primitive F de f sur $[a,b]$, on a

$$\int_a^b f(x)\,\mathrm{d}x = [F(x)]_a^b = F(b) - F(a)$$

Exemple 3. Pour tout $n \in \mathbb{N}$, on note $W_n = \int_0^{\frac{\pi}{2}} \sin(x)^n\,\mathrm{d}x$. Alors, $W_0 = \frac{\pi}{2}$ et $W_1 = 1$.

Proposition 4. Soit $F \in \mathbb{R}(X)$. Pour intégrer $x \mapsto F(x)$, on fait une décomposition en éléments simples de F, qui nous ramène à calculer des primitives de la forme p. 137

$$\int \frac{\mathrm{d}x}{(x-a)^h}\,\mathrm{d}x \text{ et } \int \frac{ax+b}{(x^2+cx+d)^h}\,\mathrm{d}x$$

où $h \in \mathbb{N}^*$ et $c - 4d < 0$.

Exemple 5.

$$\int^{x} \frac{1-x}{(x^2+x+1)^2}\,\mathrm{d}x = \frac{x+1}{x^2+x+1} + \frac{2}{\sqrt{3}}\arctan\left(\frac{2x+1}{\sqrt{3}}\right) + k \text{ avec } k \in \mathbb{R}$$

2. Changement de variable

Théorème 6 (Changement de variable)**.** Soit $[a,b] \subseteq \mathbb{R}$ un segment. Soit $\varphi : [a,b] \to \mathbb{R}$ une application de classe $\mathscr{C}^1$ et $f : I \to E$ où I est un intervalle tel que $\varphi([a,b]) \subseteq I$. Alors,

$$\int_a^b f(\varphi(t))\varphi'(t)\,\mathrm{d}t = \int_{\varphi(a)}^{\varphi(b)} f(u)\,\mathrm{d}u$$

p. 127

Exemple 7.

$$\int_0^{\frac{\pi}{2}} \ln(\sin(x))\,\mathrm{d}x = -\frac{\pi\ln(2)}{2}$$

p. 178

Proposition 8 (Règle de Bioche)**.** Soit $R \in \mathbb{R}(X,Y)$. Pour calculer une primitive d'une fonction de la forme $f : x \mapsto R(\sin(x),\cos(x))$, on peut utiliser la règle de Bioche :

(i) Si $f(x)\,\mathrm{d}x$ reste inchangé en changeant x en $\pi - x$, on pose $t = \sin(x)$.

(ii) Si $f(x)\,\mathrm{d}x$ reste inchangé en changeant x en $-x$, on pose $t = \cos(x)$.

(iii) Si $f(x)\,\mathrm{d}x$ reste inchangé en changeant x en $\pi + x$, on pose $t = \tan(x)$.

p. 139

Exemple 9.

$$\int^{u} \frac{\sin(x)^3}{1+\cos(x)^2}\,\mathrm{d}x \overset{t=\cos(x)}{=} \int^{\cos(u)} \frac{1-t^2}{1+t^2}(-\mathrm{d}t) = \cos(u) - 2\arctan(\cos(u)) + k \text{ avec } k \in \mathbb{R}$$

3. Intégration par parties

Théorème 10 (Intégration par parties)**.** Soit $[a,b] \subseteq \mathbb{R}$ un segment. Soient $u, v : [a,b] \to \mathbb{C}$ deux fonctions de classe $\mathscr{C}^1$. Alors,

$$\int_a^b u(x)v'(x)\,\mathrm{d}x = [u(x)v(x)]_a^b - \int_a^b u'(x)v(x)\,\mathrm{d}x$$

p. 127

p. 162

Exemple 11 (Fonction Γ d'Euler)**.** On pose

$$\forall x > 0, \Gamma(x) = \int_0^{+\infty} e^{-t} t^{x-1} \, \mathrm{d}t$$

Alors,

$$\forall x > 0, \Gamma(x+1) = x\Gamma(x)$$

et en particulier, $\forall n \in \mathbb{N}, \Gamma(n) = n!$.

Exemple 12 (Intégrales de Wallis)**.** En reprenant l'Théorème 3, on a p. 130

$$\forall p \in \mathbb{N}^*, W_{2p} = \frac{(2p-1)(2p-3)\dots 1}{2p(2p-2)\dots 2}\frac{\pi}{2} \text{ et } W_{2p+1} = \frac{2p(2p-2)\dots 2}{(2p-1)(2p-3)\dots 1}$$

Application 13 (Intégrale de Gauss)**.** p. 167

$$I = \int_0^{+\infty} e^{-t^2} \, \mathrm{d}t = \frac{\sqrt{\pi}}{2}$$

II - Méthodes pour les fonctions de plusieurs variables

1. Intégration sur un espace produit

Théorème 14 (Fubini-Tonelli)**.** Soient $(X, \mathscr{A}, \mu)$ et $(Y, \mathscr{B}, \nu)$ deux espaces mesurés et $f : (X \times Y) \to \overline{\mathbb{R}^+}$. On suppose μ et ν σ-finies. Alors : **[B-P]** p. 237

(i) $x \mapsto \int_Y f(x,y) \, \mathrm{d}\nu(y)$ et $y \mapsto \int_X f(x,y) \, \mathrm{d}\mu(x)$ sont mesurables.

(ii) Dans $\overline{\mathbb{R}^+}$,

$$\int_{X\times Y} f \, \mathrm{d}(\mu \otimes \nu) = \int_X \left(\int_Y f(x,y) \, \mathrm{d}\nu(y) \right) = \int_Y \left(\int_X f(x,y) \, \mathrm{d}\mu(x) \right)$$

Théorème 15 (Fubini-Lebesgue)**.** Soient $(X, \mathscr{A}, \mu)$ et $(Y, \mathscr{B}, \nu)$ deux espaces mesurés et $f \in \mathscr{L}_1(\mu \otimes \nu)$. Alors :

(i) Pour tout $y \in Y$, $x \mapsto f(x,y)$ et pour tout $x \in X$, $y \mapsto f(x,y)$ sont intégrables.

(ii) $x \mapsto \int_Y f(x,y) \, \mathrm{d}\nu(y)$ et $y \mapsto \int_X f(x,y) \, \mathrm{d}\mu(x)$ sont intégrables, les fonctions étant définies pp.

(iii) On a :

$$\int_{X\times Y} f \, \mathrm{d}(\mu \otimes \nu) = \int_X \left(\int_Y f(x,y) \, \mathrm{d}\nu(y) \right) = \int_Y \left(\int_X f(x,y) \, \mathrm{d}\mu(x) \right)$$

Contre-exemple 16. On considère $f : (x,y) \mapsto 2e^{-2xy} - e^{-xy}$. Alors, $\int_{[0,1]} \left(\int_{\mathbb{R}^+} f(x,y)\,\mathrm{d}x \right) \mathrm{d}y = 0$, mais $\int_{\mathbb{R}^+} \left(\int_{[0,1]} f(x,y)\,\mathrm{d}y \right) \mathrm{d}x = \ln(2)$.

Exemple 17. Soient $f : (x,y) \mapsto xy$ et $D = \{(x,y) \in \mathbb{R}^2 \mid x,y \geq 0 \text{ et } x+y \leq 1\}$. Alors, [GOU20] p. 359

$$\int\int_D = f(x,y)\,\mathrm{d}x\mathrm{d}y = \int_0^1 x\frac{(1-x)^2}{2}\,\mathrm{d}x = \frac{1}{24}$$

2. Changement de variable généralisé

Théorème 18. Soient E et F deux espaces de Banach et $U \subseteq E$ un ouvert.Soit $\varphi : U \to \mathbb{R}^n$ un difféomorphisme de classe $\mathscr{C}^1$. Alors, $V = \varphi(U)$ est mesurable et tout fonction f appartient à L_1 si et seulement si $|\det \mathrm{Jac}(\varphi)_a| f \circ \varphi$ appartient à L_1. Dans ce cas, [BMP] p. 9

$$\int_V f(x)\,\mathrm{d}x = \int_U |\det \mathrm{Jac}(\varphi)_a| f(\varphi(y))\,\mathrm{d}y$$

Exemple 19 (Coordonnées polaires)**.** L'application [GOU20] p. 355

$$\begin{array}{ccc} \mathbb{R}^+ \times [0,2\pi] & \to & \mathbb{R} \times \mathbb{R} \\ (r,\theta) & \mapsto & (r\cos(\theta), r\sin(\theta)) \end{array}$$

est un difféomorphisme de classe $\mathscr{C}^1$ donc le jacobien en $(r,\theta) \in \mathbb{R}^+ \times [0,2\pi]$ vaut r.

Exemple 20 (Coordonnées sphériques)**.** L'application

$$\begin{array}{ccc} \mathbb{R}^+ \times [0,2\pi] \times \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] & \to & \mathbb{R} \times \mathbb{R} \times \mathbb{R} \\ (r,\theta,\varphi) & \mapsto & (r\cos(\varphi)\cos(\theta), r\cos(\varphi)\sin(\theta), r\sin(\varphi)) \end{array}$$

est un difféomorphisme de classe $\mathscr{C}^1$ donc le jacobien en $(r,\theta,\varphi) \in \mathbb{R}^+ \times [0,2\pi] \times \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$ vaut $r^2\cos(\varphi)$.

Application 21 (Intégrale de Gauss)**.** En passant en coordonnées polaires,

$$\int_{\mathbb{R}} e^{-x^2}\,\mathrm{d}x = \sqrt{\pi}$$

III - Utilisation des théorèmes d'intégration

Soit $(X, \mathscr{A}, \mu)$ et $(Y, \mathscr{B}, \nu)$ un espace mesuré.

1. Convergence dominée

Théorème 22 (Convergence dominée)**.** Soit (f_n) une suite d'éléments de $\mathscr{L}_1$ telle que : [B-P] p. 140

(i) pp. en x, $(f_n(x))$ converge dans $\mathbb{K}$ vers $f(x)$.

(ii) $\exists g \in \mathscr{L}_1$ positive telle que

$$\forall n \in \mathbb{N}, \text{ pp. en } x, |f_n(x)| \leq g(x)$$

Alors,

$$\int_X f \, \mathrm{d}\mu = \lim_{n\to+\infty} \int_X f_n \, \mathrm{d}\mu \text{ et } \lim_{n\to+\infty} \int_X |f_n - f| \, \mathrm{d}\mu = 0$$

Exemple 23. Soit $\alpha > 1$. On pose $\forall n \geq 1$, $I_n(\alpha) = \int_0^n \left(1 + \frac{x}{n}\right)^n e^{-\alpha x} \, \mathrm{d}x$. Alors,

$$\lim_{n\to+\infty} I_n(\alpha) = \int_0^{+\infty} e^{(1-\alpha)x} \, \mathrm{d}x = \frac{1}{\alpha - 1}$$

Exemple 24. [AMR11] p. 156

$$\lim_{n\to+\infty} \int_0^{+\infty} \frac{x^n}{x^{2n}+1} \, \mathrm{d}x = 0$$

Exemple 25. [G-K] p. 104

$$\sum_{n=0}^{+\infty} \frac{(-1)^n}{3n+1} = \int_0^1 \frac{\mathrm{d}x}{x^3+1} \, \mathrm{d}x = \frac{3\ln(2) + \sqrt{3}\pi}{9}$$

2. Régularité sous l'intégrale

Soit $f : E \times X \to \mathbb{C}$ où (E, d) est un espace métrique. On pose $F : t \mapsto \int_X f(t,x) \, \mathrm{d}\mu(x)$. [Z-Q] p. 312

Théorème 26 (Continuité sous le signe intégral)**.** On suppose :

(i) $\forall t \in E$, $x \mapsto f(t,x)$ est mesurable.

(ii) pp. en $x \in X$, $t \mapsto f(t,x)$ est continue en $t_0 \in E$.

(iii) $\exists g \in L_1(X)$ positive telle que

$$|f(t,x)| \leq g(x) \quad \forall t \in E, \text{pp. en } x \in X$$

Alors F est continue en t_0.

Exemple 27. La fonction Γ de l'Théorème 11 est bien définie et continue sur $\mathbb{R}_*^+$. p. 318

On suppose maintenant que E est un intervalle I ouvert de $\mathbb{R}$. p. 313

Théorème 28 (Dérivation sous le signe intégral)**.** On suppose :

(i) $\forall t \in I,\ x \mapsto f(t,x) \in L_1(X)$.

(ii) pp. en $x \in X$, $t \mapsto f(t,x)$ est dérivable sur I. On notera $\frac{\partial f}{\partial t}$ cette dérivée définie presque partout.

(iii) $\forall K \subseteq I$ compact, $\exists g_K \in L_1(X)$ positive telle que

$$\left|\frac{\partial f}{\partial t}(x,t)\right| \leq g_K(x) \quad \forall t \in I, \text{pp. en } x$$

Alors $\forall t \in I,\ x \mapsto \frac{\partial f}{\partial t}(x,t) \in L_1(X)$ et F est dérivable sur I avec

$$\forall t \in I,\ F'(t) = \int_X \frac{\partial f}{\partial t}(x,t)\,\mathrm{d}\mu(x)$$

Application 29 (Transformée de Fourier d'une Gaussienne)**.** En résolvant une équation différentielle linéaire, on a [GOU20] p. 169

$$\forall \alpha > 0,\ \forall x \in \mathbb{R},\ \int_{\mathbb{R}} e^{-\alpha t^2} e^{-itx}\,\mathrm{d}t = \sqrt{\frac{\pi}{\alpha}} e^{-\frac{x^2}{\pi\alpha}}$$

[DEV]

Application 30 (Intégrale de Dirichlet)**.** On pose $\forall x \geq 0$, [G-K] p. 107

$$F(x) = \int_0^{+\infty} \frac{\sin(t)}{t} e^{-xt}\,\mathrm{d}t$$

alors :

(i) F est bien définie et est continue sur $\mathbb{R}^+$.

(ii) F est dérivable sur $\mathbb{R}_*^+$ et $\forall x \in \mathbb{R}_*^+,\ F'(x) = -\frac{1}{1+x^2}$.

(iii) $F(0) = \int_0^{+\infty} \frac{\sin(t)}{t}\,\mathrm{d}t = \frac{\pi}{2}$.

IV - Utilisation de l'analyse complexe

1. Formule intégrale de Cauchy

Soit Ω un ouvert de $\mathbb{C}$. Soit $f : \Omega \to \mathbb{C}$.

[QUE] p. 134

Théorème 31 (Cauchy homologique)**.** Soit Γ un cycle homologue à zéro dans Ω (ie. tel que $z \notin \Omega \implies I(a,\Gamma) = 0$). On suppose $f \in \mathscr{H}(\Omega)$. Alors,

$$\int_\Gamma f(z)\,\mathrm{d}z = 0$$

Corollaire 32 (Formule intégrale de Cauchy)**.** Soit Γ un cycle homologue à zéro dans Ω. On suppose $f \in \mathscr{H}(\Omega)$. Alors,

$$z_0 \in \Omega \setminus \Gamma^* \implies \frac{1}{2i\pi}\int_\Gamma \frac{f(z)}{z-z_0}\,\mathrm{d}z = I(z_0,\gamma) f(z_0)$$

p. 85

Corollaire 33. On a $\mathscr{H}(\Omega) \subseteq \mathscr{A}(\Omega)$. De plus, si $a \in \Omega$ et que l'on pose $d = d(a, \mathbb{C}\setminus\Omega)$, on a

$$f(a+h) = \sum_{n=0}^{+\infty} a_n h^n \text{ pour } |h| < d \text{ avec } a_n = \frac{f^{(n)}(a)}{n!} = \frac{1}{2i\pi}\int_{C^+(a,d)} \frac{f(z)}{(z-a)^{n+1}}\,\mathrm{d}z$$

[BMP] p. 64

[DEV]

Application 34 (Transformée de Fourier d'une gaussienne)**.** On définit $\forall a \in \mathbb{R}_*^+$,

[AMR08] p. 156

$$\gamma_a : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & e^{-ax^2} \end{array}$$

Alors,

$$\forall \xi \in \mathbb{R},\ \widehat{\gamma_a}(\xi) = \sqrt{\frac{\pi}{a}}\, e^{\frac{-\xi^2}{4a}}$$

2. Théorème des résidus

[QUE] p. 169

Théorème 35 (des résidus)**.** On suppose f méromorphe sur Ω et on note A l'ensemble de ses pôles. Soit γ une courbe homologue à zéro dans Ω et ne rencontrant pas A. Alors,

$$\int_\gamma f(z)\,\mathrm{d}z = 2i\pi \sum_{a\in A} I(a,\gamma)\,\mathrm{Res}(f,a)$$

p. 173

Exemple 36.

$$\int_0^{2\pi} \frac{1}{3+2\cos(t)}\,\mathrm{d}t = \frac{2\pi}{\sqrt{5}}$$

Exemple 37 (Intégrale de Dirichlet)**.**

$$\int_0^{+\infty} \frac{\sin(x)}{x}\,\mathrm{d}x = \frac{\pi}{2}$$

V - Calcul approché d'intégrales

Soit f une fonction réelle continue sur un intervalle $[a,b]$. On se donne $n+1$ points $x_0,\dots,x_n \in [a,b]$ distincts deux-à-deux. [DEM] p. 21

Définition 38. Pour $i \in [\![0,n]\!]$, on définit le i-ième **polynôme de Lagrange** associé à $x_1,\dots,x_n$ par

$$\ell_i : x \mapsto \prod_{\substack{j=0 \\ j\neq i}}^{n} \frac{x-x_j}{x_i-x_j}$$

Théorème 39. Il existe une unique fonction polynômiale p_n de degré n telle que $\forall i \in [\![0,n]\!]$, $p_n(x_i) = f(x_i)$:

$$p_n = \sum_{i=0}^{n} f(x_i)\ell_i$$

Théorème 40. On note $\pi_{n+1} : x \mapsto \prod_{j=0}^{n}(x-x_j)$ et on suppose f $n+1$ fois dérivable $[a,b]$. Alors, pour tout $x \in [a,b]$, il existe un réel $\xi_x \in]\min(x,x_i),\max(x,x_i)[$ tel que

$$f(x) - p_n(x) = \frac{\pi_{n+1}(x)}{(n+1)!} f^{(n+1)}(\xi_x)$$

Corollaire 41.

$$\|f-p_n\|_\infty \leq \frac{1}{(n+1)!}\|\pi_{n+1}\|_\infty \|f^{(n+1)}\|_\infty$$

Application 42 (Calculs approchés d'intégrales)**.** On note $I(f) = \int_a^b f(t)\,\mathrm{d}t$. L'objectif est d'approximer $I(f)$ par une expression $P(f)$ et de majorer l'erreur d'approximation $E(f) = |I(f)-P(f)|$. [DAN] p. 506

(i) Méthode des rectangles. On suppose f continue. Avec $P(f) = (b-a)f(a)$, on a $E(f) \leq \frac{(b-a)^2}{2}\|f'\|_\infty$.

(ii) Méthode du point milieu. On suppose f de classe $\mathscr{C}^2$. Avec $P(f) = (b-a)f\left(\frac{a+b}{2}\right)$, on

a $E(f) \leq \frac{(b-a)^3}{24}\|f''\|_\infty$.

(iii) Méthode des trapèzes. On suppose f de classe $\mathscr{C}^2$. Avec $P(f) = \frac{b-a}{2}(f(a)+f(b))$, on a $E(f) \leq \frac{(b-a)^3}{12}\|f''\|_\infty$.

(iv) Méthode de Simpson. On suppose f de classe $\mathscr{C}^4$. Avec $P(f) = \frac{b-a}{6}\left(f(a)+f(b)+4f\left(\frac{a+b}{2}\right)\right)$, on a $E(f) \leq \frac{(b-a)^3}{2880}\|f^{(4)}\|_\infty$.

239 Fonctions définies par une intégrale dépendant d'un paramètre. Exemples et applications.

I - Régularité d'une fonction définie par une intégrale à paramètre

Soient $(X, \mathcal{A}, \mu)$ un espace mesuré et $f : E \times X \to \mathbb{C}$ où (E, d) est un espace métrique. On pose $F : t \mapsto \int_X f(t,x)\,\mathrm{d}\mu(x)$.

1. Continuité

Théorème 1 (Continuité sous le signe intégral)**.** On suppose :

(i) $\forall t \in E$, $x \mapsto f(t,x)$ est mesurable.

(ii) pp. en $x \in X$, $t \mapsto f(t,x)$ est continue en $t_0 \in E$.

(iii) $\exists g \in L_1(X)$ positive telle que

$$|f(t,x)| \leq g(x) \quad \forall t \in E, \text{pp. en } x \in X$$

Alors F est continue en t_0.

[Z-Q] p. 312

Corollaire 2. On suppose :

(i) $\forall t \in E$, $x \mapsto f(t,x)$ est mesurable.

(ii) pp. en $x \in X$, $t \mapsto f(t,x)$ est continue sur E.

(iii) $\forall K \subseteq E$, $\exists g_K \in L_1(X)$ positive telle que

$$|f(t,x)| \leq g_K(x) \quad \forall t \in E, \text{pp. en } x$$

Alors F est continue sur E.

Exemple 3. La fonction

$$\Gamma : \begin{array}{ccc} \mathbb{R}_*^+ & \to & \mathbb{R}_*^+ \\ t & \mapsto & \int_0^{+\infty} t^{x-1} e^{-t}\,\mathrm{d}t \end{array}$$

est bien définie et continue sur $\mathbb{R}_*^+$.

p. 318

Exemple 4. Soit $f : \mathbb{R}^+ \to \mathbb{C}$ intégrable. Alors,

$$\lambda \mapsto \int_0^{+\infty} e^{-\lambda t} f(t)\,\mathrm{d}t$$

[G-K] p. 104

est bien définie et est continue sur $\mathbb{R}^+$.

2. Dérivabilité

On suppose ici que E est un intervalle I ouvert de $\mathbb{R}$.

[Z-Q] p. 313

Théorème 5 (Dérivation sous le signe intégral)**.** On suppose :

(i) $\forall t \in I, x \mapsto f(t,x) \in L_1(X)$.

(ii) pp. en $x \in X$, $t \mapsto f(t,x)$ est dérivable sur I. On notera $\frac{\partial f}{\partial t}$ cette dérivée définie presque partout.

(iii) $\forall K \subseteq I$ compact, $\exists g_K \in L_1(X)$ positive telle que

$$\left|\frac{\partial f}{\partial t}(x,t)\right| \leq g_K(x) \quad \forall t \in I, \text{pp. en } x$$

Alors $\forall t \in I, x \mapsto \frac{\partial f}{\partial t}(x,t) \in L_1(X)$ et F est dérivable sur I avec

$$\forall t \in I, F'(t) = \int_X \frac{\partial f}{\partial t}(x,t)\,\mathrm{d}\mu(x)$$

Remarque 6.
— Si dans le Théorème 5, hypothèse (i), on remplace "dérivable" par "$\mathscr{C}^1$", alors la fonction F est de classe $\mathscr{C}^1$.
— On a un résultat analogue pour les dérivées d'ordre supérieur.

Théorème 7 (k-ième dérivée sous le signe intégral)**.** On suppose :

(i) $\forall t \in I, x \mapsto f(t,x) \in L_1(X)$.

(ii) pp. en $x \in X$, $t \mapsto f(t,x) \in \mathscr{C}^k(I)$. On notera $\left(\frac{\partial}{\partial t}\right)^j f$ la j-ième dérivée définie presque partout pour $j \in [\![0,k]\!]$.

(iii) $\forall j \in [\![0,k]\!]$, $\forall K \subseteq I$ compact, $\exists g_{j,K} \in L_1(X)$ positive telle que

$$\left|\left(\frac{\partial}{\partial t}\right)^j f(x,t)\right| \leq g_{j,K}(x) \quad \forall t \in K, \text{pp. en } x$$

Alors $\forall j \in [\![0,k]\!]$, $\forall t \in I, x \mapsto \left(\frac{\partial}{\partial t}\right)^j f(x,t) \in L_1(X)$ et $F \in \mathscr{C}^k(I)$ avec

$$\forall j \in [\![0,k]\!], \forall t \in I, F^{(j)}(t) = \int_X \left(\frac{\partial}{\partial t}\right)^j f(x,t)\,\mathrm{d}\mu(x)$$

Exemple 8. La fonction Γ de l'Théorème 3 est $\mathscr{C}^\infty$ sur $\mathbb{R}_*^+$.

p. 318

[ROM19-1] p. 364

Lemme 9. La fonction Γ définie pour tout $x > 0$ par $\Gamma(x) = \int_0^{+\infty} t^{x-1} e^{-t} \, \mathrm{d}t$ vérifie :

(i) $\forall x \in \mathbb{R}_*^+, \Gamma(x+1) = x\Gamma(x)$.

(ii) $\Gamma(1) = 1$.

(iii) Γ est log-convexe sur $\mathbb{R}_*^+$.

[DEV]

Théorème 10 (Bohr-Mollerup)**.** Soit $f : \mathbb{R}_*^+ \to \mathbb{R}^+$ vérifiant le Point (i), le Point (ii) et le Point (iii) du Théorème 9. Alors $f = \Gamma$.

Exemple 11. On se place dans l'espace mesuré $(\mathbb{N}, \mathscr{P}(\mathbb{N}), \mathrm{card})$ et on considère (f_n) une suite de fonctions dérivables sur I telle que

$$\forall x \in \mathbb{R}, \sum_{n\in\mathbb{N}} |f_n(x)| + \sup_{x\in I} |f_n'(t)| < +\infty$$

Alors $x \mapsto \sum_{n\in\mathbb{N}} f_n(x)$ est dérivable sur I de dérivée $x \mapsto \sum_{n\in\mathbb{N}} f_n'(x)$.

[B-P] p. 149

Application 12 (Transformée de Fourier d'une Gaussienne)**.** En résolvant une équation différentielle linéaire, on a

$$\forall \alpha > 0, \forall x \in \mathbb{R}, \int_{\mathbb{R}} e^{-\alpha t^2} e^{-itx} \, \mathrm{d}t = \sqrt{\frac{\pi}{\alpha}} e^{-\frac{x^2}{\pi\alpha}}$$

[GOU20] p. 169

[DEV]

Application 13 (Intégrale de Dirichlet)**.** On pose $\forall x \geq 0$,

$$F(x) = \int_0^{+\infty} \frac{\sin(t)}{t} e^{-xt} \, \mathrm{d}t$$

alors :

(i) F est bien définie et est continue sur $\mathbb{R}^+$.

(ii) F est dérivable sur $\mathbb{R}_*^+$ et $\forall x \in \mathbb{R}_*^+, F'(x) = -\frac{1}{1+x^2}$.

(iii) $F(0) = \int_0^{+\infty} \frac{\sin(t)}{t} \, \mathrm{d}t = \frac{\pi}{2}$.

[G-K] p. 107

3. Holomorphie

On suppose ici que E est un ouvert Ω de $\mathbb{C}$.

Théorème 14 (Holomorphie sous le signe intégral)**.** On suppose :

(i) $\forall z \in \Omega, x \mapsto f(z,x) \in L_1(X)$.

(ii) pp. en $x \in X$, $z \mapsto f(z,x)$ est holomorphe dans Ω. On notera $\frac{\partial f}{\partial z}$ cette dérivée définie presque partout.

[Z-Q] p. 314

(iii) $\forall K \subseteq \Omega$ compact, $\exists g_K \in L_1(X)$ positive telle que

$$|f(x,z)| \leq g_K(x) \quad \forall z \in K, \text{pp. en } x$$

Alors F est holomorphe dans Ω avec

$$\forall z \in \Omega,\ F'(z) = \int_X \frac{\partial f}{\partial z}(z,t)\,\mathrm{d}\mu(z)$$

Exemple 15. La fonction Γ de l'Théorème 3 est holomorphe dans l'ouvert $\{z \in \mathbb{C} \mid \mathrm{Re}(z) > 0\}$. p. 318

II - Produit de convolution

1. Notion de convolée de deux fonctions

Définition 16. Soient f et g deux fonctions de $\mathbb{R}^d$ dans $\mathbb{R}$. On dit que **la convolée** (ou **le produit de convolution**) de f et g en $x \in \mathbb{R}$ **existe** si la fonction [AMR08] p. 75

$$\begin{array}{ccc} \mathbb{R} & \to & \mathbb{C} \\ t & \mapsto & f(x-t)g(t) \end{array}$$

est intégrable sur $\mathbb{R}^d$ pour la mesure de Lebesgue. On pose alors :

$$(f*g)(x) = \int_{\mathbb{R}^d} f(x-t)g(t)\,\mathrm{d}t$$

Proposition 17. Dans $L_1(\mathbb{R}^d)$, le produit de convolution est commutatif, bilinéaire et associatif.

Théorème 18. Soient $p, q > 0$ et $f \in L_p(\mathbb{R}^d)$ et $g \in L_q(\mathbb{R}^d)$.

(i) Si $p, q \in [1, +\infty]$ tels que $\frac{1}{p} + \frac{1}{q} = 1$, alors $(f*g)(x)$ existe pour tout $x \in \mathbb{R}^d$ et est uniformément continue. On a, $\|f*g\|_\infty \leq \|f\|_p \|g\|_q$ et, si $p \neq 1, +\infty$, $f*g \in \mathscr{C}_0(\mathbb{R})$.

(ii) Si $p = 1$ et $q = +\infty$, alors $(f*g)(x)$ existe pour tout $x \in \mathbb{R}^d$ et $f*g \in \mathscr{C}_b(\mathbb{R})$.

(iii) Si $p = 1$ et $q \in [1, +\infty[$, alors $(f*g)(x)$ existe pp. en $x \in \mathbb{R}^d$ et $f*g \in L_q(\mathbb{R})$ telle que $\|f*g\|_q \leq \|f\|_1 \|g\|_q$.

(iv) Si $p = 1$ et $q = 1$, alors $(f*g)(x)$ existe pp. en $x \in \mathbb{R}^d$ et $f*g \in L_1(\mathbb{R})$ telle que $\|f*g\|_1 \leq \|f\|_1 \|g\|_1$.

Exemple 19. Soient $a < b \in \mathbb{R}_*^+$. Alors $\mathbb{1}_{[-a,a]} * \mathbb{1}_{[-b,b]}$ existe pour tout $x \in \mathbb{R}$ et

$$\left(\mathbb{1}_{[-a,a]} * \mathbb{1}_{[-b,b]}\right)(x) = \begin{cases} 2a & \text{si } 0 \leq |x| \leq b-a \\ b+a-|x| & \text{si } b-a \leq |x| \leq b+a \\ 0 & \text{sinon} \end{cases}$$

Proposition 20. $L_1(\mathbb{R}^d)$ est une algèbre de Banach pour le produit de convolution. p. 85

Remarque 21. Cette algèbre n'a pas d'élément neutre. Afin de pallier à ce manque, nous allons voir la notion d'approximation de l'identité dans la sous-section suivante.

2. Approximation de l'identité

Définition 22. On appelle **approximation de l'identité** toute suite (ρ_n) de fonctions mesurables de $L_1(\mathbb{R}^d)$ telles que **[B-P]** p. 306

(i) $\forall n \in \mathbb{N}$, $\int_{\mathbb{R}^d} \rho_n \, \mathrm{d}\lambda_d = 1$.

(ii) $\sup_{n\geq 1} \|\rho_n\| < +\infty$.

(iii) $\forall \epsilon > 0$, $\lim_{n\to+\infty} \int_{\mathbb{R}\setminus B(0,\epsilon)} \rho_n(x)\,\mathrm{d}x = 0$.

Remarque 23. Dans la définition précédente, (ii) implique (i) lorsque les fonctions ρ_n sont positives. Plutôt que des suites, on pourra considérer les familles indexées par $\mathbb{R}_*^+$.

Exemple 24.

— Noyau de Laplace sur $\mathbb{R}$:

$$\forall t > 0,\ \rho_t(x) = \frac{1}{2t} e^{-\frac{|x|}{t}}$$

— Noyau de Cauchy sur $\mathbb{R}$:

$$\forall t > 0,\ \rho_t(x) = \frac{t}{\pi(t^2+x^2)}$$

— Noyau de Gauss sur $\mathbb{R}$:

$$\forall t > 0,\ \rho_t(x) = \frac{1}{\sqrt{2\pi}t} e^{-\frac{|x|^2}{2t^2}}$$

Application 25 (Théorème de Weierstrass)**.** Toute fonction continue $f : [a,b] \to \mathbb{R}$ (avec $a, b \in \mathbb{R}$ tels que $a \leq b$) est limite uniforme de fonctions polynômiales sur $[a,b]$. **[GOU20]** p. 304

Théorème 26. Soit (ρ_n) une approximation de l'identité. Soient $p \in [1, +\infty[$ et $f \in L_p(\mathbb{R}^d)$, alors :

$$\forall n \geq 1,\ f * \rho_n \in L_p(\mathbb{R}^d) \quad \text{et} \quad \|f * \rho_n - f\|_p \longrightarrow 0$$

[B-P] p. 307

Théorème 27. Soient (ρ_n) une approximation de l'identité et $f \in L_\infty(\mathbb{R}^d)$. Alors :

- Si f est continue en $x_0 \in \mathbb{R}^d$, alors $(f * \rho_n)(x_0) \longrightarrow_{n\to+\infty} f(x_0)$.
- Si f est uniformément continue sur $\mathbb{R}^d$, alors $\|f * \rho_n - f\|_\infty \longrightarrow_{n\to+\infty} 0$.
- Si f est continue sur un compact K, alors $\sup_{x\in K} |(f * \rho_n)(x) - f(x)| \longrightarrow_{n\to+\infty} 0$.

Définition 28. On qualifie de **régularisante** toute suite (α_n) d'approximations de l'identité telle que $\forall n \in \mathbb{N}$, $\alpha_n \in \mathscr{C}^\infty_K(\mathbb{R}^d)$.

Exemple 29. Soit $\alpha \in \mathscr{C}^\infty_K(\mathbb{R}^d)$ une densité de probabilité. Alors la suite (α_n) définie pour tout $n \in \mathbb{N}$ par $\alpha_n : x \mapsto n\alpha(nx)$ est régularisante.

p. 274

Application 30. (i) $\mathscr{C}^\infty_K(\mathbb{R}^d)$ est dense dans $\mathscr{C}_K(\mathbb{R}^d)$ pour $\|.\|_\infty$.
(ii) $\mathscr{C}^\infty_K(\mathbb{R}^d)$ est dense dans $L_p(\mathbb{R}^d)$ pour $\|.\|_p$ avec $p \in [1, +\infty[$.

[AMR08] p. 96

III - Transformée de Fourier

1. Sur $L_1(\mathbb{R}^d)$

Définition 31. Soit $f : \mathbb{R}^d \to \mathbb{C}$ une fonction mesurable. On définit, lorsque cela a un sens, sa **transformée de Fourier**, notée $\widehat{f}$ par

$$\widehat{f} : \begin{array}{ccc} \mathbb{R}^d & \to & \mathbb{C} \\ \xi & \mapsto & \int_{\mathbb{R}^d} f(x) e^{-i\langle x,\xi\rangle}\,\mathrm{d}x \end{array}$$

p. 109

Lemme 32 (Riemann-Lebesgue)**.** Soit $f \in L_1(\mathbb{R}^d)$, $\widehat{f}$ existe et

$$\lim_{\|\xi\|\to+\infty} \widehat{f}(\xi)$$

Théorème 33. $\forall f \in L_1(\mathbb{R}^d)$, $\widehat{f}$ est continue, bornée par $\|f\|_1$. Donc la transformation de Fourier

$$\mathscr{F} : \begin{array}{ccc} L_1(\mathbb{R}^d) & \to & \mathscr{C}_0(\mathbb{R}^d) \\ f & \mapsto & \widehat{f} \end{array}$$

est bien définie.

Corollaire 34. La transformation de Fourier $\mathscr{F} : L_1(\mathbb{R}^d) \to \mathscr{C}_0(\mathbb{R}^d)$ est une application linéaire continue.

Exemple 35 (Densité de Poisson)**.** On pose $\forall x \in \mathbb{R}$, $p(x) = \frac{1}{2}e^{-|x|}$. Alors $p \in L_1(\mathbb{R})$ et, $\forall \xi \in \mathbb{R}$, $\widehat{p}(\xi) = \frac{1}{1+\xi^2}$.

Exemple 36.

$$\forall \xi \in \mathbb{R},\ \widehat{\mathbb{1}_{[-1,1]}}(\xi) = \begin{cases} \frac{2\sin(\xi)}{\xi} \text{ si } \xi \neq 0 \\ 2 \text{ sinon} \end{cases}$$

Remarquons ici que la transformée de Fourier n'est pas intégrable.

Proposition 37. p. 114

$$\forall f, g \in L_1(\mathbb{R}^d),\ \widehat{f * g} = \widehat{f}\widehat{g}$$

Théorème 38 (Formule de dualité)**.**

$$\forall f, g \in L_1(\mathbb{R}^d),\ \int_{\mathbb{R}^d} f(t)\widehat{g}(t)\,\mathrm{d}t = \int_{\mathbb{R}^d} \widehat{f}(t)g(t)\,\mathrm{d}t$$

Corollaire 39. La transformation de Fourier $\mathscr{F} : L_1(\mathbb{R}^d) \to \mathscr{C}_0(\mathbb{R}^d)$ est une application injective.

Application 40. Soient I un intervalle de $\mathbb{R}$ et ρ une fonction poids. On considère (P_n) la famille des polynômes orthogonaux associée à ρ sur I. On suppose qu'il existe $a > 0$ tel que **[BMP]** p. 140

$$\int_I e^{a|x|}\rho(x)\,\mathrm{d}x < +\infty$$

alors (P_n) est une base hilbertienne de $L_2(I, \rho)$ pour la norme $\|.\|_2$.

[AMR08] p. 116

Théorème 41 (Formule d'inversion de Fourier)**.** Si $f \in L_1(\mathbb{R}^d)$ est telle que $\widehat{f} \in L_1(\mathbb{R}^d)$, alors

$$\widehat{\widehat{f}}(x) = (2\pi)^d f(x) \text{ pp. en } x \in \mathbb{R}^d$$

Proposition 42. Soient $g \in L_1(\mathbb{R}^d)$ et $f \in L_1(\mathbb{R}^d)$ telle que $\widehat{f} \in L_1(\mathbb{R}^d)$, alors

$$\widehat{fg} = \frac{1}{(2\pi)^d} \widehat{f} * \widehat{g}$$

2. Sur $L_2(\mathbb{R}^d)$

Théorème 43 (Plancherel-Parseval)**.**

$$\forall f \in L_1(\mathbb{R}^d),\ \|\widehat{f}\|_2^2 = (2\pi)^d \|f\|_2^2$$

Théorème 44. Soit $f \in L_2(\mathbb{R}^d)$. Alors :

(i) Il existe une suite (f_n) de $L_1(\mathbb{R}^d) \cap L_2(\mathbb{R}^d)$ qui converge vers f dans $L_2(\mathbb{R}^d)$.

(ii) Pour une telle suite (f_n), la suite $(\widehat{f_n})$ converge dans $L_2(\mathbb{R}^d)$ vers une limite $\widetilde{f}$ indépendante de la suite choisie.

Définition 45. La limite $\widetilde{f}$ est la **transformée de Fourier** de f dans $L_2(\mathbb{R}^d)$.

Proposition 46. Les transformations de Fourier $L_1(\mathbb{R}^d)$ et $L_2(\mathbb{R}^d)$ coïncident sur $L_1(\mathbb{R}^d) \cap L_2(\mathbb{R}^d)$.

3. Application en probabilités

Définition 47. Soit X un vecteur aléatoire. On appelle **fonction caractéristique** de X, notée ϕ_X, la transformée de Fourier de la loi $\mathbb{P}_X$ (définie à un signe près) :

$$\phi_X : t \mapsto \mathbb{E}(e^{i\langle t,x\rangle})$$

[G-K] p. 239

Théorème 48. Soient X et Y deux vecteurs aléatoires. Alors,

$$\phi_X = \phi_Y \iff \mathbb{P}_X = \mathbb{P}_Y$$

Corollaire 49. Soient X et Y deux vecteurs aléatoires tels que $\forall a \in \mathbb{R}^d$, $\langle X, a\rangle$ et $\langle Y, a\rangle$ ont même loi. Alors, X et Y ont même loi.

241 Suites et séries de fonctions. Exemples et contre-exemples.

I - Convergences de suite et de séries de fonctions

1. Suites de fonctions

Définition 1. Soient (f_n) et f respectivement une suite de fonctions et une fonction définies sur un ensemble X à valeurs dans un espace métrique (E,d). On dit que : [GOU20] p. 231

— (f_n) **converge simplement** vers f si

$$\forall x \in X,\ \forall \epsilon > 0,\ \exists N \in \mathbb{N} \text{ tel que } \forall n \geq N,\ d(f_n(x), f(x)) < \epsilon$$

— (f_n) **converge uniformément** vers f si

$$\forall \epsilon > 0,\ \exists N \in \mathbb{N} \text{ tel que } \forall n \geq N,\ \forall x \in X,\ d(f_n(x), f(x)) < \epsilon$$

Proposition 2. La convergence uniforme entraîne la convergence simple.

Contre-exemple 3. La réciproque est fausse. Il suffit en effet de considérer la suite (f_n) définie pour tout $n \in \mathbb{N}$ et pour tout $x \in [0,1]$ par $f_n(x) = x^n$ converge simplement sur $[0,1]$ mais pas uniformément.

Théorème 4 (Critère de Cauchy uniforme)**.** Soit (f_n) une suite de fonctions définies sur un ensemble X à valeurs dans un espace métrique (E,d). Alors (f_n) converge uniformément si

$$\forall \epsilon > 0,\ \exists N \in \mathbb{N} \text{ tel que } \forall p > q \geq N, \forall x \in X,\ d(f_p(x), f_q(x)) < \epsilon$$

Corollaire 5. Une limite uniforme sur $\mathbb{R}$ de fonctions polynômiales est une fonction polynômiale. p. 237

Notation 6. — Pour toute fonction g bornée sur un ensemble X et à valeurs dans un espace vectoriel normé $(E, \|.\|)$, on note p. 232

$$\|g\|_\infty = \sup_{x \in X} \|g(x)\|$$

— On note $\mathscr{B}(X,E)$ l'ensemble des applications bornées de X dans E.

Proposition 7. En reprenant les notations précédentes, une suite de fonctions (f_n) de $\mathscr{B}(X,E)$ converge uniformément vers $f \in \mathscr{B}(X,E)$ si $\|f_n - f\|_\infty \longrightarrow_{n\to+\infty} 0$.

Exemple 8. La suite de fonctions (f_n) définie pour tout $n \in \mathbb{N}$ par $f_n : x \mapsto \left(1-\frac{x}{n}\right)^n \mathbb{1}_{[0,n]}$ converge uniformément vers $f : x \mapsto e^{-x}$ sur $\mathbb{R}^+$.

2. Séries de fonctions

p. 232

Définition 9. Soit (g_n) une suite de fonctions. On appelle **série de fonctions** de terme général g_n, notée $\sum g_n$ la suite de fonctions (S_n) où

$$\forall n \in \mathbb{N},\ S_n = \sum_{k=0}^{n} g_k$$

Définition 10. Soient X un ensemble et $(E, \|.\|)$ un espace vectoriel normé. On dit qu'une série de fonctions à termes dans $\mathscr{B}(X,E)$ **converge normalement** si la série numérique $\sum \|g_n\|_\infty$ converge.

Remarque 11. En reprenant les notations précédentes, il est équivalent de dire qu'une série de fonctions $\sum g_n$ converge normalement s'il existe une série à termes positifs $\sum a_n$ convergente et telle que

$$\forall n \in \mathbb{N},\ \forall x \in X,\ \|g_n(x)\| \leq a_n$$

Exemple 12. La série de fonctions $\sum g_n$ où (g_n) est définie par

$$\forall n \in \mathbb{N},\ g_n : x \mapsto \frac{x^n}{n^2}$$

converge normalement sur $[0,1]$ car $\|g_n\|_\infty = \frac{1}{n^2}$.

Théorème 13. Une série de fonctions à valeurs dans un espace de Banach qui converge normalement sur un ensemble X converge uniformément sur X.

Contre-exemple 14. La réciproque est fausse. Par exemple, la série de fonctions $\sum (-1)^n g_n$ où (g_n) est définie par

$$\forall n \in \mathbb{N},\ g_n : x \mapsto \frac{x}{n^2+x^2}$$

converge uniformément sur $\mathbb{R}^+$ mais pas normalement.

3. Définition sur un compact

Théorème 15 (Théorèmes de Dini)**.** (i) Soit (f_n) une suite *croissante* de fonctions réelles *continues* définies sur un segment I de $\mathbb{R}$. Si (f_n) converge simplement vers une fonction *continue* sur I, alors la convergence est uniforme.

(ii) Soit (f_n) une suite de *fonctions croissantes* réelles *continues* définies sur un segment I de $\mathbb{R}$. Si (f_n) converge simplement vers une fonction *continue* sur I, alors la convergence est uniforme.

p. 238

Théorème 16 (Bernstein)**.** Soit $f : [0,1] \to \mathbb{C}$ continue. On note

$$B_n(f) : x \mapsto \sum_{k=0}^{n} f\left(\frac{k}{n}\right)\binom{n}{k} x^k (1-x)^{n-k}$$

Alors,

$$\|B_n(f) - f\|_\infty \longrightarrow_{n\to+\infty} 0$$

p. 242

[DEV]

Corollaire 17 (Weierstrass)**.** Toute fonction continue $f : [a,b] \to \mathbb{R}$ (avec $a, b \in \mathbb{R}$ tels que $a \leq b$) est limite uniforme de fonctions polynômiales sur $[a,b]$.

p. 304

On a une version plus générale de ce théorème.

Théorème 18 (Stone-Weierstrass)**.** Soit K un espace compact et $\mathscr{A}$ une sous-algèbre de l'algèbre de Banach réelle $\mathscr{C}(K,\mathbb{R})$. On suppose de plus que :

(i) $\mathscr{A}$ sépare les points de K (ie. $\forall x \in K, \exists f \in A$ telle que $f(x) \neq f(y)$).

(ii) $\mathscr{A}$ contient les constantes.

Alors $\mathscr{A}$ est dense dans $\mathscr{C}(K,\mathbb{R})$.

[LI] p. 46

Remarque 19. Il existe aussi une version "complexe" de ce théorème, où il faut supposer de plus que $\mathscr{A}$ est stable par conjugaison.

Exemple 20. La suite de polynômes réels (r_n) définie par récurrence par

$$r_0 = 0 \text{ et } \forall n \in \mathbb{N}, r_{n+1} : t \mapsto r_n(t) + \frac{1}{2}(t - r_n(t)^2)$$

converge vers $\sqrt{.}$ sur $[0,1]$.

II - Régularité de la limite

1. Continuité

Théorème 21 (de la double limite)**.** Soient X une partie non vide d'un espace vectoriel normé de dimension finie, E un espace de Banach, (f_n) une suite de fonctions de X dans E et $a \in \overline{X}$. On suppose :

(i) (f_n) converge uniformément sur X.

(ii) $\forall n \in \mathbb{N}$, $f_n(x)$ admet une limite quand x tend vers a.

Alors,

$$\lim_{n\to+\infty}\left(\lim_{x\to a} f_n(x)\right) = \lim_{x\to a}\left(\lim_{n\to+\infty} f_n(x)\right)$$

[AMR11] p. 146

Théorème 22. Soient X une partie non vide d'un espace vectoriel normé de dimension finie, E un espace de Banach, (f_n) une suite de fonctions de X dans E et $a \in X$. On suppose :

(i) (f_n) converge uniformément sur X vers f.

(ii) $\forall n \in \mathbb{N}$, $f_n(x)$ est continue en a.

Alors f est continue en a.

Exemple 23. La suite (f_n) définie sur $\mathbb{R}^+$ pour tout $n \in \mathbb{N}$ par $f_n : x \mapsto e^{-nx}$ converge vers

$$\begin{array}{rccc} & \mathbb{R}^+ & \to & \mathbb{R}^+ \\ f : & x & \mapsto & \begin{cases} 1 & \text{si } x = 0 \\ 0 & \text{sinon} \end{cases} \end{array}$$

Les fonctions f_n sont continues, mais f ne l'est pas : on n'a pas convergence uniforme sur $\mathbb{R}^+$.

Théorème 24. Soient X une partie non vide d'un espace vectoriel normé, E un espace de Banach, $\sum f_n$ une série de fonctions de X dans E et $a \in \overline{X}$. On suppose :

(i) $\sum f_n$ converge uniformément sur X.

(ii) $\forall n \in \mathbb{N}$, $f_n(x)$ admet une limite ℓ_n quand x tend vers a.

Alors, $\sum \ell_n$ converge dans E et,

$$\lim_{x\to a}\sum_{n=0}^{+\infty} f_n(x) = \sum_{n=0}^{+\infty}\lim_{x\to a} f_n(x) = \sum_{n=0}^{+\infty}\ell_n$$

p. 195

Théorème 25. Soient X une partie non vide d'un espace vectoriel normé, E un espace de Banach, $\sum f_n$ une série de fonctions de X dans E et $a \in X$. On suppose :

(i) $\sum f_n$ converge uniformément sur X.

(ii) $\forall n \in \mathbb{N}$, f_n est continue en a.

Alors, $\sum_{n=0}^{+\infty} f_n$ est continue en a.

Exemple 26. La fonction $x \mapsto \sum_{n=0}^{+\infty} \frac{e^{-n|x|}}{n^2}$ est continue sur $\mathbb{R}$.

2. Dérivabilité

Théorème 27. Soient I un intervalle non vide de $\mathbb{R}$, E un espace vectoriel normé et (f_n) une suite de fonctions de I dans E. On suppose : p. 148

(i) $\forall n \in \mathbb{N}$, f_n est dérivable sur I.

(ii) (f_n) converge simplement sur I vers f.

(iii) (f_n') converge uniformément sur I.

Alors f est dérivable sur I et $\forall x \in I$, $f'(x) = \lim_{n\to+\infty} f_n'(x)$.

Contre-exemple 28. La suite (f_n) définie sur $\mathbb{R}$ pour tout $n \in \mathbb{N}$ par $f_n : x \mapsto \left(x^2 + \frac{1}{n^2}\right)^{\frac{1}{2}}$ converge vers $x \mapsto |x|$, qui n'est pas dérivable à l'origine bien que les f_n le soient.

Théorème 29. Soient $I = [a, b]$ un segment non vide de $\mathbb{R}$, E un espace de Banach et (f_n) une suite de fonctions de I dans E. On suppose : p. 198

(i) $\forall n \in \mathbb{N}$, f_n est de classe $\mathscr{C}^1$ sur I.

(ii) Il existe $x_0 \in I$ tel que $(f_n(x_0))$ converge.

(iii) (f_n') converge uniformément sur I vers g.

Alors (f_n) converge uniformément sur I vers f de classe $\mathscr{C}^1$ sur I et $f' = g$.

Théorème 30. Soient I un intervalle non vide de $\mathbb{R}$, E un espace de Banach et $\sum f_n$ une série de fonctions de I dans E. On suppose :

(i) $\forall n \in \mathbb{N}$, f_n est dérivable sur I.

(ii) Il existe $x_0 \in I$ tel que $\sum f_n(x_0)$ converge.

(iii) $\sum f_n'$ converge uniformément sur I.

Alors $\sum f_n$ converge simplement sur I uniformément sur tout compact de I, et,

$$\left(\sum_{n=0}^{+\infty} f_n\right)' = \sum_{n=0}^{+\infty} f_n'$$

Exemple 31. La fonction $\zeta : s \mapsto \sum_{n=1}^{+\infty} \frac{1}{n^s}$ est $\mathscr{C}^\infty$ sur $]1,+\infty[$ et,

$$\forall k \in \mathbb{N},\ \forall s \in]1,+\infty[,\ \zeta^{(k)}(s) = (-1)^k \sum_{n=1}^{+\infty} \frac{(\ln(s))^k}{n^s}$$

3. Mesurabilité, intégrabilité

Théorème 32. Soient $I = [a,b]$ un segment non vide de $\mathbb{R}$, E un espace de Banach et (f_n) une suite de fonctions de I dans E. On suppose : [GOU20] p. 233

(i) $\forall n \in \mathbb{N}$, f_n est continue sur I.

(ii) (f_n) converge uniformément sur I vers f.

Alors f est continue et $\lim_{n\to+\infty} \int_a^b f_n(t)\,\mathrm{d}t = \int_a^b f(t)\,\mathrm{d}t$. Plus généralement, la fonction $F : x \mapsto \int_a^x f(t)\,\mathrm{d}t$ est limite uniforme sur I de la suite de fonctions (F_n) définie par

$$\forall n \in \mathbb{N},\ F_n : x \mapsto \int_a^x f_n(t)\,\mathrm{d}t$$

Remarque 33. L'interversion se fait sous des hypothèses beaucoup moins contraignantes à l'aide du théorème de convergence dominée.

Théorème 34 (Convergence monotone)**.** Soit (f_n) une suite croissante de fonctions mesurables positives. Alors, la limite f de cette suite est mesurable positive, et, [B-P] p. 124

$$\int_X f\,\mathrm{d}\mu = \lim_{n\to+\infty} \int_X f_n\,\mathrm{d}\mu$$

Théorème 35 (Lemme de Fatou)**.** Soit (f_n) une suite de fonctions mesurables positives. Alors, p. 137

$$0 \leq \int_X \liminf f_n\,\mathrm{d}\mu \leq \liminf \int_X f_n\,\mathrm{d}\mu \leq +\infty$$

Exemple 36. Soit f croissante sur $[0,1]$, continue en 0 et dérivable en 1 et dérivable pp. dans $[0,1]$. Alors,

$$\int_0^1 f'(x)\,\mathrm{d}x \leq f(1) - f(0)$$

Théorème 37 (Convergence dominée)**.** Soit (f_n) une suite d'éléments de $\mathscr{L}_1$ telle que :

(i) pp. en x, $(f_n(x))$ converge dans $\mathbb{K}$ vers $f(x)$.

(ii) $\exists g \in \mathscr{L}_1$ positive telle que

$$\forall n \in \mathbb{N}, \text{ pp. en } x, |f_n(x)| \leq g(x)$$

Alors,

$$\int_X f \, \mathrm{d}\mu = \lim_{n\to+\infty} \int_X f_n \, \mathrm{d}\mu \text{ et } \lim_{n\to+\infty} \int_X |f_n - f| \, \mathrm{d}\mu = 0$$

Exemple 38. — On reprend l'Théorème 36 et on suppose f partout dérivable sur $[0,1]$ de dérivée bornée. Alors l'inégalité est une égalité.

— Soit $\alpha > 1$. On pose $\forall n \geq 1$, $I_n(\alpha) = \int_0^n \left(1 + \frac{x}{n}\right)^n e^{-\alpha x} \, \mathrm{d}x$. Alors,

$$\lim_{n\to+\infty} I_n(\alpha) = \int_0^{+\infty} e^{(1-\alpha)x} \, \mathrm{d}x = \frac{1}{\alpha - 1}$$

Exemple 39. [AMR11] p. 156

$$\lim_{n\to+\infty} \int_0^{+\infty} \frac{x^n}{x^{2n}+1} \, \mathrm{d}x = 0$$

III - Séries particulières

1. Séries entières

Définition 40. On appelle **série entière** toute série de fonctions de la forme $\sum a_n z^n$ où z est une variable complexe et où (a_n) est une suite complexe. [GOU20] p. 247

Lemme 41 (Abel)**.** Soient $\sum a_n z^n$ une série entière et $z_0 \in \mathbb{C}$ tels que $(a_n z_0^n)$ soit bornée. Alors :

(i) $\forall z \in \mathbb{C}$ tel que $|z| < |z_0|$, $\sum a_n z^n$ converge absolument.

(ii) $\forall r \in]0, |z_0|[$, $\sum a_n z^n$ converge normalement dans $\overline{D}(0,r) = \{z \in \mathbb{C} \mid |z| \leq r\}$.

Définition 42. En reprenant les notations précédentes, le nombre

$$R = \sup\{r \geq 0 \mid (|a_n| r^n) \text{ est bornée}\}$$

est le **rayon de convergence** de $\sum a_n z^n$.

Exemple 43. — $\sum n^2 z^n$ a un rayon de convergence égal à 1. p. 255

— $\sum \frac{z^n}{n!}$ a un rayon de convergence infini. On note $z \mapsto e^z$ la fonction somme.

Proposition 44. Soit $\sum a_n z^n$ une série entière de rayon de convergence $r \neq 0$. Alors $S \in \mathscr{H}(D(0,r))$ et,

$$S'(z) = \sum_{n=0}^{+\infty} n a_n z^{n-1}$$

pour tout $z \in D(0,r)$.

Plus précisément, pour tout $k \in \mathbb{N}$, S est k fois dérivable avec

$$S^{(k)}(z) = \sum_{n=k}^{+\infty} n(n-1)\dots(n-k+1) a_n z^{n-k}$$

[QUE] p. 57

[DEV]

Théorème 45 (Abel angulaire)**.** Soit $\sum a_n z^n$ une série entière de rayon de convergence supérieur ou égal à 1 telle que $\sum a_n$ converge. On note f la somme de cette série sur le disque unité D de $\mathbb{C}$. On fixe $\theta_0 \in \left[0, \frac{\pi}{2}\right[$ et on pose $\Delta_{\theta_0} = \{z \in D \mid \exists \rho > 0 \text{ et } \exists \theta \in [-\theta_0, \theta_0] \text{ tels que } z = 1 - \rho e^{i\theta}\}$.

Alors $\lim\limits_{\substack{z \to 1 \\ z \in \Delta_{\theta_0}}} f(z) = \sum_{n=0}^{+\infty} a_n$.

[GOU20] p. 263

Application 46.

$$\sum_{n=0}^{+\infty} \frac{(-1)^n}{(2n+1)} = \frac{\pi}{4}$$

Application 47.

$$\sum_{n=0}^{+\infty} \frac{(-1)^{n-1}}{n} = \ln(2)$$

Contre-exemple 48. La réciproque est fausse :

$$\lim_{\substack{z \to 1 \\ |z|<1}} (-1)^n z^n = \lim_{\substack{z \to 1 \\ |z|<1}} \frac{1}{1+z} = \frac{1}{2}$$

Théorème 49 (Taubérien faible)**.** Soit $\sum a_n z^n$ une série entière de rayon de convergence 1. On note f la somme de cette série sur $D(0,1)$. On suppose que

$$\exists S \in \mathbb{C} \text{ tel que } \lim_{\substack{x \to 1 \\ x<1}} f(x) = S$$

Si $a_n = o\left(\frac{1}{n}\right)$, alors $\sum a_n$ converge et $\sum_{n=0}^{+\infty} a_n = S$.

Remarque 50. Ce dernier résultat est une réciproque partielle du Théorème 45. Il reste vrai en supposant $a_n = O\left(\frac{1}{n}\right)$ (c'est le théorème Taubérien fort).

2. Séries de Fourier

Notation 51. — Pour tout $p \in [1, +\infty]$, on note $L_p^{2\pi}$ l'espace des fonctions $f : \mathbb{R} \to \mathbb{C}$, 2π-périodiques et mesurables, telles que $\|f\|_p < +\infty$.

— Pour tout $n \in \mathbb{Z}$, on note e_n la fonction 2π-périodique définie pour tout $t \in \mathbb{R}$ par $e_n(t) = e^{int}$.

[Z-Q] p. 73

Définition 52. Soit $f \in L_1^{2\pi}$. On appelle :

— **Coefficients de Fourier complexes**, les complexes définis par

$$\forall n \in \mathbb{Z},\ c_n(f) = \frac{1}{2\pi}\int_0^{2\pi} f(t)e^{-int}\,\mathrm{d}t = \langle f, e_n\rangle$$

— **Série de Fourier** associée à f la série $(S_N(f))$ définie par

$$\forall N \in \mathbb{N},\ S_N(f) = \sum_{n=-N}^{N} c_n(f)e_n \overset{(*)}{=} \frac{a_0(f)}{2} + \sum_{n=1}^{N}\left(a_n(f)\cos(nx) + b_n(f)\sin(nx)\right)$$

[GOU20] p. 268

Théorème 53 (Dirichlet)**.** Soient $f : \mathbb{R} \to \mathbb{C}$ 2π-périodique, continue par morceaux sur $\mathbb{R}$ et $t_0 \in \mathbb{R}$ tels que la fonction

$$h \mapsto \frac{f(t_0+h) + f(t_0-h) - f(t_0^+) - f(t_0^-)}{h}$$

est bornée au voisinage de 0. Alors,

$$S_N(f)(t_0) \longrightarrow_{N\to+\infty} \frac{f(t_0^+) + f(t_0^-)}{2}$$

p. 271

Contre-exemple 54. Soit $f : \mathbb{R} \to \mathbb{R}$ paire, 2π-périodique telle que :

$$\forall x \in [0,\pi], f(x) = \sum_{p=1}^{+\infty} \frac{1}{p^2}\sin\left((2^{p^3}+1)\frac{x}{2}\right)$$

Alors f est bien définie et continue sur $\mathbb{R}$. Cependant, sa série de Fourier diverge en 0.

Corollaire 55. Soient $f : \mathbb{R} \to \mathbb{C}$ 2π-périodique, $\mathscr{C}^1$ par morceaux sur $\mathbb{R}$. Alors,

$$\forall x \in \mathbb{R},\ S_N(f)(x) \longrightarrow_{N\to+\infty} \frac{f(x^+)+f(x^-)}{2}$$

En particulier, si f est continue en x, la série de Fourier de f converge vers $f(x)$.

Exemple 56. En reprenant la fonction de l'Théorème 56,

$$\forall x \in [-\pi,\pi],\ f(x) = \frac{2}{3} - \frac{4}{\pi^2}\sum_{n=1}^{+\infty}(-1)^n\frac{\cos(nx)}{n^2}$$

Proposition 57. Soit $f \in L^{2\pi}_1$ et telle que sa série de Fourier converge normalement. Alors, la somme $g : x \mapsto \sum_{n=-\infty}^{+\infty} c_n(f)e_n(x)$ est une fonction continue 2π-périodique presque partout égale à f. De plus, si f est continue, l'égalité $f(x) = g(x)$ est vraie pour tout x.

[BMP] p. 128

Proposition 58. Soit $f : \mathbb{R} \to \mathbb{C}$ 2π-périodique continue et $\mathscr{C}^1$ par morceaux sur $\mathbb{R}$. Alors $(S_N(f))$ converge normalement vers f.

Application 59 (Développement eulérien de la cotangente)**.**

$$\forall u \in \mathbb{R}\setminus\pi\mathbb{Z},\ \operatorname{cotan}(u) = \frac{1}{u} + \sum_{n=1}^{+\infty}\frac{2u}{u^2-n^2\pi^2}$$

[AMR08] p. 211

Théorème 60 (Formule sommatoire de Poisson)**.** Soit $f : \mathbb{R} \to \mathbb{C}$ une fonction de classe $\mathscr{C}^1$ telle que $f(x) = O\left(\frac{1}{x^2}\right)$ et $f'(x) = O\left(\frac{1}{x^2}\right)$ quand $|x| \longrightarrow +\infty$. Alors :

$$\forall x \in \mathbb{R},\ \sum_{n\in\mathbb{Z}} f(x+n) = \sum_{n\in\mathbb{Z}} \widehat{f}(2\pi n)e^{2i\pi nx}$$

[GOU20] p. 284

Application 61 (Identité de Jacobi)**.**

$$\forall s > 0,\ \sum_{n=-\infty}^{+\infty} e^{-\pi n^2 s} = \frac{1}{\sqrt{s}}\sum_{n=-\infty}^{+\infty} e^{-\frac{\pi n^2}{s}}$$

243 Séries entières, propriétés de la somme. Exemples et applications.

I - Séries entières et rayons de convergence

1. Définitions

Définition 1. On appelle **série entière** toute série de fonctions de la forme $\sum a_n z^n$ où z est une variable complexe et où (a_n) est une suite complexe.

[GOU20] p. 247

Exemple 2. $\sum \frac{z^n}{n!}$ est une série entière.

Lemme 3 (Abel)**.** Soient $\sum a_n z^n$ une série entière et $z_0 \in \mathbb{C}$ tels que $(a_n z_0^n)$ soit bornée. Alors :

(i) $\forall z \in \mathbb{C}$ tel que $|z| < |z_0|$, $\sum a_n z^n$ converge absolument.

(ii) $\forall r \in]0, |z_0|[$, $\sum a_n z^n$ converge normalement dans $\overline{D}(0,r) = \{z \in \mathbb{C} \mid |z| \leq r\}$.

Définition 4. Soit $\sum a_n z^n$ une série entière. Le nombre

$$R = \sup\{r \geq 0 \mid (|a_n| r^n) \text{ est bornée}\}$$

est le **rayon de convergence** de $\sum a_n z^n$. On a :

— $\forall z \in \mathbb{C}$ tel que $|z| < R$, $\sum a_n z^n$ converge absolument.

— $\forall z \in \mathbb{C}$ tel que $|z| > R$, $\sum a_n z^n$ diverge.

— $\forall r \in [0, R[$, $\sum a_n z^n$ converge normalement sur $\overline{D}(0,r)$.

Le disque $D(0,R)$ est le **disque de convergence** de la série, le cercle $C(0,R)$ est le **cercle d'incertitude**.

2. Comparaison de rayons de convergence

Soient $\sum a_n z^n$ et $\sum b_n z^n$ deux séries entières dont on note R_a et R_b les rayons de convergence respectifs.

[AMR11] p. 234

Proposition 5. (i) Si $\forall n \in \mathbb{N}$, on a $|a_n| \leq |b_n|$, alors $R_a \geq R_b$.

(ii) Si $a_n = O(b_n)$, alors $R_a \geq R_b$.

(iii) Si $a_n \sim b_n$, alors $R_a = R_b$.

Exemple 6. La série entière $\sum e^{\cos(n)} z^n$ a un rayon de convergence égal à 1.

3. Calcul du rayon de convergence

Proposition 7 (Règle de d'Alembert)**.** Soit $\sum a_n z^n$ une série entière. Si $\lim_{n\to+\infty} \left|\frac{a_{n+1}}{a_n}\right| = \lambda$ avec $\lambda \in [0,+\infty]$, alors le rayon de convergence de $\sum a_n z^n$ est égal à $\frac{1}{\lambda}$.

p. 233

Exemple 8. La série entière $\sum \frac{z^n}{n!}$ a un rayon de convergence infini.

Proposition 9 (Formule d'Hadamard)**.** Le rayon de convergence d'une série entière $\sum a_n z^n$ est donné par $\frac{1}{\rho}$ où

$$\rho = \limsup_{n\to+\infty} |a_n|^{\frac{1}{n}}$$

Exemple 10. La série entière $\sum 2^n z^{2n}$ a un rayon de convergence égal à $\frac{1}{\sqrt{2}}$.

Corollaire 11 (Règle de Cauchy)**.** Soit $\sum a_n z^n$ une série entière. Si $\lim_{n\to+\infty} |a_n|^{\frac{1}{n}} = \lambda$ avec $\lambda \in [0,+\infty]$, alors le rayon de convergence de $\sum a_n z^n$ est égal à $\frac{1}{\lambda}$.

Exemple 12. La série entière $\sum \frac{n}{2^n} z^n$ a un rayon de convergence égal à 2.

4. Étude sur le cercle d'incertitude

Exemple 13. Le comportement d'une série entière peut varier sur le cercle d'incertitude suivant ses coefficients :

p. 231

- $\sum z^n$ dont le rayon de convergence est égal à 1 diverge en tout point de $C(0,1)$.
- $\sum \frac{1}{n^2} z^n$ dont le rayon de convergence est égal à 1 converge en tout point de $C(0,1)$.
- $\sum \frac{z^n}{n} z^n$ dont le rayon de convergence est égal à 1 converge en 1 mais diverge en tout autre point de $C(0,1)$.

[DEV]

Théorème 14 (Abel angulaire)**.** Soit $\sum a_n z^n$ une série entière de rayon de convergence supérieur ou égal à 1 telle que $\sum a_n$ converge. On note f la somme de cette série sur le disque unité D de $\mathbb{C}$. On fixe $\theta_0 \in \left[0, \frac{\pi}{2}\right[$ et on pose $\Delta_{\theta_0} = \{z \in D \mid \exists \rho > 0 \text{ et } \exists \theta \in [-\theta_0, \theta_0] \text{ tels que } z = 1 - \rho e^{i\theta}\}$.

[GOU20] p. 263

Alors $\lim\limits_{\substack{z\to 1\\ z\in\Delta_{\theta_0}}} f(z) = \sum_{n=0}^{+\infty} a_n$.

Application 15.

$$\sum_{n=0}^{+\infty} \frac{(-1)^n}{(2n+1)} = \frac{\pi}{4}$$

Application 16.

$$\sum_{n=0}^{+\infty} \frac{(-1)^{n-1}}{n} = \ln(2)$$

Contre-exemple 17. La réciproque est fausse :

$$\lim_{\substack{z\to 1\\ |z|<1}} (-1)^n z^n = \lim_{\substack{z\to 1\\ |z|<1}} \frac{1}{1+z} = \frac{1}{2}$$

Théorème 18 (Taubérien faible)**.** Soit $\sum a_n z^n$ une série entière de rayon de convergence 1. On note f la somme de cette série sur $D(0,1)$. On suppose que

$$\exists S \in \mathbb{C} \text{ tel que } \lim_{\substack{x\to 1\\ x<1}} f(x) = S$$

Si $a_n = o\left(\frac{1}{n}\right)$, alors $\sum a_n$ converge et $\sum_{n=0}^{+\infty} a_n = S$.

Remarque 19. Ce dernier résultat est une réciproque partielle du Théorème 14. Il reste vrai en supposant $a_n = O\left(\frac{1}{n}\right)$ (c'est le théorème Taubérien fort).

II - Propriétés

1. Opérations sur les séries entières

Soient $\sum a_n z^n$ et $\sum b_n z^n$ deux séries entières dont on note R_a et R_b les rayons de convergence respectifs. **[AMR11]** p. 235

Proposition 20. En multipliant $\sum a_n z^n$ par un scalaire, on ne change pas le rayon de convergence de la série initiale.

Définition 21. On appelle **série entière somme** la série entière $\sum (a_n + b_n) z^n$.

Proposition 22. On note R_{a+b} le rayon de convergence de la série somme. Alors $R_{a+b} \geq \min\{R_a, R_b\}$ avec égalité si $R_a \neq R_b$.

Exemple 23. Les séries entières $\sum z^n$ et $\sum -z^n$ ont leur rayon de convergence égal à 1 et la série somme un rayon de convergence infini. [GOU20] p. 248

Définition 24. On appelle **produit de Cauchy** la série entière $\sum c_n z^n$ où [AMR11] p. 235

$$\forall n \in \mathbb{N},\ c_n = \sum_{k=0}^{n} a_k b_{n-k}$$

Proposition 25. On note R_c le rayon de convergence du produit de Cauchy $\sum c_n z^n$. Alors,

(i) $R_c \geq \min\{R_a, R_b\}$.

(ii) $\forall z \in D(0, \min\{R_a, R_b\}),\ \sum_{n=0}^{+\infty} c_n z^n = (\sum_{n=0}^{+\infty} a_n z^n)(\sum_{n=0}^{+\infty} b_n z^n)$.

2. Propriétés de la somme

Dans toute cette sous-partie, $\sum a_n z^n$ désigne une série entière de rayon de convergence $R > 0$. On note S sa somme sur $D(0,R)$. [AMR11] p. 239

Proposition 26. S est continue sur $D(0,R)$.

Exemple 27. La série entière $\sum \frac{z^n}{n!}$ est continue sur $\mathbb{C}$.

Corollaire 28. $\forall p \in \mathbb{N}$, S admet un développement limité à l'ordre p au voisinage de l'origine, dont la partie régulière est donnée par $a_0 + a_1 z + \cdots + a_p z^p$.

Proposition 29. Soit $[a,b] \subseteq]-R,R[$, alors

$$\int_a^b S(x)\,\mathrm{d}x = \sum_{n=0}^{+\infty} a_n \int_a^b x^n\,\mathrm{d}x$$

Corollaire 30. Les primitives de S sont de la forme $\sum_{n=0}^{+\infty} \frac{a_n}{n+1} x^{n+1} + \alpha$ avec $\alpha \in \mathbb{C}$.

Proposition 31. S est de classe $\mathscr{C}^\infty$ sur $]-R,R[$ et

$$\forall k \in \mathbb{N},\ \forall x \in]-R,R[,\ S^{(k)}(x) = \sum_{k=0}^{+\infty} \frac{k!}{(n-k)!} a_n x^{n-k}$$

Remarque 32. En particulier, $\forall k \in \mathbb{N}$, $a_k = \frac{S^{(k)}(0)}{k!}$.

Exemple 33.
$$\forall x \in]-1,1[, \sum_{n=0}^{+\infty} (n+1)x^n = \frac{1}{(1-x)^2}$$

3. Développement en série entière

Définition 34. Soient $U \subseteq \mathbb{C}$ un ouvert et $f : U \to \mathbb{C}$. On dit que f est **développable en série entière en** $a \in U$ s'il existe $r > 0$ et $(a_n) \in \mathbb{C}^{\mathbb{N}}$ tels que $D(a,r) \subseteq U$ et

$$\forall z \in D(a,r), f(z) = \sum_{n=0}^{+\infty} a_n (z-a)^n$$

[BMP] p. 46

Exemple 35. Tout polynôme est développable en série entière en tout point de $\mathbb{R}$.

[AMR11] p. 241

Proposition 36. Soient $f : x \mapsto \sum_{n=0}^{+\infty} a_n x^n$ et $g : x \mapsto \sum_{n=0}^{+\infty} b_n x^n$ deux fonctions développables en séries entières en 0. Alors :

(i) $\forall \lambda \in \mathbb{C}$, $\lambda f + g$ est développable en série entière et son développement est
$$\sum_{n=0}^{+\infty} (\lambda a_n + b_n) x^n$$

(ii) fg est développable en série entière et son développement est le produit de Cauchy des deux séries entières.

Proposition 37. Soit $f : x \mapsto \sum_{n=0}^{+\infty} a_n x^n$ une fonction développable en série entière en 0. Alors $\exists I \subseteq \mathbb{R}$ avec $0 \in I$ tel que :

(i) f' est développable en série entière en 0 son développement est
$$\sum_{n=0}^{+\infty} (n+1) a_{n+1} x^n$$

(ii) f est donc $\mathscr{C}^\infty$.

(iii) f est continue et si F est une primitive de f sur I, F est développable en série entière en 0 son développement est
$$F(0) + \sum_{n=0}^{+\infty} \frac{a_n}{n+1} x^{n+1}$$

Exemple 38. Voici quelques développements en série entière usuels :

— $\forall x \in \mathbb{R}, e^x = \sum_{n=0}^{+\infty} \frac{x^n}{n!}$.

— $\forall x \in \mathbb{R}, \cos(x) = \sum_{n=0}^{+\infty} \frac{(-1)^n x^{2n}}{(2n)!}$ et $\sin(x) = \sum_{n=0}^{+\infty} \frac{(-1)^n x^{2n+1}}{(2n+1)!}$.

— $\forall \alpha > 0, \forall x \in]-1,1[, (1+x)^\alpha = \sum_{n=0}^{+\infty} \frac{\alpha(\alpha-1)\ldots(\alpha-n+1)}{n!} x^n$.

Contre-exemple 39. La fonction [BMP] p. 55

$$x \mapsto \begin{cases} e^{-\frac{1}{x^2}} \text{ si } x > 0 \\ 0 \text{ sinon} \end{cases}$$

est $\mathscr{C}^\infty$ mais n'est pas développable en série entière en 0.

III - Applications

1. Analyse complexe

Définition 40. Soient $U \subseteq \mathbb{C}$ un ouvert et $f : U \to \mathbb{C}$. On dit que f est **analytique sur** U si f est développable en série entière en tout point de U. p. 46

Théorème 41. Soient $\sum a_n z^n$ une série entière de rayon de convergence $R > 0$ et $z_0 \in D(0,R)$. On note $f : z \mapsto \sum_{n=0}^{+\infty} a_n z^n$.Alors f est holomorphe en z_0 et $f'(z_0) = \sum_{n=0}^{+\infty} n a_n z_0^{n-1}$.

Théorème 42 (Zéros isolés)**.** Soient $U \subseteq \mathbb{C}$ un ouvert connexe et $f : U \to \mathbb{C}$. Si f est une fonction analytique si f n'est pas identiquement nulle, alors l'ensemble des zéros de f n'admet pas de point d'accumulation dans U.

Corollaire 43. Soient $U \subseteq \mathbb{C}$ un ouvert connexe et $f : U \to \mathbb{C}$. Alors f admet un nombre fini de zéros dans tout compact de U.

Corollaire 44. Deux séries entières dont les sommes coïncident sur un voisinage de 0 dans $\mathbb{R}$ sont égales. [GOU20] p. 250

Théorème 45. Soit f une fonction holomorphe sur un disque ouvert de rayon ρ centré en un point a. Alors f est analytique sur ce disque.De plus, on a convergence normale sur tout compact du disque. [BMP] p. 63

2. Dénombrement

[DEV]

Application 46 (Nombres de Bell)**.** Pour tout $n \in \mathbb{N}^*$, on note B_n le nombre de partitions de $[\![1,n]\!]$. Par convention on pose $B_0 = 1$. Alors,

$$\forall k \in \mathbb{N}^*, B_k = \frac{1}{e}\sum_{n=0}^{+\infty}\frac{n^k}{n!}$$

[GOU20] p. 314

Application 47. Soit $n \in \mathbb{N}^*$. $\sigma \in S_n$ est un **dérangement de** S_n si $\forall k \in [\![1,n]\!], \sigma(k) \neq k$.Alors,

$$d_n = n!\sum_{k=0}^{n}\frac{(-1)^k}{k!}$$

[DAN] p. 336

3. Équations différentielles

Proposition 48. Pour résoudre une équation différentielle linéaire (L) à l'aide des séries entières :

(i) On suppose que $\varphi(x) = \sum_{n=0}^{+\infty} a_n x^n$ est solution de (L) et on l'introduit dans (L).

(ii) On se ramène à $\sum_{n=0}^{+\infty} b_n x^n = 0$ où les b_n dépendent des a_n.

(iii) On trouve une relation liant les a_n et on vérifie que la série $\sum_{n=0}^{+\infty} a_n x^n$ a un rayon de convergence non-nul.

[AMR11] p. 246

Exemple 49. Les solutions de $t^2(1-t)y'' - t(1+t)y' + y = 0$ sont les fonctions $t \mapsto \lambda\frac{x}{1-x}$ (où $\lambda \in \mathbb{R}$).

p. 273

Annexes

[GOU20]
p. 263

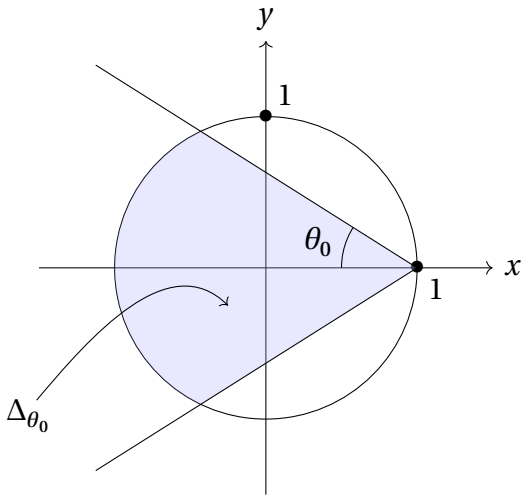


FIGURE I.28 – Illustration du théorème d'Abel angulaire.

244 Exemples d'études et d'applications de fonctions usuelles et spéciales.

I - La fonction exponentielle

1. Dans le champ complexe

Définition 1. On définit la fonction **exponentielle complexe** pour tout $z \in \mathbb{C}$ par

$$\sum_{n=0}^{+\infty} \frac{z^n}{n!}$$

on note cette somme e^z ou parfois $\exp(z)$.

[QUE] p. 4

Remarque 2. Cette somme est bien définie pour tout $z \in \mathbb{C}$ d'après le critère de d'Alembert.

Proposition 3. (i) $\forall z, z' \in \mathbb{C}$, $e^{z+z'} = e^z e^{z'}$.

(ii) exp est holomorphe sur $\mathbb{C}$, de dérivée elle-même.

(iii) exp ne s'annule jamais.

(iv) $|\exp(z)| = \exp(\mathrm{Re}(z))$ pour tout $z \in \mathbb{C}$.

Proposition 4. La fonction $\varphi : t \mapsto e^{it}$ est un morphisme surjectif de $\mathbb{R}$ sur $\mathbb{U}$.

Proposition 5. En reprenant les notations précédentes, $\mathrm{Ker}(\varphi)$ est un sous-groupe fermé de $\mathbb{R}$, de la forme $\mathrm{Ker}(\varphi) = a\mathbb{Z}$. On note $a = 2\pi$.

Application 6. Pour tout $n \in \mathbb{N}^*$, il y a n racines n-ièmes de l'unité, données par

$$e^{\frac{2ik\pi}{n}} = \cos\left(\frac{2ik\pi}{n}\right) + i\sin\left(\frac{2ik\pi}{n}\right)$$

où k parcourt les entiers de 0 à $n-1$.

[R-R] p. 259

Corollaire 7. Tout nombre complexe non nul α écrit $\alpha = re^{i\theta}$ admet exactement n racines n-ièmes données par

$$\sqrt[n]{r}e^{i\frac{\theta}{n}}e^{\frac{2ik\pi}{n}}$$

où k parcourt les entiers de 0 à $n-1$.

2. Dans le champ réel

Définition 8. On a plusieurs définitions (équivalentes) de la fonction exponentielle réelle. [D-L] p. 528

— **Vision "moderne" :** Soit $x \in \mathbb{R}$. $\exp(x) = \sum_{n=0}^{+\infty} \frac{x^k}{k!}$ (restriction de la série entière de la Théorème 1).

— **Vision "pédagogique" :** exp est l'unique solution au problème de Cauchy

$$\begin{cases} y' = y \\ y(0) = 1 \end{cases}$$

— **Vision "historique" :** Soit $x \in \mathbb{R}$. $\exp(x) = \lim_{n\to+\infty} \left(1 + \frac{x}{n}\right)^n$.

Théorème 9. [QUE] p. 6

(i) exp est une bijection croissante de $\mathbb{R}$ sur $\mathbb{R}_*^+$.

(ii) $\lim_{x\to-\infty} \exp(x) = 0$ et $\lim_{x\to+\infty} \exp(x) = +\infty$.

(iii) $x < 0 \iff \exp(x) < 1$.

3. Fonctions trigonométriques

Définition 10. On définit les fonctions sin et cos sur $\mathbb{R}$ par

$$\forall t \in \mathbb{R},\ \sin(t) = \mathrm{Im}(\exp(it)) \text{ et } \sin(t) = \mathrm{Re}(\exp(it))$$

Proposition 11. [DAN] p. 352

Soit $t \in \mathbb{R}$.

(i) $\sin(t) = \frac{e^{it} - e^{-it}}{2i} = \sum_{n=0}^{+\infty} \frac{t^{2n+1}}{(2n+1)!}$.

(ii) $\cos(t) = \frac{e^{it} + e^{-it}}{2} = \sum_{n=0}^{+\infty} \frac{t^{2n}}{(2n)!}$.

(iii) Ces fonctions sont réelles, 2π-périodiques et admettent un développement en série entière de rayon de convergence infini. Ceci permet de les prolonger de manière unique sur tout le plan complexe.

(iv) sin et cos sont dérivables avec $\cos' = -\sin$ et $\sin' = \cos$.

(v) cos est paire, sin est impaire.

Proposition 12. [ROM21] p. 36

L'application

$$\exp(i\theta) \mapsto \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix}$$

définit un isomorphisme de $\mathbb{U}$ dans $\mathrm{SO}_2(\mathbb{R})$.

4. Polynômes trigonométriques

Définition 13. — On appelle **polynôme trigonométrique** de degré inférieur à $N \in \mathbb{N}$ toute fonction de la forme $x \mapsto \sum_{n=-N}^{N} c_n e^{inx}$ avec $\forall n \in [\![-N, N]\!]$, $c_n \in \mathbb{C}$.

— On appelle **série trigonométrique** une série de fonctions de la variable réelle x et de la forme $c_n + \sum_{n\in\mathbb{N}^*}(c_n e^{inx} + c_{-n} e^{-inx})$, notée $\sum_{n\in\mathbb{Z}} c_n e^{inx}$.

[GOU20] p. 268

Exemple 14. — Pour tout $N \in \mathbb{N}$, la fonction $D_N = \sum_{n=-N}^{N} e_N$ est appelée **noyau de Dirichlet** d'ordre N.

— Pour tout $N \in \mathbb{N}$, la fonction $K_N = \frac{1}{N}\sum_{j=0}^{N-1} D_j$ est appelé **noyau de Fejér** d'ordre N.

[AMR08] p. 184

Théorème 15 (Fejér)**.** Soit $f : \mathbb{R} \to \mathbb{C}$ une fonction 2π-périodique.

(i) Si f est continue, alors $\|\sigma_N(f)\|_\infty \leq \|f\|_\infty$ et $(\sigma_N(f))$ converge uniformément vers f.

(ii) Si $f \in L_p^{2\pi}$ pour $p \in [1, +\infty[$, alors $\|\sigma_N(f)\|_p \leq \|f\|_p$ et $(\sigma_N(f))$ converge vers f pour $\|.\|_p$.

p. 190

Corollaire 16. L'espace des polynômes trigonométriques $\{\sum_{n=-N}^{N} c_n e_n \mid (c_n) \in \mathbb{C}^{\mathbb{N}}, N \in \mathbb{N}\}$ est dense dans l'espace des fonction continues 2π-périodiques pour $\|.\|_\infty$ et est dense dans $L_p^{2\pi}$ pour $\|.\|_p$ avec $p \in [1, +\infty[$.

Théorème 17 (Dirichlet)**.** Soient $f : \mathbb{R} \to \mathbb{C}$ 2π-périodique, continue par morceaux sur $\mathbb{R}$ et $t_0 \in \mathbb{R}$ tels que la fonction

$$h \mapsto \frac{f(t_0+h) + f(t_0-h) - f(t_0^+) - f(t_0^-)}{h}$$

est bornée au voisinage de 0. Alors,

$$S_N(f)(t_0) \longrightarrow_{N\to+\infty} \frac{f(t_0^+) + f(t_0^-)}{2}$$

[GOU20] p. 271

Contre-exemple 18. Soit $f : \mathbb{R} \to \mathbb{R}$ paire, 2π-périodique telle que :

$$\forall x \in [0, \pi], f(x) = \sum_{p=1}^{+\infty} \frac{1}{p^2} \sin\left((2^{p^3}+1)\frac{x}{2}\right)$$

Alors f est bien définie et continue sur $\mathbb{R}$. Cependant, sa série de Fourier diverge en 0.

Corollaire 19. Soient $f : \mathbb{R} \to \mathbb{C}$ 2π-périodique, $\mathscr{C}^1$ par morceaux sur $\mathbb{R}$. Alors,

$$\forall x \in \mathbb{R},\ S_N(f)(x) \longrightarrow_{N\to+\infty} \frac{f(x^+)+f(x^-)}{2}$$

En particulier, si f est continue en x, la série de Fourier de f converge vers $f(x)$.

Exemple 20. On considère $f : x \mapsto 1 - \frac{x^2}{\pi^2}$ sur $[-\pi,\pi]$. Alors,

$$\forall x \in [-\pi,\pi],\ f(x) = \frac{2}{3} - \frac{4}{\pi^2}\sum_{n=1}^{+\infty}(-1)^n\frac{\cos(nx)}{n^2}$$

Théorème 21 (Formule sommatoire de Poisson)**.** Soit $f : \mathbb{R} \to \mathbb{C}$ une fonction de classe $\mathscr{C}^1$ telle que $f(x) = O\left(\frac{1}{x^2}\right)$ et $f'(x) = O\left(\frac{1}{x^2}\right)$ quand $|x| \longrightarrow +\infty$. Alors :

p. 284

$$\forall x \in \mathbb{R},\ \sum_{n\in\mathbb{Z}} f(x+n) = \sum_{n\in\mathbb{Z}} \widehat{f}(2\pi n)e^{2i\pi nx}$$

Application 22 (Identité de Jacobi)**.**

$$\forall s > 0,\ \sum_{n=-\infty}^{+\infty} e^{-\pi n^2 s} = \frac{1}{\sqrt{s}}\sum_{n=-\infty}^{+\infty} e^{-\frac{\pi n^2}{s}}$$

II - Logarithmes

1. Logarithme dans le champ réel

Proposition 23. exp réalise une bijection strictement croissante de $\mathbb{R}$ sur $\mathbb{R}_*^+$.

[DAN] p. 346

Définition 24. La bijection réciproque de exp : $\mathbb{R} \to \mathbb{R}_*^+$ est appelée **logarithme népérien** et est notée ln.

Théorème 25. (i) $\forall x \in \mathbb{R}_*^+,\ \ln(x) = \int_1^x \frac{1}{x}\,\mathrm{d}x$.

(ii) $\forall x, y \in \mathbb{R}_*^+,\ \ln(xy) = \ln(x) + \ln(y)$.

Remarque 26. La fonction ln permet de définir la mise à la puissance par un réel :

$$\forall t \in \mathbb{R}_*^+,\ \forall \alpha \in \mathbb{R},\ t^\alpha = e^{\alpha\ln(t)}$$

2. Logarithmes dans le champ complexe

Théorème 27. Soient $\alpha \in \mathbb{R}$ et $\Omega_\alpha = \mathbb{C} \setminus \mathbb{R}^* e^{i\alpha}$. Alors, il existe une fonction L_α holomorphe sur Ω_α. Elle vérifie :

(i) $e^{L_\alpha(z)} = z$ pour tout $z \in \Omega_\alpha$.

(ii) $L_\alpha(z) = \ln(|z|) + i\theta_\alpha(z)$ avec $\theta_\alpha \in]\alpha, \alpha + 2\pi[$.

(iii) L_α est dérivable dans Ω_α avec $L'(z) = \frac{1}{z}$ pour tout $z \in \Omega_\alpha$.

[QUE] p. 81

Définition 28. La fonction L_α précédente est appelée **détermination d'ordre** α (ou **détermination principale** si $\alpha = -\pi$) du logarithme.

Théorème 29. On pose $D = D(0,1)$ et on définit $\ell : D \to \mathbb{C}$ par $\ell : z \mapsto \sum_{n=1}^{+\infty} (-1)^{n+1} \frac{z^n}{n}$. Alors :

(i) $1 + z = \exp(\ell(z))$ pour tout $z \in D$.

(ii) $\ell(z) = L_{-\pi}(1+z)$ pour tout $z \in D$.

III - La fonction Γ d'Euler

1. Définition

Définition 30. On pose

$$\forall x > 0, \Gamma(x) = \int_0^{+\infty} e^{-t} t^{x-1} \, \mathrm{d}t$$

[GOU20] p. 162

Proposition 31. (i) Γ est $\mathscr{C}^\infty$ sur $]0, +\infty[$ et pour tout $n \in \mathbb{N}^*$, on a

$$\forall x \in \mathbb{R}_*^+, \Gamma^{(n)}(x) = \int_0^{+\infty} (\ln(t))^n e^{-t} t^{x-1} \, \mathrm{d}t$$

(ii) $\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$.

(iii) $\forall x > 0, \Gamma(x+1) = x\Gamma(x)$ et en particulier, $\forall n \in \mathbb{N}, \Gamma(n) = n!$.

Lemme 32. La fonction Γ définie pour tout $x > 0$ par $\Gamma(x) = \int_0^{+\infty} t^{x-1} e^{-t} \, \mathrm{d}t$ vérifie :

(i) $\forall x \in \mathbb{R}_*^+, \Gamma(x+1) = x\Gamma(x)$.

(ii) $\Gamma(1) = 1$.

(iii) Γ est log-convexe sur $\mathbb{R}_*^+$.

[ROM19-1] p. 364

[DEV]

Théorème 33 (Bohr-Mollerup)**.** Soit $f : \mathbb{R}_*^+ \to \mathbb{R}^+$ vérifiant le Point (i), Point (ii) et Point (iii) du Théorème 32. Alors $f = \Gamma$.

Remarque 34. À la fin de la preuve, on obtient une formule due à Gauss :

$$\forall x \in]0,1], \Gamma(x) = \lim_{n\to+\infty} \frac{n^x n!}{(x+n)\dots(x+1)x}$$

que l'on peut aisément étendre à $\mathbb{R}_*^+$ entier.

Lemme 35. Soient X et Y deux variables aléatoires indépendantes telles que $X \sim \Gamma(a,\gamma)$ et $Y \sim \Gamma(b,\gamma)$. Alors $Z = X + Y \sim \Gamma(a+b,\gamma)$. [G-K] p. 180

[DEV] **Application 36** (Formule de Stirling)**.** p. 556

$$n! \sim \sqrt{2n\pi}\left(\frac{n}{e}\right)^n$$

2. Prolongement complexe

On suppose ici que E est un ouvert Ω de $\mathbb{C}$.

[Z-Q] p. 314

Théorème 37 (Holomorphie sous le signe intégral)**.** On suppose :

(i) $\forall z \in \Omega$, $x \mapsto f(z,x) \in L_1(X)$.

(ii) pp. en $x \in X$, $z \mapsto f(z,x)$ est holomorphe dans Ω. On notera $\frac{\partial f}{\partial z}$ cette dérivée définie presque partout.

(iii) $\forall K \subseteq \Omega$ compact, $\exists g_K \in L_1(X)$ positive telle que

$$|f(x,z)| \leq g_K(x) \quad \forall z \in K, \text{pp. en } x$$

Alors F est holomorphe dans Ω avec

$$\forall z \in \Omega, F'(z) = \int_X \frac{\partial f}{\partial z}(z,t)\,\mathrm{d}\mu(z)$$

Exemple 38. La fonction Γ est holomorphe dans l'ouvert $\{z \in \mathbb{C} \mid \mathrm{Re}(z) > 0\}$. p. 318

Théorème 39. On peut prolonger Γ en une fonction holomorphe non nulle sur $\mathbb{C} \setminus -\mathbb{N}$.

[QUE] p. 255

Théorème 40 (Formule des compléments)**.**

$$\forall \mathbb{C} \setminus \mathbb{Z},\ \Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin(\pi z)}$$

IV - La fonction ζ de Riemann

1. Définition

Définition 41. Pour tout $s > 1$, on pose

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s}$$

[GOU20] p. 302

Proposition 42. ζ définit une fonction de classe $\mathscr{C}^\infty$ sur $]1,+\infty[$ et,

$$\forall p \in \mathbb{N}^*,\ \forall s \in]1,+\infty[,\ \zeta^{(p)}(s) = \sum_{n=1}^{+\infty} \frac{\ln(n)^p}{n^s}$$

Proposition 43.

$$\lim_{s\to+\infty} \zeta(s) = 1 \text{ et } \zeta(s) \sim_{1^+} \frac{1}{s-1} + \gamma + o(1)$$

où γ désigne la constante d'Euler.

Proposition 44.

$$\forall s > 1,\ \zeta(s)\Gamma(s) = \int_0^{+\infty} t^{s-1} \frac{e^{-t}}{1-e^{-t}}\,\mathrm{d}t$$

[G-K] p. 108

2. Prolongement complexe

Proposition 45. On prolonge la définition de ζ donnée à la Théorème 41 en posant

$$\zeta : \begin{array}{ccc} \{s \in \mathbb{C} \mid \mathrm{Re}(s) > 0\} & \longmapsto & \mathbb{C} \\ s & \longmapsto & \sum_{n=1}^{+\infty} \frac{1}{n^s} \end{array}$$

[Z-Q] p. 20

Proposition 46. ζ est holomorphe sur $\{s \in \mathbb{C} \mid \mathrm{Re}(s) > 1\}$.

Théorème 47. Il existe une fonction $\widetilde{\zeta}$, holomorphe dans $\mathbb{C} \setminus \{1\}$ telle que :

p. 28

(i) Pour tout $s \in \mathbb{C} \setminus \{1\}$, $\widetilde{\zeta}(s) = \frac{1}{s-1} + \eta(s)$ avec η holomorphe dans $\mathbb{C}$.

(ii) Pour tout $s \in \mathbb{C}$ tel que $\mathrm{Re}(s) > 1$, $\widetilde{\zeta}(s) = \zeta(s)$.

(iii) En posant $I(s) = \pi^{\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s)$, on a $I(s) = I(1-s)$.

245 Fonctions holomorphes et méromorphes sur un ouvert de $\mathbb{C}$. Exemples et applications.

Soit $\Omega \subseteq \mathbb{C}$ un ouvert. Soit $f : \Omega \to \mathbb{C}$.

I - Dérivabilité au sens complexe

Définition 1. On dit que f est **holomorphe** en $a \in \Omega$ s'il existe un complexe $f'(a)$ tel que

$$f'(a) = \lim_{\substack{h \to 0 \\ h \neq 0}} \frac{f(a+h) - f(a)}{h}$$

On dit que f est holomorphe sur Ω si elle l'est en tout point de Ω et on note f' la fonction $f' : z \mapsto f'(z)$ ainsi que $\mathscr{H}(\Omega)$ l'ensemble des fonctions holomorphes sur Ω.

[QUE] p. 76

Exemple 2.
— $z \mapsto z^2$ est holomorphe sur $\mathbb{C}$, de dérivée $z \mapsto 2z$.
— $z \mapsto \overline{z}$ n'est holomorphe en aucun point de $\mathbb{C}$.

Proposition 3. (i) $\mathscr{H}(\Omega)$ est une algèbre sur $\mathbb{C}$ avec pour tout $g, h \in \mathscr{H}(\Omega)$ et $\lambda \in \mathbb{C}$:
— $(g+h)' = g' + h'$.
— $(\lambda g)' = \lambda g'$.
— $(gh)' = g'h + gh'$.
— $\left(\frac{g}{h}\right)' = \frac{g'h - gh'}{g^2}$ quand g ne s'annule pas sur Ω.

(ii) Pour tout $g \in \mathscr{H}(\Omega)$, $h \in \mathscr{H}(\Omega_1)$ où $g(\Omega) \subseteq \Omega_1$

$$h \circ g \in \mathscr{H}(\Omega) \text{ et } (h \circ g)' = (h' \circ g) g'$$

(iii) Soit $g \in \mathscr{H}(\Omega)$ holomorphe bijective d'inverse h. On suppose h continue en $b = g(a)$ et $g'(a) \neq 0$. Alors h est holomorphe en b et

$$h'(b) = \frac{1}{g'(a)}$$

Théorème 4 (Conditions de Cauchy-Riemann)**.** On pose $u = \mathrm{Re}(f)$ et $v = \mathrm{Im}(f)$. On suppose f $\mathbb{R}$-différentiable en $a \in \Omega$. Alors, les propositions suivantes sont équivalentes :

(i) f est holomorphe en a.
(ii) $\mathrm{d}f_a$ est $\mathbb{C}$-linéaire.
(iii) $\frac{\partial f}{\partial y}(a) = i\frac{\partial f}{\partial x}(a)$.

[BMP] p. 57

(iv) $\frac{\partial u}{\partial x}(a) = \frac{\partial v}{\partial y}(a)$ et $\frac{\partial u}{\partial y}(a) = -\frac{\partial v}{\partial x}(a)$.

Exemple 5. $z \mapsto \mathrm{Re}(z)$ et $z \mapsto \mathrm{Im}(z)$ ne sont holomorphes en aucun point de $\mathbb{C}$. [QUE] p. 115

Théorème 6 (Weierstrass)**.** Une suite de fonctions holomorphes qui converge uniformément sur tout compact de Ω a une limite holomorphe sur Ω. De plus, la suite des dérivées k-ième converge uniformément sur tout compact vers la dérivée k-ième de la limite pour tout $k \in \mathbb{N}$. [BMP] p. 69

II - Séries entières et analycité

1. Généralités sur les séries entières

Définition 7. On appelle **série entière** toute série de fonctions de la forme $\sum a_n z^n$ où z est une variable complexe et où (a_n) est une suite complexe. [GOU20] p. 247

Lemme 8 (Abel)**.** Soient $\sum a_n z^n$ une série entière et $z_0 \in \mathbb{C}$ tels que $(a_n z_0^n)$ soit bornée. Alors :

(i) $\forall z \in \mathbb{C}$ tel que $|z| < |z_0|$, $\sum a_n z^n$ converge absolument.

(ii) $\forall r \in]0, |z_0|[$, $\sum a_n z^n$ converge normalement dans $\overline{D}(0,r) = \{z \in \mathbb{C} \mid |z| \leq r\}$.

Définition 9. En reprenant les notations précédentes, le nombre

$$R = \sup\{r \geq 0 \mid (|a_n| r^n) \text{ est bornée}\}$$

est le **rayon de convergence** de $\sum a_n z^n$.

Exemple 10.
— $\sum n^2 z^n$ a un rayon de convergence égal à 1.
— $\sum \frac{z^n}{n!}$ a un rayon de convergence infini. On note $z \mapsto e^z$ la fonction somme. p. 255

Proposition 11. Soit $\sum a_n z^n$ une série entière de rayon de convergence $r \neq 0$. Alors $S \in \mathscr{H}(D(0,r))$ et, [QUE] p. 57

$$S'(z) = \sum_{n=0}^{+\infty} n a_n z^{n-1}$$

pour tout $z \in D(0,r)$.

Plus précisément, pour tout $k \in \mathbb{N}$, S est k fois dérivable avec

$$S^{(k)}(z) = \sum_{n=k}^{+\infty} n(n-1)\dots(n-k+1)a_n z^{n-k}$$

2. Analycité

Définition 12. On dit que f est **analytique** sur Ω si, pour tout $a \in \Omega$, il existe $r > 0$ et une série entière $\sum a_n z^n$ de rayon de convergence $\geq r$, tels que

$$D(a,r) \subseteq \Omega \text{ et } \forall z \in D(a,r),\ f(z) = \sum_{n=0}^{+\infty} a_n z^n$$

ie. f est développable en série entière en tout point de Ω. On note $\mathscr{A}(\Omega)$ l'ensemble des fonctions analytiques sur Ω.

p. 57

Proposition 13. Soit $\sum a_n z^n$ une série entière de rayon de convergence $r \neq 0$. Alors $S \in \mathscr{A}(D(0,r))$ et, si $|z-a| \leq r - |a|$:

$$f(z) = \sum_{k=0}^{+\infty} \frac{S^{(k)}(a)}{k!}(z-a)^k$$

(où $S^{(k)}$ désigne la k-ième dérivée complexe de S).

Proposition 14. $\mathscr{A}(\Omega) \subseteq \mathscr{H}(\Omega)$.

p. 85

Proposition 15. Si $f = P/Q$ est une fraction rationnelle, alors f est développable en série entière au voisinage de chaque point qui n'est pas un pôle de f (cf. Théorème 40).

p. 78

Théorème 16 (Zéros isolés)**.** On suppose Ω connexe et $f \in \mathscr{A}(\Omega)$. Si f n'est pas identiquement nulle sur Ω, alors l'ensemble des zéros de f n'admet pas de point d'accumulation dans Ω.

[BMP] p. 53

Corollaire 17. $\mathscr{A}(\Omega)$ est une algèbre intègre.

p. 73

Remarque 18 (Prolongement analytique). Reformulé de manière équivalente au Théorème 16, si deux fonctions analytiques coïncident sur un sous-ensemble de Ω qui possède un point d'accumulation dans Ω, alors elles sont égales sur Ω.

p. 53

p. 77

Exemple 19. Il existe une unique fonction g holomorphe sur $\mathbb{C}$ telle que

$$\forall n \in \mathbb{N}^*, g\left(\frac{1}{n}\right) = \frac{1}{n}$$

et c'est la fonction identité.

Contre-exemple 20. Il existe au moins deux fonctions g holomorphes sur $\Omega = \{z \in \mathbb{C} \mid \mathrm{Re}(z) > 0\}$ telles que

$$\forall n \in \mathbb{N}^*, g\left(\frac{1}{n}\right) = 0$$

III - Holomorphie et intégration

1. Intégration sur une courbe

[QUE] p. 85

Définition 21. — Un **chemin** est une application $\gamma : [a,b] \to \mathbb{C}$ (où $[a,b]$ est un segment de $\mathbb{R}$) continue.

— Si $\gamma(a) = \gamma(b)$, on dit que γ est **fermé**.

— Si γ est un chemin $\mathscr{C}^1$ par morceaux, on dit que γ est une **courbe**.

— On appelle $\gamma^* = \gamma([a,b])$ l'**image** de γ.

Exemple 22. Soient $\omega \in \mathbb{C}$ et $r \in \mathbb{R}_*^+$. Alors,

$$\gamma : \begin{array}{ccc} [0,2\pi] & \to & \mathbb{C} \\ t & \mapsto & \omega + re^{it} \end{array}$$

est une courbe fermée (c'est la paramétrisation du cercle de centre ω et de rayon r).

Définition 23. Soit $\gamma : [a,b] \to \Omega$ une courbe. L'**intégrale curviligne** le long de γ est

$$\int_\gamma f(z)\,\mathrm{d}z = \int_b^a f(\gamma(t))\gamma'(t)\,\mathrm{d}t$$

Proposition 24. Soit $\gamma : [a,b] \to \Omega$ une courbe de longueur $L(\gamma) = \int_a^b |\gamma'(t)|\,\mathrm{d}t$, alors,

$$\left|\int_\gamma f(z)\,\mathrm{d}z\right| \leq \sup_{z\in\gamma^*} |f(z)| \times L(\gamma)$$

Proposition 25. Soit $\gamma : [a,b] \to \Omega$ une courbe. On suppose $\gamma^* \subseteq \Omega$, f holomorphe sur Ω telle que f' est continue sur γ^*. Alors,

$$\int_\gamma f'(z)\,\mathrm{d}z = f(\gamma(b)) - f(\gamma(a))$$

2. Théorie de Cauchy et lien avec l'analycité

Définition 26. Soit $\gamma : [a,b] \to \Omega$ une courbe telle que $\omega \notin \gamma^*$. **L'indice** de ω par rapport à γ, noté $I(\omega,\gamma)$, est défini par

$$I(\omega,\gamma) = \frac{1}{2i\pi}\int_\gamma \frac{1}{z-a}\,\mathrm{d}z = \frac{1}{2i\pi}\int_b^a \frac{1}{\gamma(t)-a}\gamma'(t)\,\mathrm{d}t$$

Remarque 27. En reprenant les notations précédentes, $I(\omega,\gamma)$ compte le nombre de tours orientés que γ fait autour de ω. En particulier :

(i) On a toujours $I(\omega,\gamma) \in \mathbb{Z}$.

(ii) On note $\gamma^* = \gamma([a,b])$ l'image de γ. $I(\omega,\gamma)$ est nulle sur la composante connexe non bornée de $\mathbb{C} \setminus \gamma^*$.

Théorème 28 (Cauchy homologique)**.** Soit Γ un cycle homologue à zéro dans Ω (ie. tel que $z \notin \Omega \implies I(a,\Gamma) = 0$). On suppose $f \in \mathscr{H}(\Omega)$. Alors, p. 134

$$\int_\Gamma f(z)\,\mathrm{d}z = 0$$

Corollaire 29 (Formule intégrale de Cauchy)**.** Soit Γ un cycle homologue à zéro dans Ω. On suppose $f \in \mathscr{H}(\Omega)$. Alors,

$$z_0 \in \Omega \setminus \Gamma^* \implies \frac{1}{2i\pi}\int_\Gamma \frac{f(z)}{z-z_0}\,\mathrm{d}z = I(z_0,\gamma) f(z_0)$$

Corollaire 30. On a $\mathscr{H}(\Omega) \subseteq \mathscr{A}(\Omega)$. De plus, si $a \in \Omega$ et que l'on pose $d = d(a, \mathbb{C}\setminus\Omega)$, on a p. 85

$$f(a+h) = \sum_{n=0}^{+\infty} a_n h^n \text{ pour } |h| < d \text{ avec } a_n = \frac{f^{(n)}(a)}{n!} = \frac{1}{2i\pi}\int_{C^+(a,d)} \frac{f(z)}{(z-a)^{n+1}}\,\mathrm{d}z$$

[BMP] p. 64

3. Conséquences

Proposition 31 (Inégalités de Cauchy)**.** On suppose f holomorphe au voisinage du disque $\overline{D}(a,R)$. On note c_n les coefficients du développement en série entière de f en a. Alors,

$$\forall n \in \mathbb{N},\ \forall r \in [0,R],\ |c_n| \leq \frac{M(r)}{r^n}$$

où $M(r) = \sup_{|z-a|=r} |f(z)|$.

[QUE] p. 102

Corollaire 32 (Théorème de Liouville)**.** On suppose f holomorphe sur $\mathbb{C}$ tout entier. Si f est bornée, alors f est constante.

Théorème 33 (Principe du maximum)**.** On suppose Ω borné et f holomorphe dans Ω et continue dans $\overline{\Omega}$. On note M le sup de f sur la frontière (compacte) de Ω. Alors,

$$\forall z \in \Omega,\ |f(z)| \leq M$$

p. 107

4. Holomorphie d'une intégrale à paramètre

Théorème 34 (Holomorphie sous le signe intégral)**.** On suppose :

(i) $\forall z \in \Omega,\ x \mapsto f(z,x) \in L_1(X)$.

(ii) pp. en $x \in X$, $z \mapsto f(z,x)$ est holomorphe dans Ω. On notera $\frac{\partial f}{\partial z}$ cette dérivée définie presque partout.

(iii) $\forall K \subseteq \Omega$ compact, $\exists g_K \in L_1(X)$ positive telle que

$$|f(x,z)| \leq g_K(x) \quad \forall z \in K, \text{pp. en } x$$

Alors F est holomorphe dans Ω avec

$$\forall z \in \Omega,\ F'(z) = \int_X \frac{\partial f}{\partial z}(z,t)\,\mathrm{d}\mu(z)$$

p. 101

Application 35. Soit $f \in L_1(\mathbb{R})$ ainsi que sa transformée de Fourier $\widehat{f} : x \mapsto \int_{\mathbb{R}} f(t)e^{-ixt}\,\mathrm{d}t$. Alors $f = 0$.

p. 115

Application 36. $F : z \mapsto \int_{\mathbb{R}} e^{zx}e^{-x^2}\,\mathrm{d}x$ définit une fonction holomorphe sur $\mathbb{C}$ qui coïncide

[BMP] p. 83

avec la transformée de Fourier de $f : x \mapsto e^{-x^2}$ sur $\mathbb{R}$. On trouve en particulier,

$$\forall t \in \mathbb{R}, \widehat{f}(t) = F(it) = \sqrt{\pi} e^{-\frac{t^2}{4}}$$

Notation 37. Soient I un intervalle de $\mathbb{R}$ et $\rho : I \to \mathbb{R}$ une fonction poids. On note : p. 110

- $\forall n \in \mathbb{N}$, $g_n : x \mapsto x^n$.
- $L_2(I, \rho)$ l'espace des fonctions de carré intégrable pour la mesure de densité ρ par rapport à la mesure de Lebesgue.

Lemme 38. On suppose que $\forall n \in \mathbb{N}$, $g_n \in L_1(I, \rho)$ et on considère (P_n) la famille des polynômes orthogonaux associée à ρ sur I. Alors $\forall n \in \mathbb{N}$, $g_n \in L_2(I, \rho)$. En particulier, l'algorithme de Gram-Schmidt a bien du sens et (P_n) est bien définie. p. 140

[DEV]

Application 39. Soient I un intervalle de $\mathbb{R}$ et ρ une fonction poids. On considère (P_n) la famille des polynômes orthogonaux associée à ρ sur I.

On suppose qu'il existe $a > 0$ tel que

$$\int_I e^{a|x|} \rho(x) \, \mathrm{d}x < +\infty$$

alors (P_n) est une base hilbertienne de $L_2(I, \rho)$ pour la norme $\|.\|_2$.

IV - Méromorphie

1. Singularités

Définition 40. Soit $a \in \Omega$. On suppose $f \in \mathscr{H}(\Omega \setminus \{a\})$. [QUE] p. 165

- On dit que a est une **singularité effaçable** pour f s'il existe $g \in \mathscr{H}(\Omega)$ tel que $f(z) = g(z)$ pour tout $z \in \Omega \setminus \{a\}$.
- On dit que a est un **pôle** d'ordre m s'il existe des scalaires $c_{-1}, \dots, c_{-m}$ avec $c_{-m} \neq 0$ tels que $z \mapsto f(z) - \sum_{k=1}^{m} \frac{c_{-k}}{(z-a)^k}$ ait une singularité effaçable en a.
- $\sum_{k=1}^{m} \frac{c_{-k}}{(z-a)^k}$ est la **partie principale** de f en a et c_{-1} est le **résidu** de f en a noté $\mathrm{Res}(f, a)$.

Exemple 41.
- $z \mapsto \frac{\sin(z)}{z}$ a une singularité effaçable en 0.
- $z \mapsto \frac{e^z}{z}$ a un pôle d'ordre 1 (simple) en 0 avec partie principale égale à $\frac{1}{z}$ et $\mathrm{Res}(f, 0) = 1$.

Définition 42. On dit que f est **méromorphe** sur Ω s'il existe $A \subseteq \Omega$ tel que :

— A n'a que des points isolés dans Ω (en particulier, A est au plus dénombrable et $\Omega \setminus A$ est ouvert).

— $f \in \mathscr{H}(\Omega \setminus A)$.

— f a un pôle en chaque point de a.

Exemple 43. $z \mapsto \frac{1}{\sin(z)}$ est méromorphe dans $\mathbb{C}$ et en reprenant les notations précédentes, $A = \{k\pi \mid k \in \mathbb{Z}\}$.

Exemple 44. La fonction Γ définie par [BMP] p. 82

$$\Gamma : \begin{array}{ccc} \{z \in \mathbb{C} \mid \mathrm{Re}(z) > 0\} & \to & \mathbb{C} \\ z & \mapsto & \int_0^{+\infty} e^{-t} t^{z-1} \, \mathrm{d}t \end{array}$$

se prolonge en une fonction méromorphe sur $\mathbb{C} \setminus \mathbb{N}$.

Proposition 45. On suppose $f = \frac{g}{h}$ où g et h sont holomorphes en un voisinage de $a \in \Omega$ avec a un zéro simple de h et $g(a) \neq 0$. Alors, a est un pôle simple de f de résidu [QUE] p. 168

$$\mathrm{Res}(f, a) = \frac{g(a)}{h'(a)}$$

Exemple 46. Le résidu de $z \mapsto \frac{z^2}{(z+1)(z-1)^2}$ en 1 est égal à $\frac{3}{4}$.

2. Théorème des résidus

Théorème 47 (des résidus)**.** On suppose f méromorphe sur Ω et on note A l'ensemble de ses pôles. Soit γ une courbe homologue à zéro dans Ω et ne rencontrant pas A. Alors,

$$\int_\gamma f(z) \, \mathrm{d}z = 2i\pi \sum_{a \in A} I(a, \gamma) \, \mathrm{Res}(f, a)$$

Exemple 48. p. 173

$$\int_0^{2\pi} \frac{1}{3 + 2\cos(t)} \, \mathrm{d}t = \frac{2\pi}{\sqrt{5}}$$

Exemple 49 (Intégrale de Dirichlet)**.**

$$\int_0^{+\infty} \frac{\sin(x)}{x}\,\mathrm{d}x = \frac{\pi}{2}$$

[DEV]

Exemple 50 (Transformée de Fourier d'une gaussienne)**.** On définit $\forall a \in \mathbb{R}_*^+$,

$$\gamma_a : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & e^{-ax^2} \end{array}$$

Alors,

$$\forall \xi \in \mathbb{R},\ \widehat{\gamma_a}(\xi) = \sqrt{\frac{\pi}{a}} e^{\frac{-\xi^2}{4a}}$$

[AMR08] p. 156

Application 51 (Théorème de Kronecker)**.** On suppose f holomorphe sur Ω et non identiquement nulle dans Ω. Soit γ une courbe homologue à zéro dans Ω et qui ne rencontre pas l'ensemble des zéros de f. Alors, le nombre $Z = Z(f)$ des zéros de f à l'intérieur de γ comptés avec multiplicités vérifie

$$Z = \frac{1}{2i\pi} \int_\gamma \frac{f'(z)}{f(z)}\,\mathrm{d}z$$

[QUE] p. 171

Application 52 (Théorème de Rouché)**.** Soient γ un cycle homologue à zéro dans Ω et $g, h \in \mathscr{H}(\Omega)$. On suppose

$$z \in \gamma^* \implies |g(z)| \leq |f(z)|$$

Alors,

$$Z(g) = Z(g+h)$$

Exemple 53. $z \mapsto z^8 - 5z^3 + z - 2$ a trois zéros dans $D(0,1)$.

[BMP] p. 67

246 Séries de Fourier. Exemples et applications.

I - Coefficients de Fourier

1. Définitions

Notation 1. — Pour tout $p \in [1,+\infty]$, on note $L_p^{2\pi}$ l'espace des fonctions $f : \mathbb{R} \to \mathbb{C}$, 2π-périodiques et mesurables, telles que $\|f\|_p < +\infty$.

— Pour tout $n \in \mathbb{Z}$, on note e_n la fonction 2π-périodique définie pour tout $t \in \mathbb{R}$ par $e_n(t) = e^{int}$.

[Z-Q] p. 73

Remarque 2.

$$1 \leq p < q \leq +\infty \implies L_q^{2\pi} \subseteq L_p^{2\pi} \text{ et } \|.\|_p \leq \|.\|_q$$

Proposition 3. $L_2^{2\pi}$ est un espace de Hilbert pour le produit scalaire

$$\langle .,. \rangle : (f,g) \mapsto \frac{1}{2\pi} \int_0^{2\pi} f(t)\overline{g(t)}\,\mathrm{d}t$$

Définition 4. Soit $f \in L_1^{2\pi}$. On appelle :

— **Coefficients de Fourier complexes**, les complexes définis par

$$\forall n \in \mathbb{Z},\ c_n(f) = \frac{1}{2\pi} \int_0^{2\pi} f(t)e^{-int}\,\mathrm{d}t = \langle f, e_n \rangle$$

— **Coefficients de Fourier réels**, les complexes définis par

$$\forall n \in \mathbb{N},\ a_n(f) = \frac{1}{\pi} \int_0^{2\pi} f(t)\cos(nt)\,\mathrm{d}t \text{ et } \forall n \in \mathbb{N}^*,\ b_n(f) = \frac{1}{\pi} \int_0^{2\pi} f(t)\sin(nt)\,\mathrm{d}t$$

[GOU20] p. 268

Remarque 5. Soit $f \in L_1^{2\pi}$.

— On utilise en général les coefficients réels lorsque f est à valeurs réelles.

— Si f est paire (resp. impaire), les coefficients $b_n(f)$ (resp. $a_n(f)$) sont nuls.

— $\forall n \in \mathbb{N}, a_n(f) = c_n(f) + c_{-n}(f)$ et $\forall n \in \mathbb{N}^*, b_n(f) = i(c_n(f) + c_{-n}(f))$.

— On pourrait plus généralement définir les coefficients de Fourier d'une fonction T-périodique pour toute période $T > 0$.

p. 273

Exemple 6. On définit $\forall \alpha \in \mathbb{R} \setminus \mathbb{Z}$, $f_\alpha : t \mapsto \cos(\alpha t)$. Alors,

$$\forall n \in \mathbb{N},\ a_n(f_\alpha) = (-1)^n \frac{2\alpha \sin(\alpha\pi)}{\pi(\alpha^2 - n^2)} \text{ et } \forall n \in \mathbb{N}^*,\ b_n(f_\alpha) = 0$$

2. Propriétés structurelles des espaces $L_p^{2\pi}$

a. L'algèbre $L_1^{2\pi}$

Proposition 7. Tout comme sur $L_1(\mathbb{R})$, on a un opérateur de convolution sur $L_1^{2\pi}$: **[BMP]** p. 125

$$\forall f, g \in L_1^{2\pi},\ \forall x \in \mathbb{R},\ f * g(x) = \frac{1}{2\pi} \int_0^{2\pi} f(y) g(x-y)\,\mathrm{d}y$$

qui munit $L_1^{2\pi}$ d'une structure d'algèbre normée.

Proposition 8. Soient $f \in L_1^{2\pi}$, $a \in \mathbb{R}$ et $k, n \in \mathbb{Z}$. **[AMR08]** p. 174

(i) $f * e_n = c_n(f) e_n$.
(ii) $|c_n(f)| \leq \|f\|_1$.
(iii) $c_{-n}(f) = c_n(x \mapsto f(-x))$.
(iv) $c_n(\overline{f}) = \overline{c_{-n}(f)}$.
(v) $c_n(x \mapsto f(x-a)) = e_n(a) c_n(f)$.
(vi) $c_n(e_k f) = c_{n-k}(f) e_n$.
(vii) $c_n(f') = in c_n(f)$ si f est continue et $\mathscr{C}^1$ par morceaux.

Lemme 9 (Riemann-Lebesgue)**.** Soit $f \in L_1^{2\pi}$. Alors $(c_n(f))$ tend vers 0 lorsque n tend vers $\pm\infty$. **[BMP]** p. 126

Théorème 10. Soit c_0 l'espace des suites de complexes qui convergent vers 0 en $-\infty$ et $+\infty$. L'application

$$\mathscr{F} : \begin{array}{ccc} L_1^{2\pi} & \to & c_0 \\ f & \mapsto & (c_n(f))_{n\in\mathbb{Z}} \end{array}$$

est un morphisme d'algèbres de $(L_1^{2\pi}, +, *, \|.\|_1)$ dans $(c_0, +, \cdot, \|.\|_\infty)$ continu, de norme 1.

b. Propriétés hilbertiennes de $L_2^{2\pi}$

Théorème 11. Soit H un espace de Hilbert et $(\epsilon_n)_{n\in I}$ une famille orthonormée dénombrable de H. Les propriétés suivantes sont équivalentes : p. 109

(i) La famille orthonormée $(\epsilon_n)_{n\in I}$ est une base hilbertienne de H.

(ii) $\forall x \in H,\ x = \sum_{n=0}^{+\infty} \langle x, \epsilon_n\rangle \epsilon_n$.

(iii) $\forall x \in H,\ \|x\|_2 = \sum_{n=0}^{+\infty} |\langle x, \epsilon_n\rangle|^2$.

Remarque 12. L'égalité du Théorème 11 Point (iii) est appelée **égalité de Parseval**.

Théorème 13. La famille $(e_n)_{n\in\mathbb{Z}}$ est une base hilbertienne de $L_2^{2\pi}$. p. 123

Corollaire 14.

$$\forall f \in L_2^{2\pi},\ f = \sum_{n=-\infty}^{+\infty} c_n(f) e_n$$

Exemple 15. On considère $f : x \mapsto 1 - \frac{x^2}{\pi^2}$ sur $[-\pi, \pi]$. Alors, [GOU20] p. 272

$$\frac{\pi^4}{90} = \|f\|_2 = \sum_{n=0}^{+\infty} \frac{1}{n^4}$$

Remarque 16. L'égalité du Théorème 14 est valable dans $L_2^{2\pi}$, elle signifie donc que [BMP] p. 124

$$\left\| \sum_{n=-N}^{N} c_n(f) e_n - f \right\|_2 \longrightarrow_{N\to+\infty} 0$$

3. Séries de Fourier

Définition 17. Soit $f \in L_1^{2\pi}$. On appelle **série de Fourier** associée à f la série $(S_N(f))$ définie par [GOU20] p. 269

$$\forall N \in \mathbb{N},\ S_N(f) = \sum_{n=-N}^{N} c_n(f) e_n \overset{(*)}{=} \frac{a_0(f)}{2} + \sum_{n=1}^{N} (a_n(f)\cos(nx) + b_n(f)\sin(nx))$$

Remarque 18. L'égalité $(*)$ de la définition précédente est justifiée car,

$$\forall n \in \mathbb{N}^*,\ \forall x \in \mathbb{R},\ c_n(f) e^{inx} + c_{-n}(f) e^{-inx} = a_n(f)\cos(nx) + b_n(f)\sin(nx)$$

II - Divers modes de convergence

Nous avons vu que pour $f \in L^{2\pi}_2$, il y a convergence dans $L^{2\pi}_2$ de $(S_N(f))$ vers f. Cette section est dédiée à l'étude d'autres modes de convergence. En particulier, nous allons nous poser plusieurs questions : [AMR08] p. 178

— Pour quelles fonctions f y a-t-il convergence de $(S_N(f))$?

— Y a-t-il convergence vers f ?

— De quel type de convergence s'agit-il ?

1. Convergence au sens de Cesàro

p. 184

Définition 19. Pour tout $N \in \mathbb{N}$, la fonction $D_N = \sum_{n=-N}^{N} e_N$ est appelé **noyau de Dirichlet** d'ordre N.

Proposition 20. Soit $N \in \mathbb{N}$.

(i) D_N est une fonction paire, 2π-périodique, et de norme 1.

(ii)
$$\forall x \in \mathbb{R} \setminus 2\pi\mathbb{Z},\ D_N(x) = \frac{\sin\left(\left(N+\frac{1}{2}\right)x\right)}{\sin\left(\frac{x}{2}\right)}$$

(iii) Pour tout $f \in L^{2\pi}_1$, $S_N(f) = f * D_N$.

Définition 21. Pour tout $N \in \mathbb{N}$, la fonction $K_N = \frac{1}{N}\sum_{j=0}^{N-1} D_j$ est appelé **noyau de Fejér** d'ordre N.

Notation 22. Pour tout $N \in \mathbb{N}^*$, on note $\sigma_N = \frac{1}{N}\sum_{k=0}^{N-1} S_n(f)$ la somme de Cesàro d'ordre N de la série de Fourier d'une fonction $f \in L^{2\pi}_1$.

Proposition 23. Soient $N \in \mathbb{N}^*$ et $f \in L^{2\pi}_1$.

(i) K_N est une fonction positive et de norme 1.

(ii)
$$\forall x \in \mathbb{R} \setminus 2\pi\mathbb{Z},\ K_N(x) = \frac{1}{N}\left(\frac{\sin\left(\frac{Nx}{2}\right)}{\sin\left(\frac{x}{2}\right)}\right)^2$$

(iii) $K_N = \sum_{n=-N}^{N}\left(1-\frac{|n|}{N}\right)e_n$.

(iv) $\sigma_N(f) = f * K_N$.

[DEV] p. 190

Théorème 24 (Fejér)**.** Soit $f : \mathbb{R} \to \mathbb{C}$ une fonction 2π-périodique.

(i) Si f est continue, alors $\|\sigma_N(f)\|_\infty \leq \|f\|_\infty$ et $(\sigma_N(f))$ converge uniformément vers f.

(ii) Si $f \in L_p^{2\pi}$ pour $p \in [1, +\infty[$, alors $\|\sigma_N(f)\|_p \leq \|f\|_p$ et $(\sigma_N(f))$ converge vers f pour $\|.\|_p$.

Corollaire 25. L'espace des polynômes trigonométriques $\{\sum_{n=-N}^{N} c_n e_n \mid (c_n) \in \mathbb{C}^{\mathbb{N}}, N \in \mathbb{N}\}$ est dense dans l'espace des fonction continues 2π-périodiques pour $\|.\|_\infty$ et est dense dans $L_p^{2\pi}$ pour $\|.\|_p$ avec $p \in [1, +\infty[$.

Application 26. L'application $\mathscr{F}$ du Théorème 10 est injective. **[BMP]** p. 128

Application 27 (Théorème de Weierstrass)**.** Toute fonction continue sur un intervalle compact $[a, b]$ est limite uniforme sur $[a, b]$ d'une suite de polynômes. **[AMR08]** p. 192

2. Convergence ponctuelle

Théorème 28 (Dirichlet)**.** Soient $f : \mathbb{R} \to \mathbb{C}$ 2π-périodique, continue par morceaux sur $\mathbb{R}$ et $t_0 \in \mathbb{R}$ tels que la fonction **[GOU20]** p. 271

$$h \mapsto \frac{f(t_0 + h) + f(t_0 - h) - f(t_0^+) - f(t_0^-)}{h}$$

est bornée au voisinage de 0. Alors,

$$S_N(f)(t_0) \longrightarrow_{N \to +\infty} \frac{f(t_0^+) + f(t_0^-)}{2}$$

Contre-exemple 29. Soit $f : \mathbb{R} \to \mathbb{R}$ paire, 2π-périodique telle que :

$$\forall x \in [0, \pi], f(x) = \sum_{p=1}^{+\infty} \frac{1}{p^2} \sin\left((2^{p^3} + 1)\frac{x}{2}\right)$$

Alors f est bien définie et continue sur $\mathbb{R}$. Cependant, sa série de Fourier diverge en 0.

Corollaire 30. Soient $f : \mathbb{R} \to \mathbb{C}$ 2π-périodique, $\mathscr{C}^1$ par morceaux sur $\mathbb{R}$. Alors,

$$\forall x \in \mathbb{R}, S_N(f)(x) \longrightarrow_{N \to +\infty} \frac{f(x^+) + f(x^-)}{2}$$

En particulier, si f est continue en x, la série de Fourier de f converge vers $f(x)$.

Exemple 31. En reprenant la fonction de l'Théorème 15,

$$\forall x \in [-\pi,\pi],\ f(x) = \frac{2}{3} - \frac{4}{\pi^2}\sum_{n=1}^{+\infty}(-1)^n \frac{\cos(nx)}{n^2}$$

3. Convergence normale

Proposition 32. Soit $f \in L^{2\pi}_1$ et telle que sa série de Fourier converge normalement. Alors, la somme $g : x \mapsto \sum_{n=-\infty}^{+\infty} c_n(f)e_n(x)$ est une fonction continue 2π-périodique presque partout égale à f. De plus, si f est continue, l'égalité $f(x) = g(x)$ est vraie pour tout x. **[BMP]** p. 128

Proposition 33. Soit $f : \mathbb{R} \to \mathbb{C}$ 2π-périodique continue et $\mathscr{C}^1$ par morceaux sur $\mathbb{R}$. Alors $(S_N(f))$ converge normalement vers f.

Application 34 (Développement eulérien de la cotangente)**.** **[AMR08]** p. 211

$$\forall u \in \mathbb{R} \setminus \pi\mathbb{Z},\ \operatorname{cotan}(u) = \frac{1}{u} + \sum_{n=1}^{+\infty} \frac{2u}{u^2 - n^2\pi^2}$$

III - Applications

1. Calcul de sommes, de produits et d'intégrales

Application 35. En utilisant l'Théorème 31, avec $x = \pi$, on retrouve **[GOU20]** p. 272

$$\sum_{n=1}^{+\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

Application 36.

$$\forall t \in]-\pi,\pi[,\ \sin(t) = t\prod_{n=1}^{+\infty}\left(1 - \frac{t^2}{n^2\pi^2}\right)$$

Application 37 (Sommes de Gauss)**.** **[AMR08]** p. 221

$$\forall m \in \mathbb{N}^*,\ \sum_{n=0}^{m-1} e^{\frac{2i\pi n^2}{m}} = \frac{1 + i^{-m}}{1 + i^{-1}}$$

Application 38 (Intégrales de Fresnel)**.**

$$\int_{-\infty}^{+\infty} \cos(2\pi u^2)\,\mathrm{d}u = \int_{-\infty}^{+\infty} \sin(2\pi u^2)\,\mathrm{d}u = \frac{1}{2}$$

Application 39. Soit $a > 0$. En considérant la fonction $t \mapsto \frac{1}{\cosh(a)+\cos(t)}$, on en déduit que

[AMR11] p. 325

$$\forall n \in \mathbb{N},\ \int_0^{\pi} \frac{\cos(nt)}{\cosh(a)+\cos(t)}\,\mathrm{d}t = (-1)^n \frac{\pi e^{-na}}{\sinh(a)}$$

2. Équations fonctionnelles

[DEV]

Théorème 40 (Formule sommatoire de Poisson)**.** Soit $f : \mathbb{R} \to \mathbb{C}$ une fonction de classe $\mathscr{C}^1$ telle que $f(x) = O\left(\frac{1}{x^2}\right)$ et $f'(x) = O\left(\frac{1}{x^2}\right)$ quand $|x| \longrightarrow +\infty$. Alors :

[GOU20] p. 284

$$\forall x \in \mathbb{R},\ \sum_{n\in\mathbb{Z}} f(x+n) = \sum_{n\in\mathbb{Z}} \widehat{f}(2\pi n) e^{2i\pi nx}$$

où $\widehat{f}$ désigne la transformée de Fourier de f.

Application 41 (Identité de Jacobi)**.**

$$\forall s > 0,\ \sum_{n=-\infty}^{+\infty} e^{-\pi n^2 s} = \frac{1}{\sqrt{s}} \sum_{n=-\infty}^{+\infty} e^{-\frac{\pi n^2}{s}}$$

3. Inégalités remarquables

Application 42 (Inégalité isopérimétrique)**.** Soit $\gamma : [0,1] \to \mathbb{R}^2$ une courbe de Jordan (ie. $\gamma(0) = \gamma(1)$, γ est injective sur $]0,1[$ et $\gamma' \neq 0$) de classe $\mathscr{C}^1$ de longueur L et enfermant une surface S. Alors,

[AMR08] p. 215

$$S \leq \frac{L^2}{4\pi}$$

avec égalité si et seulement si γ définit un cercle.

Application 43 (Inégalité de Wirtinger)**.** Soit $f : [a,b] \to \mathbb{C}$ de classe $\mathscr{C}^1$ telle que $f(a) = f(b) = 0$. Alors,

$$\int_a^b |f(x)|^2\,\mathrm{d}x \leq \frac{(b-a)^2}{\pi}^2 \int_a^b |f'(x)|^2\,\mathrm{d}x$$

De plus, la constante $\frac{(b-a)^2}{\pi}^2$ est optimale.

Application 44 (Inégalité de Bernstein)**.** Soient $\lambda > 0$ et $\lambda_1, \dots, \lambda_n \in \mathbb{R}$ distincts et tels que $\max_{j\in[\![1,n]\!]} |\lambda_j| < \lambda$. On définit

$$h : t \mapsto \sum_{j=1}^{n} a_j e^{i\lambda_j t} \text{ où } a_1, \dots, a_n \in \mathbb{C}$$

Alors h et sa dérivée h' sont bornées et on a :

$$\|h'\|_\infty \leq \lambda \|h\|_\infty$$

[Z-Q] p. 106

Annexes

Hypothèses sur f	**Convergence de sa série de Fourier** $(S_N(f))$
$f \in L_2^{2\pi}$	Convergence pour $\|.\|_2$.
f continue	Convergence uniforme au sens de Cesàro.
$f \in L_p^{2\pi}$ $(p \in L_p[1,+\infty[)$	Convergence pour $\|.\|_p$ au sens de Cesàro.
f $\mathscr{C}^1$ par morceaux	Convergence ponctuelle vers une valeur moyenne.
f continue et $\mathscr{C}^1$ par morceaux	Convergence normale.

FIGURE I.29 – Convergence d'une série de Fourier selon les hypothèses sur la fonction de départ.

250 Transformation de Fourier. Applications.

I - Transformation de Fourier dans $L_1(\mathbb{R}^d)$

1. Définitions et premières propriétés

Définition 1. Soit $f : \mathbb{R}^d \to \mathbb{C}$ une fonction mesurable. On définit, lorsque cela a un sens, sa **transformée de Fourier**, notée $\widehat{f}$ par

$$\widehat{f} : \begin{array}{ccc} \mathbb{R}^d & \to & \mathbb{C} \\ \xi & \mapsto & \int_{\mathbb{R}^d} f(x) e^{-i\langle x,\xi\rangle} \, \mathrm{d}x \end{array}$$

[AMR08] p. 109

Exemple 2 (Densité de Poisson)**.** On pose $\forall x \in \mathbb{R}$, $p(x) = \frac{1}{2} e^{-|x|}$. Alors $p \in L_1(\mathbb{R})$ et, $\forall \xi \in \mathbb{R}$, $\widehat{p}(\xi) = \frac{1}{1+\xi^2}$.

[DEV]

Exemple 3 (Transformée de Fourier d'une gaussienne)**.** On définit $\forall a \in \mathbb{R}_*^+$,

$$\gamma_a : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & e^{-ax^2} \end{array}$$

Alors,

$$\forall \xi \in \mathbb{R}, \widehat{\gamma_a}(\xi) = \sqrt{\frac{\pi}{a}} e^{\frac{-\xi^2}{4a}}$$

p. 156

Lemme 4 (Riemann-Lebesgue)**.** Soit $f \in L_1(\mathbb{R}^d)$, $\widehat{f}$ existe et

$$\lim_{\|\xi\| \to +\infty} \widehat{f}(\xi)$$

p. 109

Remarque 5. La transformée de Fourier d'une fonction intégrable n'est pas forcément intégrable.

Théorème 6. $\forall f \in L_1(\mathbb{R}^d)$, $\widehat{f}$ est continue, bornée par $\|f\|_1$. Donc la **transformation de Fourier**

$$\mathscr{F} : \begin{array}{ccc} L_1(\mathbb{R}^d) & \to & \mathscr{C}_0(\mathbb{R}^d) \\ f & \mapsto & \widehat{f} \end{array}$$

est bien définie.

Corollaire 7. La transformation de Fourier $\mathscr{F} : L_1(\mathbb{R}^d) \to \mathscr{C}_0(\mathbb{R}^d)$ est une application linéaire continue.

Proposition 8. Soit $f \in L_1(\mathbb{R}^d)$. Alors :

(i) $\mathscr{F}(x \mapsto f(-x)) = \xi \mapsto \mathscr{F}(f)(-\xi)$.

(ii) $\mathscr{F}(\overline{f}) = \xi \mapsto \overline{\mathscr{F}(f)(-\xi)}$.

(iii) Pour tout $\lambda \in \mathbb{R}_*$, et $\xi \in \mathbb{R}^d$,

$$\mathscr{F}(x \mapsto f(\lambda x)) = \frac{1}{|\lambda|^d}\mathscr{F}(f)\left(\frac{\xi}{\lambda}\right)$$

(iv) Pour tout $a \in \mathbb{R}^d$,

$$\mathscr{F}(x \mapsto f(x-a)) = e^{-i\langle a,\xi\rangle}\mathscr{F}(f) \text{ et } \mathscr{F}(x \mapsto e^{-i\langle a,\xi\rangle}f(x)) = \xi \mapsto \mathscr{F}(f)(\xi - a)$$

Proposition 9. Soit $f \in L_1(\mathbb{R}^d)$. p. 120

(i) On suppose $f \in \mathscr{C}^1(\mathbb{R}^d)$ et $\frac{\partial f}{\partial x_j} \in L_1(\mathbb{R}^d)$. Alors,

$$\forall \xi = (\xi_1, \dots, \xi_d) \in \mathbb{R}^d,\ \widehat{\frac{\partial f}{\partial x_j}}(\xi) = i\xi_j \widehat{f}(\xi)$$

(ii) On suppose $y_j f \in L_1(\mathbb{R}^d)$. Alors, la j-ième dérivée partielle de $\widehat{f}$ existe, et,

$$\forall \xi \in \mathbb{R}^d,\ \frac{\partial \widehat{f}}{\partial x_j}(\xi) = -i\widehat{(y_j f)}(\xi)$$

Application 10. On considère $f : x \mapsto e^{-\alpha x^2}$ pour $\alpha > 0$. Alors, f vérifie **[GOU20]** p. 169

$$\forall x \in \mathbb{R},\ \widehat{f}(\xi) = \frac{1}{i\xi}f(\xi)$$

ce qui permet de retrouver l'Théorème 3.

2. Convolution

Définition 11. Soient f et g deux fonctions de $\mathbb{R}^d$ dans $\mathbb{R}$. On dit que **la convolée** (ou **le produit de convolution**) de f et g en $x \in \mathbb{R}$ **existe** si la fonction

$$\begin{array}{ccc} \mathbb{R} & \to & \mathbb{C} \\ t & \mapsto & f(x-t)g(t) \end{array}$$

est intégrable sur $\mathbb{R}^d$ pour la mesure de Lebesgue. On pose alors :

$$(f*g)(x) = \int_{\mathbb{R}^d} f(x-t)g(t)\,\mathrm{d}t$$

[AMR08] p. 75

Exemple 12. Soient $a < b \in \mathbb{R}_*^+$. Alors $\mathbb{1}_{[-a,a]} * \mathbb{1}_{[-b,b]}$ existe pour tout $x \in \mathbb{R}$ et

$$\left(\mathbb{1}_{[-a,a]} * \mathbb{1}_{[-b,b]}\right)(x) = \begin{cases} 2a & \text{si } 0 \le |x| \le b-a \\ b+a-|x| & \text{si } b-a \le |x| \le b+a \\ 0 & \text{sinon} \end{cases}$$

Proposition 13. Dans $L_1(\mathbb{R}^d)$, dès qu'il a un sens, le produit de convolution de deux fonctions est commutatif, bilinéaire et associatif.

Théorème 14 (Convolution dans $L_1(\mathbb{R}^d)$)**.** Soient $f, g \in L_1(\mathbb{R}^d)$. Alors :

(i) pp. en $x \in \mathbb{R}^d$, $t \mapsto f(x-t)g(t)$ est intégrable sur $\mathbb{R}^d$.

(ii) $f*g$ est intégrable sur $\mathbb{R}^d$.

(iii) $\|f*g\|_1 \le \|f\|_1 \|g\|_1$.

(iv) L'espace vectoriel normé $(L_1(\mathbb{R}^d), \|.\|_1)$ muni de $*$ est une algèbre de Banach commutative.

Proposition 15.

$$\forall f, g \in L_1(\mathbb{R}^d),\ \widehat{f*g} = \hat{f}\hat{g}$$

ie. $\mathscr{F} : (L_1(\mathbb{R}^d), +, *, \cdot) \to (\mathscr{C}_0(\mathbb{R}^d), +, \times, \cdot)$ est un morphisme d'algèbres.

p. 114

Corollaire 16. L'algèbre $(L_1(\mathbb{R}^d), +, *, \cdot)$ n'a pas d'élément unité.

Application 17.

$$f*f = f \iff f = 0$$

Théorème 18 (Formule de dualité)**.**

$$\forall f,g \in L_1(\mathbb{R}^d), \int_{\mathbb{R}^d} f(t)\widehat{g}(t)\,\mathrm{d}t = \int_{\mathbb{R}^d} \widehat{f}(t)g(t)\,\mathrm{d}t$$

3. Inversion

Théorème 19 (Formule d'inversion de Fourier)**.** Si $f \in L_1(\mathbb{R}^d)$ est telle que $\widehat{f} \in L_1(\mathbb{R}^d)$, alors

$$\widehat{\widehat{f}}(x) = (2\pi)^d f(x) \text{ pp. en } x \in \mathbb{R}^d$$

Exemple 20. Une solution de l'équation intégrale d'inconnue y :

$$\int_{\mathbb{R}} \frac{y(t)}{(x-t)^2+a^2} = \frac{1}{x^2+b^2}$$

est $x \mapsto \frac{a(b-a)}{b\pi(x^2+(b-a)^2)}$ pour $0 < a < b$.

Corollaire 21. La transformation de Fourier $\mathscr{F} : L_1(\mathbb{R}^d) \to \mathscr{C}_0(\mathbb{R}^d)$ est une application injective.

Proposition 22. Soient $g \in L_1(\mathbb{R}^d)$ et $f \in L_1(\mathbb{R}^d)$ telle que $\widehat{f} \in L_1(\mathbb{R}^d)$, alors

$$\widehat{fg} = \frac{1}{(2\pi)^d}\widehat{f} * \widehat{g}$$

II - Transformation de Fourier dans d'autres espaces

1. Dans $L_2(\mathbb{R}^d)$

Théorème 23 (Plancherel-Parseval)**.**

p. 122

$$\forall f \in L_1(\mathbb{R}^d) \cap L_2(\mathbb{R}^d),\ \|\widehat{f}\|_2^2 = (2\pi)^d \|f\|_2^2$$

Remarque 24. En termes de produit scalaire, la formule précédente s'écrit

$$\forall f,g \in L_2(\mathbb{R}^d), \int_{\mathbb{R}^d} \widehat{f}(\xi)\overline{\widehat{g}(\xi)}\,\mathrm{d}\xi = (2\pi)^d \int_{\mathbb{R}^d} f(x)\overline{g(x)}\,\mathrm{d}x$$

Théorème 25. Soit $f \in L_2(\mathbb{R}^d)$. Alors :

(i) Il existe une suite (f_n) de $L_1(\mathbb{R}^d) \cap L_2(\mathbb{R}^d)$ qui converge vers f dans $L_2(\mathbb{R}^d)$.

(ii) Pour une telle suite (f_n), la suite $(\widehat{f_n})$ converge dans $L_2(\mathbb{R}^d)$ vers une limite $\widetilde{f}$ indépendante de la suite choisie.

Définition 26. La limite $\widetilde{f}$ est la **transformée de Fourier** de f dans $L_2(\mathbb{R}^d)$.

Proposition 27. Les transformations de Fourier $L_1(\mathbb{R}^d)$ et $L_2(\mathbb{R}^d)$ coïncident sur $L_1(\mathbb{R}^d) \cap L_2(\mathbb{R}^d)$.

Remarque 28. On a prolongé $\mathscr{F}$ à $L_2(\mathbb{R}^d)$, mais il faut prendre garde au fait que $\mathscr{F}$ désigne deux applications distinctes : $\mathscr{F} : L_1(\mathbb{R}^d) \to \mathscr{C}_0(\mathbb{R}^d)$ et $\mathscr{F} : L_2(\mathbb{R}^d) \to L_2(\mathbb{R}^d)$, ces deux applications ne coïncidant que sur $L_1(\mathbb{R}^d) \cap L_2(\mathbb{R}^d)$.

Proposition 29. Soit $f \in L_2(\mathbb{R})$. On a les relations suivantes :

$$\lim_{A\to+\infty} \|\varphi_A - f\|_2 = 0 \text{ et } \lim_{A\to+\infty} \|\psi_A - f\|_2 = 0$$

où

$$\varphi_A(\xi) = \int_{-A}^{A} f(x)e^{-ix\xi}\,\mathrm{d}x \text{ et } \psi_A(\xi) = \frac{1}{2\pi}\int_{-A}^{A} \widehat{f}(\xi)e^{-ix\xi}\,\mathrm{d}\xi$$

Corollaire 30. Lorsque $f \in L_2(\mathbb{R})$ et $\widehat{f} \in L_1(\mathbb{R})$, on a

$$\text{pp. en } x \in \mathbb{R},\ f(x) = \frac{1}{2\pi}\int_{-\infty}^{+\infty} \widehat{f}(\xi)e^{-ix\xi}\,\mathrm{d}\xi$$

Théorème 31 (Formule d'inversion de Fourier-Plancherel)**. L'opérateur de Fourier-Plancherel**

$$\mathscr{P} : \begin{array}{ccc} L_2(\mathbb{R}^d) & \to & L_2(\mathbb{R}^d) \\ f & \mapsto & \frac{1}{(\sqrt{2\pi})^d}\mathscr{F}(f) \end{array}$$

est un automorphisme d'inverse $\mathscr{P}^{-1} = \overline{\mathscr{P}}$.

Exemple 32. On pose $f = \mathbb{1}_{[-a,a]}$ et on a $\forall \xi \neq 0$, $\widehat{f}(\xi) = \frac{2\sin(a\xi)}{\xi}$. Or, $\widehat{f} \in L_2(\mathbb{R}) \setminus L_1(\mathbb{R})$. On peut calculer sa transformée de Fourier dans $L_2(\mathbb{R})$: [D-L] p. 451

$$\forall x \in \mathbb{R},\ \widehat{\widehat{f}}(x) = (\widehat{\widehat{f}})(x) = f(-x) = \mathbb{1}_{[-a,a]}(x)$$

2. Dans $\mathscr{S}(\mathbb{R}^d)$

Définition 33. Une fonction $f : \mathbb{R}^d \to \mathbb{C}$ est dite **à décroissance rapide** si

$$\forall \alpha \in \mathbb{N}^d, \lim_{\|x\| \to +\infty} |x^\alpha f(x)| = 0$$

où $(x_1, \dots, x_d)^{(\alpha_1, \dots, \alpha_d)} = x_1^{\alpha_1} \dots x_d^{\alpha_d}$.

[AMR08] p. 133

Exemple 34. $x \mapsto e^{-|x|}$ est à décroissance rapide sur $\mathbb{R}$.

Définition 35. On appelle **classe de Schwartz**, noté $\mathscr{S}(\mathbb{R}^d)$, l'espaces des fonctions de $f : \mathbb{R}^d \to \mathbb{C}$ telles que :

— $f \in \mathscr{C}^\infty(\mathbb{R}^d)$.

— f est à décroissance rapide ainsi que toutes ses dérivées.

Proposition 36. $\mathscr{S}(\mathbb{R}^d)$ est un espace vectoriel stable par dérivation, par multiplication par un polynôme, par produit, par conjugaison et par translation.

Théorème 37. (i) $\mathscr{S}(\mathbb{R}^d) \subseteq L_1(\mathbb{R}^d)$.

(ii) $\mathscr{F}(\mathscr{S}(\mathbb{R}^d)) \subseteq \mathscr{S}(\mathbb{R}^d)$.

Théorème 38. $\mathscr{F} : \mathscr{S}(\mathbb{R}^d) \to \mathscr{S}(\mathbb{R}^d)$ est un automorphisme bicontinu de $\mathscr{S}(\mathbb{R}^d)$ dont l'inverse est donné par

$$\mathscr{F}^{-1} = \frac{1}{(2\pi)^d} \overline{F}$$

III - Applications

1. Séries de fonctions

Théorème 39 (Formule sommatoire de Poisson)**.** Soit $f : \mathbb{R} \to \mathbb{C}$ une fonction de classe $\mathscr{C}^1$ telle que $f(x) = O\left(\frac{1}{x^2}\right)$ et $f'(x) = O\left(\frac{1}{x^2}\right)$ quand $|x| \longrightarrow +\infty$. Alors :

$$\forall x \in \mathbb{R}, \sum_{n \in \mathbb{Z}} f(x+n) = \sum_{n \in \mathbb{Z}} \widehat{f}(2\pi n) e^{2i\pi n x}$$

[GOU20] p. 284

Application 40 (Identité de Jacobi)**.**

$$\forall s>0,\ \sum_{n=-\infty}^{+\infty} e^{-\pi n^2 s} = \frac{1}{\sqrt{s}} \sum_{n=-\infty}^{+\infty} e^{-\frac{\pi n^2}{s}}$$

2. Bases hilbertiennes

Soit I un intervalle de $\mathbb{R}$. On pose $\forall n \in \mathbb{N}$, $g_n : x \mapsto x^n$.

[BMP] p. 110

Définition 41. On appelle **fonction poids** une fonction $\rho : I \to \mathbb{R}$ mesurable, positive et telle que $\forall n \in \mathbb{N}, \rho g_n \in L_1(I)$.

Soit $\rho : I \to \mathbb{R}$ une fonction poids.

Notation 42. On note $L_2(I,\rho)$ l'espace des fonctions de carré intégrable pour la mesure de densité ρ par rapport à la mesure de Lebesgue.

Proposition 43. Muni de

$$\langle .,. \rangle : (f,g) \mapsto \int_I f(x)\overline{g(x)}\rho(x)\,\mathrm{d}x$$

$L_2(I,\rho)$ est un espace de Hilbert.

Théorème 44. Il existe une unique famille (P_n) de polynômes unitaires orthogonaux deux-à-deux telle que $\deg(P_n) = n$ pour tout entier n. C'est la famille de **polynômes orthogonaux** associée à ρ sur I.

Exemple 45 (Polynômes de Hermite)**.** Si $\forall x \in I$, $\rho(x) = e^{-x^2}$, alors

$$\forall n \in \mathbb{N},\ \forall x \in I,\ P_n(x) = \frac{(-1)^n}{2^n} e^{x^2} \frac{\partial}{\partial x^n}\left(e^{-x^2}\right)$$

Lemme 46. On suppose que $\forall n \in \mathbb{N}$, $g_n \in L_1(I,\rho)$ et on considère (P_n) la famille des polynômes orthogonaux associée à ρ sur I. Alors $\forall n \in \mathbb{N}$, $g_n \in L_2(I,\rho)$. En particulier, l'algorithme de Gram-Schmidt a bien du sens et (P_n) est bien définie.

p. 140

[DEV]

Application 47. On considère (P_n) la famille des polynômes orthogonaux associée à ρ sur I et on suppose qu'il existe $a > 0$ tel que

$$\int_I e^{a|x|}\rho(x)\,\mathrm{d}x < +\infty$$

alors (P_n) est une base hilbertienne de $L_2(I,\rho)$ pour la norme $\|.\|_2$.

Contre-exemple 48. On considère, sur $I=\mathbb{R}_*^+$, la fonction poids $\rho : x \mapsto x^{-\ln(x)}$. Alors, la famille des g_n n'est pas totale. La famille des polynômes orthogonaux associée à ce poids particulier n'est donc pas totale non plus : ce n'est pas une base hilbertienne.

3. En probabilités

Soit $X : (\Omega, \mathcal{A}, \mathbb{P}) \to (\mathbb{R}^d, \mathcal{B}(\mathbb{R}^d))$ un vecteur aléatoire.

[G-K] p. 239

Définition 49. On appelle **fonction caractéristique** de X, notée ϕ_X, la transformée de Fourier de la loi $\mathbb{P}_X$ (définie à un signe près) :

$$\phi_X : t \mapsto \mathbb{E}(e^{i\langle t,x\rangle})$$

Remarque 50. Si X est un vecteur aléatoire réel admettant f pour densité, alors p. 165

$$\forall t \in \mathbb{R}^d,\ \phi_X(t) = \int_{\mathbb{R}^d} e^{i\langle t,x\rangle} f(x)\,\mathrm{d}\mathbb{P}(x)$$

Théorème 51. Soient X et Y deux vecteurs aléatoires réels. Alors, p. 239

$$\phi_X = \phi_Y \iff \mathbb{P}_X = \mathbb{P}_Y$$

Exemple 52.
- $X \sim \mathcal{U}([-1,1]) \iff \forall t \in \mathbb{R},\ \phi_X(t) = \begin{cases} \frac{\sin(t)}{t} \text{ si } t \neq 0 \\ 1 \text{ sinon} \end{cases}$
- $X \sim \mathcal{E}(\lambda) \iff \forall t \in \mathbb{R},\ \phi_X(t) = \frac{1}{1-it}$.
- $X(\Omega) \subseteq \mathbb{N} \implies \forall t \in \mathbb{R},\ \phi_X(t) = G_X(e^{it})$ où G_X est la fonction génératrice de X.

Théorème 53. Soit $N \in \mathbb{N}^*$, alors dans pour une variable aléatoire réelle,

$$\mathbb{E}(|X|^N) < +\infty \implies \phi_X \in \mathcal{C}^n(\mathbb{R})$$

Corollaire 54. On se place dans le cadre du théorème précédent. On a :

$$\forall k \in [\![0,N]\!],\ \phi_X^{(k)}(0) = i^k \mathbb{E}(X^k)$$

Théorème 55. Si X et Y sont deux vecteurs aléatoires réels indépendants :

(i) $\phi_{X+Y} = \phi_X \phi_Y$.

(ii) $\forall s,t \in \mathbb{R}^d$, $\phi_{(X,Y)}(s,t) = \phi_X(s)\phi_Y(t)$.

253 Utilisation de la notion de convexité en analyse.

Soit E un espace vectoriel sur $\mathbb{R}$ ou $\mathbb{C}$.

I - Convexité d'une fonction, d'un ensemble

1. Ensembles convexes

a. Généralités

Définition 1. — Soient $a, b \in E$. On appelle **segment** d'extrémités a et b, l'ensemble

$$[a,b] = \{ta + (1-t)b \mid t \in [0,1]\}$$

— On dit qu'une partie C de E est **convexe** si

$$\forall a, b \in E, [a,b] \subseteq E$$

[GOU21] p. 51

Exemple 2. Un sous-espace vectoriel de E est convexe.

Remarque 3. Une partie convexe est connexe.

Proposition 4. (i) Dans $\mathbb{R}$, les intervalles sont à la fois les parties connexes et convexes.
(ii) Une intersection de parties convexes est convexe.

[BMP] p. 26

b. Enveloppes convexes

Définition 5. Soit $A \subseteq E$. On appelle **enveloppe convexe** de A le plus petit (au sens de l'inclusion) convexe contenant A. On la note $\mathrm{Conv}(A)$.

[GOU21] p. 51

Proposition 6. Soit $A \subseteq E$. Alors,

$$x \in \mathrm{Conv}(A) \iff x = \sum_{i=1}^{n} \lambda_i x_i \text{ avec } x_1, \dots, x_n \in A \text{ et } \lambda_1, \dots, \lambda_n \in \mathbb{R}^+ \text{ tels que } \sum_{i=1}^{n} \lambda_i = 1$$

Théorème 7 (Carathéodory)**.** Soit $A \subseteq E$. On suppose que E est un espace vectoriel normé de dimension finie n. Alors, tout élément de $\mathrm{Conv}(A)$ est combinaison convexe de $n+1$ éléments de A.

p. 54

Application 8. Soit $A \subseteq E$ compact. On suppose que E est un espace vectoriel normé de dimension finie. Alors $\mathrm{Conv}(A)$ est compacte.

Proposition 9. On suppose que E est un espace vectoriel normé. Alors, pour toute partie convexe C de E, $\overline{C}$ et $\mathring{C}$ sont convexes.

Théorème 10 (Hahn-Banach géométrique)**.** On se place dans le cas où E est un espace de Hilbert sur $\mathbb{R}$. Soit C une partie de E convexe compacte. Alors, si $x \notin C$, il existe $f \in E'$ et $\alpha \in \mathbb{R}$ tels que

$$\forall y \in C,\ f(x) < \alpha < f(y)$$

[BMP] p. 97

Corollaire 11. On se place dans le cas où E est un espace de Hilbert sur $\mathbb{R}$. Soit $A \subseteq E$. Alors,

$$x \in \overline{\mathrm{Conv}(A)} \iff \forall f \in H',\ f(x) \leq \sup_{y \in A} f(y)$$

p. 133

2. Fonctions convexes

On munit E d'une norme $\|.\|$. Soit I une partie convexe de E.

Définition 12.
— Une fonction $f : I \to \mathbb{R}$ est **convexe** si

$$\forall x, y \in I,\ \forall t \in [0,1],\ f((1-t)x + ty) \leq (1-t)f(x) + tf(y)$$

— Une fonction $f : I \to \mathbb{R}$ est **concave** si $-f$ est convexe.

[ROM19-1] p. 225

Remarque 13. Les définitions de f **strictement convexe** et f **strictement concave** s'obtiennent en remplaçant les inégalités larges par des inégalités strictes dans la définition précédente.

Exemple 14.
— $x \mapsto \|x\|$ est convexe sur E.
— exp est convexe sur $\mathbb{R}$.

Proposition 15. Une fonction $f : I \to \mathbb{R}$ est convexe si et seulement si son épigraphe est convexe dans $E \times \mathbb{R}$.

Théorème 16. Une fonction $f : I \to \mathbb{R}$ est convexe si et seulement si $\forall x, y \in I$, $t \mapsto f((1-t)x + ty)$ est convexe sur $[0,1]$.

Ce dernier théorème justifie que l'étude des fonctions convexes se ramène à l'étude des fonctions convexes sur un intervalle réel.

Proposition 17. — Une combinaison linéaire à coefficients positifs de fonctions convexes est convexe.

— La composée $\varphi \circ g$ d'une fonction convexe croissante $\varphi : J \to \mathbb{R}$ avec une fonction fonction convexe $g : I \to J$ est croissante.

— Une limite simple d'une suite de fonctions convexes est convexe.

3. Fonctions log-convexes

Définition 18. On dit qu'une fonction $f : I \to \mathbb{R}_*^+$ est **log-convexe** si $\ln \circ f$ est convexe sur I. p. 228

Proposition 19. Une fonction log-convexe est convexe.

Contre-exemple 20. $x \mapsto x$ est convexe mais non log-convexe.

Théorème 21. Pour une fonction $f : I \to \mathbb{R}_*^+$, les assertions suivantes sont équivalentes :

(i) f est log-convexe.

(ii) $\forall \alpha > 0$, $x \mapsto \alpha^x f(x)$ est convexe.

(iii) $\forall x, y \in I$, $\forall t \in [0,1]$, $f((1-t)x + ty) \leq (f(x))^{1-t}(f(y))^t$.

(iv) $\forall \alpha > 0$, f^α est convexe.

Lemme 22. La fonction Γ définie pour tout $x > 0$ par $\Gamma(x) = \int_0^{+\infty} t^{x-1} e^{-t} \, \mathrm{d}t$ vérifie : p. 364

(i) $\forall x \in \mathbb{R}_*^+$, $\Gamma(x+1) = x\Gamma(x)$.

(ii) $\Gamma(1) = 1$.

(iii) Γ est log-convexe sur $\mathbb{R}_*^+$.

[DEV]

Théorème 23 (Bohr-Mollerup)**.** Soit $f : \mathbb{R}_*^+ \to \mathbb{R}^+$ vérifiant le Point (i), Point (ii) et Point (iii) du Théorème 22. Alors $f = \Gamma$.

Remarque 24. À la fin de la preuve, on obtient une formule due à Gauss :

$$\forall x \in]0,1], \Gamma(x) = \lim_{n \to +\infty} \frac{n^x n!}{(x+n)\dots(x+1)x}$$

que l'on peut aisément étendre à $\mathbb{R}_*^+$ entier.

II - Inégalités de convexité

1. Inégalités pour des familles de réels

Proposition 25 (Inégalité de Hölder)**.** Soient $p, q > 0$ tels que $\frac{1}{p} + \frac{1}{q} = 1$. Alors,

$$\forall a_1, \dots, a_n, b_1, \dots, b_n \geq 0, \sum_{i=1}^{n} a_i b_i \leq \left(\sum_{i=1}^{n} a_i^p\right)^{\frac{1}{p}} \left(\sum_{i=1}^{n} b_i^q\right)^{\frac{1}{q}}$$

[GOU20] p. 97

Proposition 26 (Inégalité de Minkowski)**.** Soit $p \geq 1$. Alors,

$$\forall x_1, \dots, x_n, y_1, \dots, y_n \geq 0, \left(\sum_{i=1}^{n} |x_i + y_i|^p\right)^{\frac{1}{p}} \leq \left(\sum_{i=1}^{n} x_i^p\right)^{\frac{1}{p}} \left(\sum_{i=1}^{n} y_i^p\right)^{\frac{1}{p}}$$

Proposition 27 (Comparaison des moyennes harmonique, géométrique et arithmétique)**.** Pour toute suite finie $x = (x_i)$ de n réels strictement positifs, on a :

$$\frac{n}{\sum_{i=1}^{n} \frac{1}{x_i}} \leq \left(\prod_{i=1}^{n} x_i\right)^{\frac{1}{n}} \leq \frac{1}{n} \sum_{i=1}^{n} x_i$$

[ROM19-1] p. 242

2. Inégalités en théorie de l'intégration

Proposition 28 (Inégalité de Jensen)**.** Si $f : \mathbb{R} \to \mathbb{R}$ est convexe, alors pour toute fonction u continue sur un intervalle $[a, b]$, on a :

$$f\left(\frac{1}{b-a} \int_a^b u(t)\,\mathrm{d}t\right) \leq \frac{1}{b-a} \int_a^b f \circ u(t)\,\mathrm{d}t$$

Théorème 29 (Inégalité de Hölder)**.** Soient $p, q \in]1, +\infty[$ tels que $\frac{1}{p} + \frac{1}{q} = 1$, $f \in \mathscr{L}_p$ et $g \in \mathscr{L}_q$. Alors $fg \in \mathscr{L}_1$ et

$$\|fg\|_1 \leq \|f\|_p \|g\|_q$$

[G-K] p. 209

Remarque 30. C'est encore vrai pour $q = +\infty$ en convenant que $\frac{1}{+\infty} = 0$.

Application 31. Dans un espace de mesure finie,

$$1 \leq p < q \leq +\infty \implies L_q \subseteq L_p$$

Théorème 32 (Inégalité de Minkowski)**.**

$$\forall f, g \in \mathscr{L}_p,\ \|f+g\|_p \leq \|f\|_p + \|g\|_p$$

III - Convexité et optimisation

1. Pour les fonctions convexes

Soit $I \subseteq \mathbb{R}$ un intervalle réel non réduit à un point.

[ROM19-1] p. 234

Proposition 33. Une fonction $f : \mathbb{R} \to \mathbb{R}$ est constante si et seulement si elle est convexe et majorée.

Contre-exemple 34. La fonction f définie sur $\mathbb{R}^+$ par $f(x) = \frac{1}{1+x}$ est convexe, majorée, mais non constante.

Proposition 35. Si $f : I \to \mathbb{R}$ est convexe et est dérivable en un point $\alpha \in \mathring{I}$ tel que $f'(\alpha) = 0$, alors f admet un minimum global en α.

Proposition 36. Si $f : I \to \mathbb{R}$ est convexe et admet un minimum local, alors ce minimum est global.

2. Dans un espace de Hilbert

Pour toute la suite, on fixe H un espace de Hilbert de norme $\|.\|$ et on note $\langle .,. \rangle$ le produit scalaire associé.

[LI] p. 32

Lemme 37 (Identité du parallélogramme)**.**

$$\forall x, y \in H,\ \|x+y\|^2 + \|x-y\|^2 = 2(\|x\|^2\|y\|^2)$$

et cette identité caractérise les normes issues d'un produit scalaire.

[DEV]

Théorème 38 (Projection sur un convexe fermé)**.** Soit $C \subseteq H$ un convexe fermé non-vide.

Alors :

$$\forall x \in H, \exists! y \in C \text{ tel que } d(x,C) = \inf_{z\in C} \|x-z\| = d(x,y)$$

On peut donc noter $y = P_C(x)$, le **projeté orthogonal de x sur C**. Il s'agit de l'unique point de C vérifiant

$$\forall z \in C, \langle x - P_C(x), z - P_C(x)\rangle \leq 0$$

Théorème 39. Si F est un sous espace vectoriel fermé dans H, alors P_F est une application linéaire continue. De plus, pour tout $x \in H$, $P_F(x)$ est l'unique point $y \in F$ tel que $x - y \in F^\perp$.

Théorème 40. Si F est un sous espace vectoriel fermé dans H, alors

$$H = F \oplus F^\perp$$

et P_F est la projection sur F parallèlement à $F^\perp$: c'est la **projection orthogonale** sur F.

Corollaire 41. Soit F un sous-espace vectoriel de H. Alors,

$$\overline{F} = H \iff F^\perp = 0$$

Théorème 42 (de représentation de Riesz)**.**

$$\forall \varphi \in H', \exists! y \in H, \text{ tel que } \forall x \in H, \varphi(x) = \langle x, y\rangle$$

et de plus, $|||\varphi||| = \|y\|$.

Corollaire 43.

$$\forall T \in H', \exists! U \in H' \text{ tel que } \forall x, y \in H, \langle T(x), y\rangle = \langle x, U(y)\rangle$$

On note alors $U = T^*$: c'est **l'adjoint** de T. On a alors $|||T||| = |||T^*|||$.

Application 44. L'application

$$\varphi : \begin{array}{ll} L_q & \to (L_p)' \\ g & \mapsto \left(\varphi_g : f \mapsto \int_X fg\,\mathrm{d}\mu\right) \end{array} \qquad \text{où } \frac{1}{p} + \frac{1}{q} = 1$$

est une isométrie linéaire surjective. C'est donc un isomorphisme isométrique.

[Z-Q] p. 222

261 Loi d'une variable aléatoire : caractérisations, exemples, applications.

Soit $(\Omega, \mathscr{A}, \mathbb{P})$ un espace probabilisé.

I - Loi d'une variable aléatoire

1. Définitions

a. Préliminaires théoriques

Définition 1. Soient $(E, \mathscr{F})$ un espace probabilisable. On appelle **variable aléatoire** toute fonction $X : \Omega \to E$ mesurable. On appelle **loi** de X la mesure image de $\mathbb{P}$ par X, définie par

$$\mathbb{P}_X : \begin{array}{ccc} \mathscr{F} & \to & [0,1] \\ F & \mapsto & \mathbb{P}(X^{-1}(F)) \end{array}$$

[GOU21] p. 334

Notation 2. Pour alléger les notations, on écrira $\{X \in F\}$ pour désigner l'ensemble $X^{-1}(F)$. Ainsi, $\mathbb{P}(X^{-1}(F))$ devient $\mathbb{P}(X \in F)$. De même, $\{X = x\}$ désigne l'ensemble $X^{-1}(\{x\})$, $\{X \leq a\}$ désigne l'ensemble $X^{-1}(]-\infty, a])$ (dans le cas réel), etc.

Exemple 3. On se place dans $(\mathbb{R}, \mathscr{B}(\mathbb{R}), \mathbb{P})$ où $\mathbb{P} = \frac{1}{3}\delta_{-1} + \frac{1}{2}\delta_0 + \frac{1}{6}\delta_1$ et on considère la fonction réelle $X : \omega \mapsto \omega$. Alors, X est une variable aléatoire, dont la loi est $\mathbb{P}_X = \mathbb{P}$.

[G-K] p. 118

Définition 4. Une variable aléatoire X est dite **réelle** si son espace d'arrivée est $(\mathbb{R}, \mathscr{B}(\mathbb{R}))$.

[GOU21] p. 334

b. Lois discrètes

Définition 5.
— On dit qu'une loi μ est **discrète** s'il existe un ensemble D fini tel que $\mu(D) = 1$.
— On dit que la variable aléatoire X est discrète si sa loi $\mathbb{P}_X$ est discrète.

[G-K] p. 335

Remarque 6. Cela revient à dire que $X(\Omega)$ est fini ou est dénombrable.

[GOU21] p. 335

Exemple 7. On pose $\Omega = \{(\omega_n) \in \mathbb{R}^n \mid \omega_n \in \{0,1\}\ \forall n \in \mathbb{N}\}$ et $X : (\omega_n) \mapsto \inf\{n \in \mathbb{N} \mid \omega_n = 0\}$. Alors X est une variable aléatoire discrète, à valeurs dans $\mathbb{N} \cup \{+\infty\}$.

Proposition 8. Si X est une variable aléatoire discrète à valeurs dans un ensemble dénombrable D, alors : [G-K] p. 131

(i) $\forall A \in \mathscr{B}(\mathbb{R}), \mathbb{P}_X(A) = \sum_{i \in D \cap A} \mathbb{P}(X = i)$.

(ii) $\mathbb{P}_X = \sum_{i \in D} \mathbb{P}(X = i)\delta_i$ où les δ_i sont des masses de Dirac (voir Théorème 9 Théorème 9).

Exemple 9. Soit $X : \Omega \to \mathbb{R}$ une variable aléatoire réelle. Voici quelques exemples de lois discrètes classiques. p. 137

— Si $x \in \Omega$, on pose $\delta_x : A \mapsto \mathbb{1}_A(x)$. C'est une loi discrète sur $\mathscr{P}(\Omega)$.

— Soit $E \subseteq \Omega$ fini. On appelle loi uniforme sur E la loi discrète définie sur $\mathscr{P}(\Omega)$ par

$$\begin{array}{ccc} \mathscr{P}(\Omega) & \to & [\![0,1]\!] \\ A & \mapsto & \frac{|A \cap E|}{|E|} \end{array}$$

— X suit une loi de Bernoulli de paramètre $p \in [0,1]$, notée $\mathscr{B}(p)$, si $\mathbb{P}(X = 1) = p$ et $\mathbb{P}(X = 0) = 1 - p$. Dans ce cas, X est bien une loi discrète et on a

$$\mathbb{P}_X = (1-p)\delta_0 + p\delta_1$$

— X suit une loi de binomiale de paramètres $n \in \mathbb{N}$ et $p \in [0,1]$, notée $\mathscr{B}(n,p)$, si X est la somme de n variables aléatoires indépendantes qui suivent des lois de Bernoulli de paramètre p. Dans ce cas, X est bien une loi discrète et on a

$$\forall k \in \mathbb{N}, \mathbb{P}(X = k) = \binom{n}{k} p^k (1-p)^{n-k}$$

— X suit une loi géométrique de paramètre $p \in]0,1]$, notée $\mathscr{G}(p)$, si l'on a

$$\forall k \in \mathbb{N}^*, \mathbb{P}(X = k) = p(1-p)^{k-1}$$

— X suit une loi de Poisson de paramètre $\lambda > 0$, notée $\mathscr{P}(\lambda)$, si l'on a

$$\forall k \in \mathbb{N}^*, \mathbb{P}(X = k) = e^{-\lambda} \frac{\lambda^k}{k!}$$

c. Lois à densité

Définition 10. On dit qu'une loi réelle μ est **à densité** s'il existe une fonction mesurable f telle que

$$\forall A \in \mathscr{B}(\mathbb{R}),\ \mu(A) = \int_A f \,\mathrm{d}\lambda$$

p. 134

Proposition 11. Soit X une variable aléatoire de densité f.

(i) Pour tout $a, b \in \mathbb{R}$ tels que $a \leq b$,

$$\begin{aligned}\mathbb{P}(a \leq X \leq b) &= \mathbb{P}(a \leq X < b)\\ &= \mathbb{P}(a < X \leq b)\\ &= \mathbb{P}(a < X < b)\\ &= \int_{[a,b]} f \,\mathrm{d}\lambda\end{aligned}$$

(ii) Pour tout $a \in \mathbb{R}$,

$$\mathbb{P}(a \leq X) = \mathbb{P}(a < X) = \int_{[a,+\infty[} f \,\mathrm{d}\lambda = \int_{]a,+\infty[} f \,\mathrm{d}\lambda$$

et

$$\mathbb{P}(a \geq X) = \mathbb{P}(a > X) = \int_{]-\infty,a]} f \,\mathrm{d}\lambda = \int_{]-\infty,a[} f \,\mathrm{d}\lambda$$

(iii)

$$\int_{\mathbb{R}} f \,\mathrm{d}\lambda = 1$$

Exemple 12. Soit $X : \Omega \to \mathbb{R}$ une variable aléatoire réelle. Voici quelques exemples de lois à densité classiques.

p. 141

— X suit une loi uniforme sur un compact K de $\mathbb{R}$ si elle admet la densité

$$x \mapsto \frac{1}{\lambda(K)} \mathbb{1}_K(x)$$

— X suit une loi gaussienne de paramètres $m \in \mathbb{R}$ et $\sigma^2 > 0$, notée $\mathscr{N}(m, \sigma^2)$ si elle admet la densité

$$x \mapsto \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-m)^2}{2\sigma^2}}$$

— X suit une loi exponentielle de paramètre $a > 0$, notée $\mathscr{E}(a)$ si elle admet la densité

$$x \mapsto a e^{-ax} \mathbb{1}_{\mathbb{R}^+}(x)$$

— X suit une loi Gamma de paramètres $a, \gamma > 0$, notée $\Gamma(a,\gamma)$ si elle admet la densité

$$x \mapsto \frac{\gamma^a}{\Gamma(a)} x^{a-1} e^{-\gamma x} \mathbb{1}_{\mathbb{R}_*^+}(x)$$

où $\Gamma(a)$ est la valeur au point a de la fonction Γ d'Euler.

Théorème 13. Soient X et Y deux variables aléatoires réelles indépendantes de densités respectives f et g. Alors, $X+Y$ admet comme densité la fonction $f*g : x \mapsto \int_{\mathbb{R}} f(x-t)g(t)\,\mathrm{d}t$.

p. 179

2. Espérance

Définition 14. — On note $\mathscr{L}_1(\Omega,\mathscr{A},\mathbb{P})$ (ou simplement $\mathscr{L}_1(\Omega)$ voire $\mathscr{L}_1$ s'il n'y a pas d'ambiguïté) l'espace des variables aléatoires intégrables sur $(\Omega,\mathscr{A},\mathbb{P})$.

— Si $X \in \mathscr{L}_1$, on peut définir son **espérance**

$$\mathbb{E}(X) = \int_\Omega X(\omega)\,\mathrm{d}\mathbb{P}(\omega)$$

p. 159

Théorème 15 (Transfert)**.** Si X est une variable aléatoire dont la loi $\mathbb{P}_X$ admet une densité f par rapport à $\mathbb{P}$ et si g est une fonction mesurable, alors

$$g(X) \in \mathscr{L}_1 \iff \int_{\mathbb{R}} |g(x)| f(x)\,\mathrm{d}\mathbb{P}(x) < +\infty$$

et dans ce cas,

$$\mathbb{E}(g(X)) = \int_{\mathbb{R}} g(x) f(x)\,\mathrm{d}\mathbb{P}(x)$$

p. 164

Corollaire 16. Soit g une fonction mesurable. Si X est une variable aléatoire discrète telle que $X(\Omega) = D$, alors

$$g(X) \in \mathscr{L}_1 \iff \sum_{i\in D} |g(i)| \mathbb{P}(X=i) < +\infty$$

et dans ce cas,

$$\mathbb{E}(g(X)) = \sum_{i\in D} g(i)\mathbb{P}(X=i)$$

Remarque 17. En reprenant les notations précédentes, et avec $g : x \mapsto x$, on a

$$X \in \mathscr{L}_1 \iff \sum_{i\in D} |i| \mathbb{P}(X=i) < +\infty$$

et dans ce cas,

$$\mathbb{E}(X) = \sum_{i \in D} i\mathbb{P}(X = i)$$

Corollaire 18. Soit g une fonction mesurable. Si X est une variable aléatoire admettant f comme densité, alors

$$g(X) \in \mathscr{L}_1 \iff \int_{\mathbb{R}} |g| f \, \mathrm{d}\lambda < +\infty$$

et dans ce cas,

$$\mathbb{E}(g(X)) = \int_{\mathbb{R}} |g| f \, \mathrm{d}\lambda$$

Remarque 19. En reprenant les notations précédentes, et avec $g : x \mapsto x$, on a

$$X \in \mathscr{L}_1 \iff \int_{\mathbb{R}} |x| f(x) \, \mathrm{d}x < +\infty$$

et dans ce cas,

$$\mathbb{E}(X) = \int_{\mathbb{R}} |x| f(x) \, \mathrm{d}x$$

Exemple 20. Soit $X : \Omega \to \mathbb{R}$ une variable aléatoire réelle. p. 187

- $\mathbb{E}(\mathbb{1}_A) = \mathbb{P}(A)$.
- $X \sim \mathscr{B}(n,p) \implies \mathbb{E}(X) = np$.
- $X \sim \mathscr{G}(p) \implies \mathbb{E}(X) = \frac{1}{p}$.
- $X \sim \mathscr{P}(\lambda) \implies \mathbb{E}(X) = \lambda$.

3. Indépendance

Définition 21. Soient $(E, \mathscr{F})$ un espace probabilisable. On dit que deux variables aléatoires $X : \Omega \to E$ et $Y : \Omega \to E$ sont indépendantes si les tribus qu'elles engendrent sont indépendantes ie. p. 126

$$\forall A, B \in \mathscr{F}, \mathbb{P}(\{X \in A\} \cap \{X \in B\}) = \mathbb{P}_X(A)\mathbb{P}_X(B)$$

Proposition 22. Si X et Y sont deux variables aléatoires indépendantes, alors $f(X)$ et $g(Y)$ sont indépendantes pour toutes fonctions mesurables f et g.

Théorème 23. Soient X et Y deux variables aléatoires. Alors, X et Y sont indépendantes si et seulement si $\mathbb{P}_{(X,Y)} = \mathbb{P}_X \otimes \mathbb{P}_Y$.

Corollaire 24. Soient X et Y deux variables aléatoires indépendantes. Alors, $\mathbb{P}_{X+Y} = \mathbb{P}_X * \mathbb{P}_Y$.

II - Caractérisation de la loi par des fonctions

Soit $X : \Omega \to \mathbb{R}^d$.

1. Fonctions de répartition

Définition 25. On appelle **fonction de répartition** de X, notée F_X la fonction définie sur $\mathbb{R}^d$ par

$$\forall (t_1, \dots, t_d) \in \mathbb{R}^d,\ F_X(t_1, \dots, t_d) = \mathbb{P}(X_1 \leq t_1, \dots, X_d)$$

où l'on a noté $X = (X_1, \dots, X_d)$.

p. 118

Exemple 26. Si $X \sim \mathcal{E}(\lambda)$, alors

$$\forall t \in \mathbb{R},\ F_X(t) = 1 - e^{\lambda t} \mathbb{1}_{\mathbb{R}^+}(t)$$

p. 143

Théorème 27. Si deux variables (ou vecteurs) aléatoires ont la même fonction de répartition, alors elles ont même loi.

p. 118

Théorème 28.
(i) F_X est à valeurs dans $[0, 1]$.
(ii) F_X est croissante sur $\mathbb{R}$.
(iii) $\lim_{t \to -\infty} F_X(t) = 0$ et $\lim_{t \to +\infty} F_X(t) = 1$.
(iv) En tout point x de $\mathbb{R}$, F_X est continue à droite et admet une limite à gauche, qui vaut $F_X(x)$ si et seulement si $\mathbb{P}(X = x) = 0$.
(v) L'ensemble des points de discontinuité de F est fini ou dénombrable.

Théorème 29. Soit $F : \mathbb{R} \to \mathbb{R}$ croissante, continue à droite et telle que $\lim_{t \to -\infty} F(t) = 0$ et $\lim_{t \to +\infty} F(t) = 1$. Alors, il existe une mesure de probabilité sur $\mathbb{R}$ dont F est la fonction de répartition.

2. Fonctions caractéristiques

Définition 30. On appelle **fonction caractéristique** de X la fonction ϕ_X définie sur $\mathbb{R}^d$ par

$$\phi_X : t \mapsto \mathbb{E}\left(e^{i\langle t,X\rangle}\right)$$

p. 239

Exemple 31. Si $X \sim \mathcal{N}(0,\sigma^2)$, alors

$$\forall t \in \mathbb{R},\ \phi_X(t) = e^{-\frac{(xt)^2}{2}}$$

[AMR08] p. 156

Théorème 32. Si deux variables (ou vecteurs) aléatoires ont la même fonction caractéristique, alors elles ont même loi.

[G-K] p. 239

Théorème 33. (i) $\phi_X(0) = 1$.

(ii) $|\phi_X| \leq 1$.

(iii) ϕ est uniformément continue sur $\mathbb{R}^d$.

Théorème 34. Soient X et Y deux variables aléatoires indépendantes et $\mathscr{L}_1$. Alors,

$$\mathbb{E}(XY) = \mathbb{E}(X)\mathbb{E}(Y)$$

Corollaire 35. Si deux variables aléatoires réelles X et Y sont indépendantes, alors $\phi_{X+Y} = \phi_X\phi_Y$.

Théorème 36. Si X admet un moment d'ordre N (ie. $\mathbb{E}(\|X\|^N)) < +\infty$), alors ϕ_X est $\mathscr{C}^N$ et, si $d = 1$,

$$\forall k \in [\![1,N]\!],\ \phi_X^{(k)}(0) = i^k\mathbb{E}(X^k)$$

Exemple 37. Si X admet un moment d'ordre 2 et est centrée avec une variance σ^2, on a alors

$$\phi_X(t) = 1 - \frac{\sigma^2 t^2}{2} + o(t^2)$$

quand t tend vers 0.

3. Fonctions génératrices

On suppose dans cette sous-section que X est à valeurs dans $(\mathbb{N}, \mathscr{P}(\mathbb{N}))$.

Définition 38. On appelle **fonction génératrice** de X la fonction

$$G_X : \begin{array}{ccc} [-1,1] & \to & \mathbb{R} \\ z & \mapsto & \sum_{k=0}^{+\infty} \mathbb{P}(X=k) z^k \end{array}$$

p. 235

Remarque 39.

$$\forall t \in \mathbb{R}, \phi_X(t) = G_X(e^{it})$$

p. 246

Exemple 40.
- $X \sim \mathscr{B}(p) \implies \forall s \in [-1,1], G_X(s) = (1-p) + ps$.
- $X \sim \mathscr{B}(n,p) \implies \forall s \in [-1,1], G_X(s) = ((1-p)+ps)^n$.
- $X \sim \mathscr{G}(p) \implies \forall s \in [-1,1], G_X(s) = \frac{ps}{1-(1-p)s}$.
- $X \sim \mathscr{P}(\lambda) \implies \forall s \in [-1,1], G_X(s) = e^{-\lambda(1-s)}$.

p. 236

Proposition 41. Soient X_1 et X_2 deux variables aléatoires indépendantes et à valeurs dans $\mathbb{N}$. Alors,

$$G_{X_1 X_2} = G_{X_1} + G_{X_2}$$

Théorème 42. Sur $[0,1]$, la fonction G_X est infiniment dérivable et ses dérivées sont toutes positives, avec

$$G_X^{(n)}(s) = \mathbb{E}(X(X-1)\dots(X-n+1)s^{X-n})$$

En particulier,

$$\mathbb{P}(X=n) = \frac{G_X^{(n)}(0)}{n!}$$

ce qui montre que la fonction génératrice caractérise la loi.

Exemple 43. Si $X_1 \sim \mathscr{B}(n,p)$ et $X_2 \sim \mathscr{B}(m,p)$ sont indépendantes, alors $X_1 + X_2 \sim \mathscr{B}(n+m,p)$.

[GOU21] p. 346

Théorème 44. $X \in \mathscr{L}_1$ si et seulement si G_X admet une dérivée à gauche en 1. Dans ce cas, $G_X'(1) = \mathbb{E}(X)$. [G-K] p. 238

III - Convergence en loi

Soit (X_n) une suite de vecteurs aléatoires à valeurs dans $(\mathbb{R}^d, \mathscr{B}(\mathbb{R}^d))$.

1. Définition et premières propriétés

Définition 45. On dit que (X_n) **converge en loi** vers $X : \Omega \to \mathbb{R}^d$ si p. 295

$$\forall f \in \mathscr{C}_b(\mathbb{R}^d, \mathbb{R}),\ \mathbb{E}(f(X_n)) \longrightarrow_{n\to+\infty} \mathbb{E}(f(X))$$

On note cela $X_n \xrightarrow{(d)} X$.

Exemple 46. Si $\forall n \geq 1$, X_n suit une loi uniforme sur $[\![1, n-1]\!]$, alors $\frac{X_n}{n}$ converge en loi vers la loi uniforme sur $[0,1]$. p. 313

Proposition 47. Si $X_n \xrightarrow{(d)} X$ et $Y_n \xrightarrow{(d)} Y$, alors : p. 295

(i) La limite X est unique.

(ii) $\langle X_n, Y_n \rangle \xrightarrow{(d)} \langle X, Y \rangle$.

Plus généralement, si $\forall n \in \mathbb{N}$, X_n et X sont à valeurs dans E, alors $f(X_n) \xrightarrow{(d)} f(X)$ pour toute f fonction définie et continue sur E.

Théorème 48 (Lemme de Scheffé)**.** On suppose :

— $X_n \xrightarrow{(ps.)} X$.

— $\lim_{n\to+\infty} \int_\Omega X_n \, \mathrm{d}\mathbb{P} = \int_\Omega X \, \mathrm{d}\mathbb{P}$.

Alors, $X_n \xrightarrow{(L_1)} X$.

Corollaire 49. On suppose :

— $\forall n \in \mathbb{N}$, X_n admet une densité f_n.

— (f_n) converge presque partout vers une fonction f.

— Il existe une variable aléatoire X admettant f pour densité.

Alors, $X_n \xrightarrow{(d)} X$.

Corollaire 50. Si X et X_n sont des variables aléatoires à valeurs dans un ensemble dénombrable D pour tout $n \in \mathbb{N}$, en supposant

$$\forall k \in D, \mathbb{P}(X_n = k) = \mathbb{P}(X = k)$$

alors $X_n \xrightarrow{(d)} X$.

Application 51. Soit, pour $n \geq 1$, une variable aléatoire X_n suivant la loi binomiale de paramètres n et p_n. On suppose que $\lim_{n\to+\infty} np_n = \lambda > 0$.Alors,

$$X_n \xrightarrow{(d)} X$$

où X suit une loi de Poisson de paramètre λ.

Théorème 52. En notant F_X la fonction de répartition d'une variable aléatoire X, on a,

$$X_n \xrightarrow{(d)} X \iff F_{X_n}(x) \longrightarrow_{n\to+\infty} F_X(x)$$

en tout point x où F_X est continue.

p. 302

Théorème 53. Soit $X : \Omega \to \mathbb{R}^d$ une variable aléatoire.

(i) Si (X_n) converge en probabilité vers X, alors (X_n) converge en loi vers X.

(ii) Si (X_n) converge en loi vers une constante a (ou de manière équivalente, vers une masse de Dirac δ_a), alors (X_n) converge en probabilité vers a.

Contre-exemple 54. Si (X_n) est une suite de variables aléatoires indépendantes identiquement distribuées de loi $\mathscr{B}(p)$, alors (X_n) converge en loi vers $\mathscr{B}(2p(1-p))$, mais pas en probabilité.

[HAU] p. 362

2. Théorème central limite et applications

Théorème 55 (Slutsky)**.** Si $X_n \xrightarrow{(d)} X$ et $Y_n \xrightarrow{(d)} c$ où c est un vecteur constant, alors :

(i) $X_n + Y_n \xrightarrow{(d)} X + c$.

(ii) $\langle X_n, Y_n \rangle \xrightarrow{(d)} \langle X, c \rangle$.

[G-K] p. 305

Théorème 56 (Lévy)**.** On suppose que (X_n) est une suite de variables aléatoires réelles et X

[Z-Q] p. 544

une variable aléatoire réelle. Alors :

$$X_n \xrightarrow{(d)} X \iff \phi_{X_n} \text{ converge simplement vers } \phi_X$$

[DEV]

Théorème 57 (Central limite)**.** On suppose que (X_n) est une suite de variables aléatoires réelles indépendantes de même loi admettant un moment d'ordre 2. On note m l'espérance et σ^2 la variance commune à ces variables. On pose $S_n = X_1 + \cdots + X_n - nm$. Alors,

$$\left(\frac{S_n}{\sqrt{n}}\right) \xrightarrow{(d)} \mathcal{N}(0, \sigma^2)$$

[G-K] p. 307

Application 58 (Théorème de Moivre-Laplace)**.** On suppose que (X_n) est une suite de variables aléatoires indépendantes de même loi $\mathcal{B}(p)$. Alors,

$$\frac{\sum_{k=1}^{n} X_k - np}{\sqrt{n}} \xrightarrow{(d)} \mathcal{N}(0, p(1-p))$$

Lemme 59. Soient X et Y deux variables aléatoires indépendantes telles que $X \sim \Gamma(a, \gamma)$ et $Y \sim \Gamma(b, \gamma)$. Alors $Z = X + Y \sim \Gamma(a+b, \gamma)$.

p. 180

Application 60 (Formule de Stirling)**.**

$$n! \sim \sqrt{2n\pi}\left(\frac{n}{e}\right)^n$$

p. 556

[DEV]

Application 61 (Théorème des événements rares de Poisson)**.** Soit $(N_n)_{n\geq 1}$ une suite d'entiers tendant vers l'infini. On suppose que pour tout n, $A_{n,N_1}, \ldots, A_{n,N_n}$ sont des événements indépendants avec $\mathbb{P}(A_{n,N_k}) = p_{n,k}$. On suppose également que :

(i) $\lim_{n\to+\infty} s_n = \lambda > 0$ où $\forall n \in \mathbb{N}, s_n = \sum_{k=1}^{N_n} p_{n,k}$.

(ii) $\lim_{n\to+\infty} \sup_{k\in[\![1,N_n]\!]} p_{n,k} = 0$.

Alors, la suite de variables aléatoires (S_n) définie par

$$\forall n \in \mathbb{N}^*, S_n = \sum_{k=1}^{n} \mathbb{1}_{A_{n,k}}$$

converge en loi vers la loi de Poisson de paramètre λ.

p. 390

262 Convergences d'une suite de variables aléatoires. Théorèmes limite. Exemples et applications.

Soient $(\Omega, \mathcal{A}, \mathbb{P})$ un espace probabilisé et (X_n) une suite de vecteurs aléatoires à valeurs dans $(\mathbb{R}^d, \mathcal{B}(\mathbb{R}^d))$.

I - Premiers modes de convergence

1. Convergence presque sûre

Définition 1. On dit que (X_n) **converge presque sûrement** vers $X : \Omega \to \mathbb{R}^d$ si

$$\mathbb{P}(\{\omega \in \Omega \mid X_n(\omega) \longrightarrow_{n\to+\infty} X(\omega)\}) = 1$$

On note cela $X_n \overset{(ps.)}{\longrightarrow} X$.

[G-K] p. 265

Remarque 2. La convergence presque sûre d'une suite de vecteurs aléatoires équivaut à la convergence presque sûre de chacune des composantes. Pour cette raison, on peut se limiter à l'étude du cas $d = 1$.

Exemple 3. Si (X_n) est telle que $\forall n \geq 1, \mathbb{P}(X_n = \pm\sqrt{n}) = \frac{1}{2}$, alors $\frac{1}{n^2}\sum_{k=1}^{n} X_k^2 \overset{(ps.)}{\longrightarrow} 0$.

p. 285

Proposition 4. Si $X_n \overset{(ps.)}{\longrightarrow} X$ et $Y_n \overset{(ps.)}{\longrightarrow} Y$, alors :

(i) $\forall a \in \mathbb{R}, aX_n \overset{(ps.)}{\longrightarrow} aX$.

(ii) $X_n + Y_n \overset{(ps.)}{\longrightarrow} X + Y$.

(iii) $X_n Y_n \overset{(ps.)}{\longrightarrow} XY$.

Plus généralement, si $\forall n \in \mathbb{N}$, X_n et X sont à valeurs dans E, alors $f(X_n) \overset{(ps.)}{\longrightarrow} f(X)$ pour toute f fonction définie et continue sur E.

p. 265

Théorème 5 (1^{er} lemme de Borel-Cantelli)**.** Soit (A_n) une suite d'événements. Si $\sum \mathbb{P}(A_n)$ converge, alors

$$\mathbb{P}\left(\limsup_{n\to+\infty} A_n\right) = 0$$

p. 272

Remarque 6. Cela signifie que presque sûrement, seul un nombre fini d'événements A_n se réalisent.

Corollaire 7. Si $\sum \mathbb{P}(|X_n - X| > \epsilon)$ converge pour tout $\epsilon > 0$, alors $X_n \xrightarrow{(ps.)} X$.

Exemple 8. Si (X_n) est telle que $\forall n \geq 1, \mathbb{P}(X_n = n) = \mathbb{P}(X_n = \pm n) = \frac{1}{2n^2}$ et $\mathbb{P}(X_n = 0) = 1 - \frac{1}{2n^2}$, alors la suite (S_n) définie pour tout $n \geq 1$ par $S_n = \sum_{k=1}^{n} X_k$ est constante à partir d'un certain rang. p. 285

Théorème 9 (2^e lemme de Borel-Cantelli)**.** Soit (A_n) une suite d'événements indépendants. Si $\sum \mathbb{P}(A_n)$ diverge, alors p. 273

$$\mathbb{P}\left(\limsup_{n\to+\infty} A_n\right) = 1$$

Remarque 10. Cela signifie que presque sûrement, un nombre infini d'événements A_n se réalisent.

Exemple 11. On fait une infinité de lancers d'une pièce de monnaie équilibrée. Alors, la probabilité de l'événement "on obtient une infinité de fois deux "Face" consécutifs" est 1. p. 286

Corollaire 12 (Loi du 0-1 de Borel)**.** Soit (A_n) une suite d'événements indépendants, alors

$$\mathbb{P}\left(\limsup_{n\to+\infty} A_n\right) = 0 \text{ ou } 1$$

et elle vaut 1 si et seulement si $\sum \mathbb{P}(A_n)$ diverge.

2. Convergence en probabilité

Définition 13. On dit que (X_n) **converge en probabilité** vers $X : \Omega \to \mathbb{R}^d$ si p. 268

$$\forall \epsilon, \mathbb{P}(|X_n - X| \geq \epsilon) = 0$$

On note cela $X_n \xrightarrow{(p)} X$.

Exemple 14. On suppose que (X_n) est une suite de variables aléatoires indépendantes identiquement distribuées telle que $\mathbb{P}(X_1 = 1) = p$ et $\mathbb{P}(X_1 = 0) = 1 - p$. On définit la suite (Y_n) par p. 285

$$\forall n \geq 1, Y_n = \begin{cases} 0 \text{ si } X_k = X_{k+1} \\ 1 \text{ sinon} \end{cases}$$

et la suite (S_n) par $\forall n \geq 1, M_n = \frac{Y_1 + \cdots + Y_n}{n}$. On a $M_n - 2p(1-p) \xrightarrow{(p)} 0$.

Proposition 15. Si $X_n \xrightarrow{(p)} X$ et $Y_n \xrightarrow{(p)} Y$, alors :
(i) $(X_n, Y_n) \xrightarrow{(p)} (X, Y)$.
(ii) $X_n + Y_n \xrightarrow{(p)} X + Y$.

p. 268

Théorème 16. La convergence presque sûre implique la convergence en probabilité.

Contre-exemple 17. La suite $(M_n - 2p(1-p))$ de l'Théorème 14 ne converge pas vers 0 presque sûrement.

p. 285

Théorème 18. Si $X_n \xrightarrow{(p)} X$, alors il existe une sous-suite (X_{n_k}) de (X_n) telle que $X_{n_k} \xrightarrow{(ps.)} X$.

p. 274

Corollaire 19. On suppose $X_n \xrightarrow{(p)} X$. Si $\forall n \in \mathbb{N}$, X_n et X sont à valeurs dans E, alors $f(X_n) \xrightarrow{(p)} f(X)$ pour toute f fonction définie et continue sur E.

3. Lois des grands nombres

Théorème 20 (Loi faible des grands nombres)**.** Soit (X_n) une suite de variables aléatoires deux à deux indépendantes de même loi et $\mathscr{L}_1$. On pose $M_n = \frac{X_1+\cdots+X_n}{n}$. Alors,

$$M_n \xrightarrow{(p)} \mathbb{E}(X_1)$$

p. 270

Théorème 21 (Loi forte des grands nombres)**.** Soit (X_n) une suite de variables aléatoires mutuellement indépendantes de même loi. On pose $M_n = \frac{X_1+\cdots+X_n}{n}$. Alors,

$$X_1 \in \mathscr{L}_1 \iff M_n \xrightarrow{(ps.)} \ell \in \mathbb{R}$$

Dans ce cas, on a $\ell = \mathbb{E}(X_1)$.

[Z-Q] p. 532

Application 22 (Théorème de Bernstein)**.** Soit $f : [0,1] \to \mathbb{R}$ continue. On note

$$\forall n \in \mathbb{N}^*, B_n(f) : x \mapsto \sum_{k=0}^{n} \binom{n}{k} f\left(\frac{k}{n}\right) x^k (1-x)^{n-k}$$

le n-ième polynôme de Bernstein associé à f. Alors le suite de fonctions $(B_n(f))$ converge uniformément vers f.

[G-K] p. 195

Corollaire 23 (Théorème de Weierstrass)**.** Toute fonction continue $f : [a,b] \to \mathbb{R}$ (avec $a, b \in \mathbb{R}$ tels que $a \leq b$) est limite uniforme de fonctions polynômiales sur $[a,b]$.

II - Convergence L_p

Définition 24. On dit que (X_n) **converge dans** L_p vers $X : \Omega \to \mathbb{R}^d$ si

$$\forall n \in \mathbb{N}, X_n \in L_p, X \in L_p \text{ et } \mathbb{E}(|X_n - X|^p)$$

On note cela $X_n \xrightarrow{(L_p)} X$.

p. 268

Proposition 25. Comme les espaces sont de mesure finie,

$$p \geq q \implies L_p(\Omega, \mathscr{A}, \mathbb{P}) \subseteq L_q(\Omega, \mathscr{A}, \mathbb{P})$$

[D-L] p. 510

Corollaire 26. Pour $1 \leq p \leq q$, la convergence dans L_q implique la convergence dans L_p qui implique elle-même la convergence dans L_1.

Contre-exemple 27. Si,

$$\forall n \in \mathbb{N}, \forall \omega \in \Omega, X_n(\omega) = \sqrt{n}\mathbb{1}_{\left[0, \frac{1}{n}\right]}$$

alors, (X_n) converge dans L_1 mais pas dans L_2.

[HAU] p. 365

Théorème 28 (Convergence dominée)**.** Si $X_n \xrightarrow{(ps.)} X$ et $\exists g \in L_1$ telle que $\|X_n\|_1 \leq g$, alors $X_n \xrightarrow{(L_1)} X$.

[G-K] p. 65

Contre-exemple 29. On se place dans le cas où $(\Omega, \mathscr{A}, \mathbb{P}) = ([0,1[, \mathscr{B}([0,1[), \lambda_{[0,1[})$. Si $\forall n \geq 1$, $X_n = n\mathbb{1}_{\left]0, \frac{1}{n}\right[}$, alors (X_n) converge vers 0 presque sûrement, mais pas dans L_1.

[HAU] p. 365

Proposition 30. Si $X_n \xrightarrow{(L_p)} X$, alors il existe une sous-suite (X_{n_k}) de (X_n) telle que $X_{n_k} \xrightarrow{(ps.)} X$.

[G-K] p. 265

Théorème 31. La convergence dans L_p (pour $p \geq 1$) implique la convergence en probabilité.

Exemple 32. La convergence en probabilité de l'Théorème 14 est en fait une convergence dans L_2.

Contre-exemple 33. Soit X une variable aléatoire de densité $f : x \mapsto e^{-x}\mathbb{1}_{\mathbb{R}^+}$. On pose $\forall n \geq 1$, $Y_n = X\mathbb{1}_{[0,n[}(X) + e^{2n}\mathbb{1}_{[n,+\infty[}(X)$. Alors (Y_n) converge vers X en probabilité, mais pas dans L_1. p. 281

III - Convergence en loi

1. Définition et premières propriétés

Définition 34. On dit que (X_n) **converge en loi** vers $X : \Omega \to \mathbb{R}^d$ si

$$\forall f \in \mathscr{C}_b(\mathbb{R}^d, \mathbb{R}),\ \mathbb{E}(f(X_n)) \longrightarrow_{n\to+\infty} \mathbb{E}(f(X))$$

On note cela $X_n \xrightarrow{(d)} X$. p. 295

Exemple 35. Si $\forall n \geq 1$, X_n suit une loi uniforme sur $[\![1, n-1]\!]$, alors $\frac{X_n}{n}$ converge en loi vers la loi uniforme sur $[0,1]$. p. 313

Proposition 36. Si $X_n \xrightarrow{(d)} X$ et $Y_n \xrightarrow{(d)} Y$, alors : p. 295

(i) La limite X est unique.

(ii) $\langle X_n, Y_n\rangle \xrightarrow{(d)} \langle X, Y\rangle$.

Plus généralement, si $\forall n \in \mathbb{N}$, X_n et X sont à valeurs dans E, alors $f(X_n) \xrightarrow{(d)} f(X)$ pour toute f fonction définie et continue sur E.

Théorème 37 (Lemme de Scheffé)**.** On suppose :

— $X_n \xrightarrow{(ps.)} X$.

— $\lim_{n\to+\infty} \int_\Omega X_n \, \mathrm{d}\mathbb{P} = \int_\Omega X \, \mathrm{d}\mathbb{P}$.

Alors, $X_n \xrightarrow{(L_1)} X$.

Corollaire 38. On suppose :

— $\forall n \in \mathbb{N}$, X_n admet une densité f_n.

— (f_n) converge presque partout vers une fonction f.

— Il existe une variable aléatoire X admettant f pour densité.

Alors, $X_n \xrightarrow{(d)} X$.

Corollaire 39. Si X et X_n sont des variables aléatoires à valeurs dans un ensemble dénombrable D pour tout $n \in \mathbb{N}$, en supposant

$$\forall k \in D, \mathbb{P}(X_n = k) = \mathbb{P}(X = k)$$

alors $X_n \xrightarrow{(d)} X$.

Application 40. Soit, pour $n \geq 1$, une variable aléatoire X_n suivant la loi binomiale de paramètres n et p_n. On suppose que $\lim_{n\to+\infty} np_n = \lambda > 0$.Alors,

$$X_n \xrightarrow{(d)} X$$

où X suit une loi de Poisson de paramètre λ.

Théorème 41. En notant F_X la fonction de répartition d'une variable aléatoire X, on a,

$$X_n \xrightarrow{(d)} X \iff F_{X_n}(x) \longrightarrow_{n\to+\infty} F_X(x)$$

en tout point x où F_X est continue.

p. 302

Théorème 42. Soit $X : \Omega \to \mathbb{R}^d$ une variable aléatoire.

(i) Si (X_n) converge en probabilité vers X, alors (X_n) converge en loi vers X.

(ii) Si (X_n) converge en loi vers une constante a (ou de manière équivalente, vers une masse de Dirac δ_a), alors (X_n) converge en probabilité vers a.

Contre-exemple 43. Si (X_n) est une suite de variables aléatoires indépendantes identiquement distribuées de loi $\mathscr{B}(p)$, alors (X_n) converge en loi vers $\mathscr{B}(2p(1-p))$, mais pas en probabilité.

[HAU] p. 362

2. Théorème central limite et applications

Théorème 44 (Slutsky)**.** Si $X_n \xrightarrow{(d)} X$ et $Y_n \xrightarrow{(d)} c$ où c est un vecteur constant, alors :

(i) $X_n + Y_n \xrightarrow{(d)} X + c$.

(ii) $\langle X_n, Y_n \rangle \xrightarrow{(d)} \langle X, c \rangle$.

[G-K] p. 305

Notation 45. Si X est une variable aléatoire réelle, on note ϕ_X sa fonction caractéristique.

Théorème 46 (Lévy)**.** On suppose que (X_n) est une suite de variables aléatoires réelles et X une variable aléatoire réelle. Alors :

$$X_n \xrightarrow{(d)} X \iff \phi_{X_n} \text{ converge simplement vers } \phi_X$$

[Z-Q] p. 544

[DEV]

Théorème 47 (Central limite)**.** On suppose que (X_n) est une suite de variables aléatoires réelles indépendantes de même loi admettant un moment d'ordre 2. On note m l'espérance et σ^2 la variance commune à ces variables. On pose $S_n = X_1 + \cdots + X_n - nm$. Alors,

$$\left(\frac{S_n}{\sqrt{n}}\right) \xrightarrow{(d)} \mathcal{N}(0,\sigma^2)$$

[G-K] p. 307

Application 48 (Théorème de Moivre-Laplace)**.** On suppose que (X_n) est une suite de variables aléatoires indépendantes de même loi $\mathcal{B}(p)$. Alors,

$$\frac{\sum_{k=1}^n X_k - np}{\sqrt{n}} \xrightarrow{(d)} \mathcal{N}(0, p(1-p))$$

Lemme 49. Soient X et Y deux variables aléatoires indépendantes telles que $X \sim \Gamma(a,\gamma)$ et $Y \sim \Gamma(b,\gamma)$. Alors $Z = X + Y \sim \Gamma(a+b,\gamma)$.

p. 180

Application 50 (Formule de Stirling)**.**

$$n! \sim \sqrt{2n\pi}\left(\frac{n}{e}\right)^n$$

p. 556

[DEV]

Application 51 (Théorème des événements rares de Poisson)**.** Soit $(N_n)_{n\geq 1}$ une suite d'entiers tendant vers l'infini. On suppose que pour tout n, $A_{n,N_1}, \dots, A_{n,N_n}$ sont des événements indépendants avec $\mathbb{P}(A_{n,N_k}) = p_{n,k}$. On suppose également que :

(i) $\lim_{n\to+\infty} s_n = \lambda > 0$ où $\forall n \in \mathbb{N}, s_n = \sum_{k=1}^{N_n} p_{n,k}$.

(ii) $\lim_{n\to+\infty} \sup_{k\in[\![1,N_n]\!]} p_{n,k} = 0$.

Alors, la suite de variables aléatoires (S_n) définie par

$$\forall n \in \mathbb{N}^*, S_n = \sum_{k=1}^{n} \mathbb{1}_{A_{n,k}}$$

converge en loi vers la loi de Poisson de paramètre λ.

p. 390

Annexes

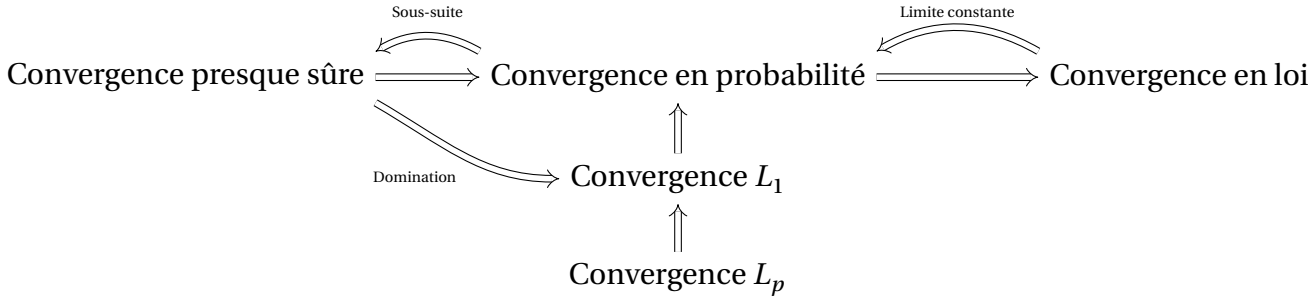


FIGURE I.30 – Liens entre les différents modes de convergence.

264 Variables aléatoires discrètes. Exemples et applications.

Soient $(\Omega, \mathscr{A}, \mathbb{P})$ un espace probabilisé et $X : \Omega \to \mathbb{R}$ une variable aléatoire réelle. On munit $\mathbb{R}$ de sa tribu borélienne $\mathscr{B}(\mathbb{R})$.

I - Généralités

1. Définitions

Définition 1. — On dit qu'une loi μ est **discrète** s'il existe un ensemble D fini tel que $\mu(D) = 1$.
— On dit que la variable aléatoire X est discrète si sa loi $\mathbb{P}_X$ est discrète.

[G-K] p. 335

Remarque 2. Cela revient à dire que $X(\Omega)$ est fini ou est dénombrable.

[GOU21] p. 335

Exemple 3. On pose $\Omega = \{(\omega_n) \in \mathbb{R}^n \mid \omega_n \in \{0,1\}\, \forall n \in \mathbb{N}\}$ et $X : (\omega_n) \mapsto \inf\{n \in \mathbb{N} \mid \omega_n = 0\}$. Alors X est une variable aléatoire discrète, à valeurs dans $\mathbb{N} \cup \{+\infty\}$.

Proposition 4. Si X est une variable aléatoire discrète à valeurs dans un ensemble dénombrable D, alors :
(i) $\forall A \in \mathscr{B}(\mathbb{R}), \mathbb{P}_X(A) = \sum_{i \in D \cap A} \mathbb{P}(X = i)$.
(ii) $\mathbb{P}_X = \sum_{i \in D} \mathbb{P}(X = i)\delta_i$ où les δ_i sont des masses de Dirac (voir Théorème 7).

[G-K] p. 131

Remarque 5. Si D est un ensemble fini ou dénombrable et $(p_i)_{i \in D}$ est une famille de réels positifs de somme égale à 1, alors en posant $\Omega = D$, $\mathscr{A} = \mathscr{P}(D)$, $X : \omega \mapsto \omega$ et $\mathbb{P} = \sum_{i \in D} \mathbb{P}(X = i)\delta_i$, on a construit une variable aléatoire discrète X sur $(\Omega, \mathscr{A}, \mathbb{P})$.

2. Lois discrètes usuelles

Définition 6. Si $A \subseteq \Omega$, l'application $\mathbb{1}_A$, appelée **indicatrice** de A est définie sur Ω par

$$\mathbb{1}_A : \begin{array}{ccc} \Omega & \to & \{0;1\} \\ x & \mapsto & \begin{cases} 1 \text{ si } x \in A \\ 0 \text{ sinon} \end{cases} \end{array}$$

p. 137

Exemple 7 (Mesure de Dirac)**.** Si $x \in \Omega$, on pose $\delta_x : A \mapsto \mathbb{1}_A(x)$. C'est une loi discrète sur $\mathscr{P}(\Omega)$.

Exemple 8 (Loi uniforme)**.** Soit $E \subseteq \Omega$ fini. On appelle loi uniforme sur E la loi discrète définie sur $\mathscr{P}(\Omega)$ par

$$\begin{array}{ccc} \mathscr{P}(\Omega) & \to & [\![0,1]\!] \\ A & \mapsto & \frac{|A\cap E|}{|E|} \end{array}$$

Remarque 9. Il s'agit du nombre de cas favorables sur le nombre de cas possibles. Ainsi, X suit la loi uniforme sur E si on a $\forall x \in E, \mathbb{P}(X = x) = \frac{1}{|E|}$ et $\forall x \notin E, \mathbb{P}(X = x) = 0$.

C'est, par exemple, la loi suivie par une variable aléatoire représentant le lancer d'un dé non truqué avec $E = [\![1,6]\!]$.

Exemple 10 (Loi de Bernoulli)**.** X suit une loi de Bernoulli de paramètre $p \in [0,1]$, notée $\mathscr{B}(p)$, si $\mathbb{P}(X = 1) = p$ et $\mathbb{P}(X = 0) = 1 - p$. Dans ce cas, X est bien une loi discrète et on a

$$\mathbb{P}_X = (1-p)\delta_0 + p\delta_1$$

Exemple 11 (Loi binomiale)**.** X suit une loi de binomiale de paramètres $n \in \mathbb{N}$ et $p \in [0,1]$, notée $\mathscr{B}(n,p)$, si X est la somme de n variables aléatoires indépendantes qui suivent des lois de Bernoulli de paramètre p. Dans ce cas, X est bien une loi discrète et on a

$$\forall k \in \mathbb{N}, \mathbb{P}(X = k) = \binom{n}{k} p^k (1-p)^{n-k}$$

Remarque 12. Il s'agit du nombre de succès pour n tentatives.

C'est, par exemple, la loi suivie par une variable aléatoire représentant le nombre de "Pile" obtenus lors d'un lancer de pièce équilibrée.

Exemple 13 (Loi géométrique)**.** X suit une loi géométrique de paramètre $p \in]0,1]$, notée $\mathscr{G}(p)$, si l'on a

$$\forall k \in \mathbb{N}^*, \mathbb{P}(X = k) = p(1-p)^{k-1}$$

Remarque 14. Il s'agit d'une succession de $k-1$ échecs consécutifs suivie d'un succès.

C'est, par exemple, la loi suivie par une variable aléatoire représentant le nombre de lancers effectués avant d'obtenir "Pile" lors d'un lancer de pièce équilibrée.

Exemple 15 (Loi de Poisson)**.** X suit une loi de Poisson de paramètre $\lambda > 0$, notée $\mathscr{P}(\lambda)$, si l'on a

$$\forall k \in \mathbb{N}^*, \mathbb{P}(X = k) = e^{-\lambda}\frac{\lambda^k}{k!}$$

Remarque 16. Cette loi est une bonne modélisation pour le nombre de fois où un événement rare survient (par exemple, un tremblement de terre).

p. 298

II - Propriétés spécifiques aux variables aléatoires discrètes

1. Indépendance

Définition 17. On dit que des variables aléatoires $X_1, \dots X_n$, sont **indépendantes** si

$$\mathbb{P}_{(X_1,\dots,X_n)} = \bigotimes_{i=1}^{n} \mathbb{P}_{X_i}$$

p. 128

Exemple 18. Si X_1 et X_2 sont des variables aléatoires indépendantes suivant des lois de Poisson de paramètres respectifs λ et μ, alors $X_1 + X_2$ suit une loi de Poisson de paramètre $\lambda + \mu$.

p. 238

Contre-exemple 19. Soient X_1 et X_2 deux variables aléatoires indépendantes telles que

$$\forall i \in [\![1,2]\!], \mathbb{P}(X_i = 1) = \mathbb{P}(X_i = -1) = \frac{1}{2}$$

On pose $X_3 = X_1X_2$. Alors, X_2 et X_3 sont indépendantes, X_1 et X_3 aussi, mais X_1, X_2 et X_3 ne le sont pas.

Proposition 20. Des variables aléatoires discrètes $X_1, \dots, X_n$ sont indépendantes si et seulement si

$$\forall j \in [\![, 1, n]\!], \forall x_j \in X_j(\Omega), \mathbb{P}(X_1 = x_1, \dots, X_n = x_n) = \prod_{j=1}^{n} \mathbb{P}(X = x_i)$$

[GOU21] p. 337

Proposition 21. Soient $X_1, \dots, X_n$ des variables aléatoires discrètes définies sur $(\Omega, \mathscr{A}, \mathbb{P})$, $f : X_1(\Omega) \times \cdots \times X_m(\Omega) \to F$ et $g : X_{m+1}(\Omega) \times \cdots \times X_n(\Omega) \to F'$ deux fonctions. Si $X_1, \dots, X_n$ sont indépendantes, alors il en est de même de $f(X_1, \dots, X_m)$ et $g(X_{m+1}, \dots, X_n)$.

2. Espérance

Définition 22. — On note $\mathscr{L}_1(\Omega,\mathscr{A},\mathbb{P})$ (ou simplement $\mathscr{L}_1(\Omega)$ voire $\mathscr{L}_1$ s'il n'y a pas d'ambiguïté) l'espace des variables aléatoires intégrables sur $(\Omega,\mathscr{A},\mathbb{P})$. [G-K] p. 159

— Si $X \in \mathscr{L}_1$, on peut définir son **espérance**

$$\mathbb{E}(X) = \int_\Omega X(\omega)\,\mathrm{d}\mathbb{P}(\omega)$$

Théorème 23 (Transfert)**.** Si X est une variable aléatoire dont la loi $\mathbb{P}_X$ admet une densité f par rapport à $\mathbb{P}$ et si g est une fonction mesurable, alors p. 164

$$g(X) \in \mathscr{L}_1 \iff \int_{\mathbb{R}} |g(x)|f(x)\,\mathrm{d}\mathbb{P}(x) < +\infty$$

et dans ce cas,

$$\mathbb{E}(g(X)) = \int_{\mathbb{R}} g(x)f(x)\,\mathrm{d}\mathbb{P}(x)$$

Corollaire 24. Soit g une fonction mesurable. Si X est une variable aléatoire discrète telle que $X(\Omega) = D$, alors

$$g(X) \in \mathscr{L}_1 \iff \sum_{i\in D} |g(i)|\mathbb{P}(X=i) < +\infty$$

et dans ce cas,

$$\mathbb{E}(g(X)) = \sum_{i\in D} g(i)\mathbb{P}(X=i)$$

Remarque 25. En reprenant les notations précédentes, et avec $g : x \mapsto x$, on a

$$X \in \mathscr{L}_1 \iff \sum_{i\in D} |i|\mathbb{P}(X=i) < +\infty$$

et dans ce cas,

$$\mathbb{E}(X) = \sum_{i\in D} i\mathbb{P}(X=i)$$

Exemple 26. — $\mathbb{E}(\mathbb{1}_A) = \mathbb{P}(A)$. p. 187

— $X \sim \mathscr{B}(n,p) \implies \mathbb{E}(X) = np$.

— $X \sim \mathscr{G}(p) \implies \mathbb{E}(X) = \frac{1}{p}$.

— $X \sim \mathscr{P}(\lambda) \implies \mathbb{E}(X) = \lambda$.

Proposition 27. Si X est à valeurs dans $(\mathbb{N},\mathscr{P}(\mathbb{N}))$, alors $\mathbb{E}(X) = \sum_{k=0}^{+\infty} \mathbb{P}(X > k)$. p. 171

3. Fonctions génératrices

On suppose dans cette sous-section que X est à valeurs dans $(\mathbb{N}, \mathscr{P}(\mathbb{N}))$.

Définition 28. On appelle **fonction génératrice** de X la fonction

$$G_X : \begin{array}{ccc} [-1,1] & \to & \mathbb{R} \\ z & \mapsto & \sum_{k=0}^{+\infty} \mathbb{P}(X=k) z^k \end{array}$$

p. 235

Exemple 29.
- $X \sim \mathscr{B}(p) \implies \forall s \in [-1,1], G_X(s) = (1-p) + ps$.
- $X \sim \mathscr{B}(n,p) \implies \forall s \in [-1,1], G_X(s) = ((1-p)+ps)^n$.
- $X \sim \mathscr{G}(p) \implies \forall s \in [-1,1], G_X(s) = \frac{ps}{1-(1-p)s}$.
- $X \sim \mathscr{P}(\lambda) \implies \forall s \in [-1,1], G_X(s) = e^{-\lambda(1-s)}$.

Théorème 30. Soient X_1 et X_2 deux variables aléatoires indépendantes et $\mathscr{L}_1$. Alors,

$$\mathbb{E}(X_1 X_2) = \mathbb{E}(X_1)\mathbb{E}(X_2)$$

Corollaire 31. Soient X_1 et X_2 deux variables aléatoires indépendantes et à valeurs dans $\mathbb{N}$. Alors,

$$G_{X_1 X_2} = G_{X_1} + G_{X_2}$$

Théorème 32. Sur $[0,1]$, la fonction G_X est infiniment dérivable et ses dérivées sont toutes positives, avec

$$G_X^{(n)}(s) = \mathbb{E}(X(X-1)\dots(X-n+1)s^{X-n})$$

En particulier,

$$\mathbb{P}(X=n) = \frac{G_X^{(n)}(0)}{n!}$$

ce qui montre que la fonction génératrice caractérise la loi.

Exemple 33. Si $X_1 \sim \mathscr{B}(n,p)$ et $X_2 \sim \mathscr{B}(m,p)$ sont indépendantes, alors $X_1 + X_2 \sim \mathscr{B}(n+m,p)$.

[GOU21] p. 346

Théorème 34. $X \in \mathscr{L}_1$ si et seulement si G_X admet une dérivée à gauche en 1. Dans ce cas, $G'_X(1) = \mathbb{E}(X)$. [G-K] p. 238

III - Application en analyse réelle

Définition 35. On dit que X **admet un moment d'ordre** 2 si elle est de carré intégrable, ie. $X^2 \in \mathscr{L}_1$. On note $\mathscr{L}_1(\Omega, \mathscr{A}, \mathbb{P})$ (ou simplement $\mathscr{L}_1(\Omega)$ voire $\mathscr{L}_1$ s'il n'y a pas d'ambiguïté) l'espace des variables aléatoires de carré intégrable. p. 171

Proposition 36.

$$X_1, X_2 \in \mathscr{L}_2 \implies X_1 X_2 \in \mathscr{L}_1$$

En particulier, $X_1 \in \mathscr{L}_2 \implies X_1 \in \mathscr{L}_1$.

Définition 37. Soient X_1 et X_2 deux variables aléatoires admettant chacune un moment d'ordre 2.

— On appelle **covariance** du couple (X_1, X_2) le réel

$$\text{Covar}(X_1, X_2) = \mathbb{E}((X_1 - \mathbb{E}(X_1))(X_2 - \mathbb{E}(X_2)))$$

— On appelle **variance** de X_1 le réel positif

$$\text{Var}(X_1) = \text{Covar}(X_1, X_1) = \mathbb{E}(X_1 - \mathbb{E}(X_1))^2 = \mathbb{E}(X_1^2) - (\mathbb{E}(X_1))^2$$

Proposition 38. Si X est à valeurs dans $\mathbb{N}$, alors $X \in \mathscr{L}_2$ si et seulement si $G_X \in \mathscr{C}^2([0,1])$, et dans ce cas, [GOU21] p. 346

$$\text{Var}(X) = G''_X(1) + G'_X(1) - G'_X(1)^2$$

Exemple 39. [G-K] p. 186

— $\text{Var}(\mathbb{1}_A) = \mathbb{P}(A)$.

— $X \sim \mathscr{B}(n,p) \implies \text{Var}(X) = np(1-p)$.

— $X \sim \mathscr{G}(p) \implies \text{Var}(X) = \frac{1-p}{p^2}$.

— $X \sim \mathscr{P}(\lambda) \implies \text{Var}(X) = \lambda$.

Proposition 40 (Inégalité de Bienaymé-Tchebychev)**.** On suppose $X \in \mathscr{L}_2$. Alors, p. 177

$$\forall a > 0, \mathbb{P}(|X - \mathbb{E}(X)| \geq a) \leq \frac{\text{Var}(X)}{a^2}$$

[DEV]

Théorème 41 (Bernstein)**.** Soit $f : [0,1] \to \mathbb{R}$ continue. On note

$$\forall n \in \mathbb{N}^*, B_n(f) : x \mapsto \sum_{k=0}^{n} \binom{n}{k} f\left(\frac{k}{n}\right) x^k (1-x)^{n-k}$$

le n-ième polynôme de Bernstein associé à f. Alors le suite de fonctions $(B_n(f))$ converge uniformément vers f.

p. 195

Théorème 42 (Weierstrass)**.** Toute fonction continue $f : [a,b] \to \mathbb{R}$ (avec $a, b \in \mathbb{R}$ tels que $a \leq b$) est limite uniforme de fonctions polynômiales sur $[a,b]$.

IV - Théorèmes limites et d'approximations

1. Théorèmes limites

Théorème 43 (Lévy)**.** Soient (X_n) une suite de variables aléatoires réelles et X une variable aléatoire réelle. Alors :

$$X_n \xrightarrow{(d)} X \iff \phi_{X_n} \text{ converge simplement vers } \phi_X$$

où ϕ_Y désigne la fonction caractéristique d'une variable aléatoire réelle Y.

[Z-Q] p. 544

Théorème 44 (Central limite)**.** Soit (X_n) une suite de variables aléatoires réelles indépendantes de même loi admettant un moment d'ordre 2. On note m l'espérance et σ^2 la variance commune à ces variables. On pose $S_n = X_1 + \cdots + X_n - nm$. Alors,

$$\left(\frac{S_n}{\sqrt{n}}\right) \xrightarrow{(d)} \mathcal{N}(0, \sigma^2)$$

[G-K] p. 307

[DEV]

Application 45 (Théorème des événements rares de Poisson)**.** Soit $(N_n)_{n\geq 1}$ une suite d'entiers tendant vers l'infini. On suppose que pour tout n, $A_{n,N_1}, \ldots, A_{n,N_n}$ sont des événements indépendants avec $\mathbb{P}(A_{n,N_k}) = p_{n,k}$. On suppose également que :

(i) $\lim_{n\to+\infty} s_n = \lambda > 0$ où $\forall n \in \mathbb{N}, s_n = \sum_{k=1}^{N_n} p_{n,k}$.

(ii) $\lim_{n\to+\infty} \sup_{k\in[\![1,N_n]\!]} p_{n,k} = 0$.

Alors, la suite de variables aléatoires (S_n) définie par

$$\forall n \in \mathbb{N}^*, S_n = \sum_{k=1}^{n} \mathbb{1}_{A_{n,k}}$$

p. 390

converge en loi vers la loi de Poisson de paramètre λ.

Théorème 46 (Loi faible des grands nombres)**.** Soit (X_n) une suite de variables aléatoires deux à deux indépendantes de même loi et $\mathscr{L}_1$. On pose $M_n = \frac{X_1+\cdots+X_n}{n}$. Alors,

$$M_n \xrightarrow{(p)} \mathbb{E}(X_1)$$

p. 270

Théorème 47 (Loi forte des grands nombres)**.** Soit (X_n) une suite de variables aléatoires mutuellement indépendantes de même loi. On pose $M_n = \frac{X_1+\cdots+X_n}{n}$. Alors,

$$X_1 \in \mathscr{L}_1 \iff M_n \xrightarrow{(ps.)} \ell \in \mathbb{R}$$

Dans ce cas, on a $\ell = \mathbb{E}(X_1)$.

[Z-Q] p. 532

2. Approximation d'une loi normale

Théorème 48 (Moivre-Laplace)**.** Soit (X_n) une suite de variables aléatoires indépendantes de même loi $\mathscr{B}(p)$. Alors,

$$\frac{\sum_{k=1}^{n} X_k - np}{\sqrt{n}} \xrightarrow{(d)} \mathscr{N}(0, p(1-p))$$

[G-K] p. 308

3. Approximation d'une loi de Poisson

Théorème 49. Soit, pour $n \geq 1$, une variable aléatoire X_n suivant la loi binomiale de paramètres n et p_n. On suppose que $\lim_{n\to+\infty} np_n = \lambda > 0$.Alors,

$$X_n \xrightarrow{(d)} \mathscr{P}(\lambda)$$

p. 297

Remarque 50. En pratique, pour $n \geq 30$ et $np \leq 10$, on a une "bonne" approximation de $\mathscr{P}(\lambda)$.

Exemple 51. Si chaque seconde, il y a une probabilité $p = \frac{1}{600}$ qu'un client entre dans un magasin, le nombre de clients qui entrent sut un intervalle d'une heure suit approximativement une loi de Poisson de paramètre $\lambda = 3600p = 6$.

Pour cette raison, on appelle parfois cette loi la *loi des événements rares*.

[GOU21] p. 343

[G-K] p. 297

Application 52 (Nombre de dérangements)**.** Soit σ_n une permutation aléatoire suivant la loi uniforme sur S_n. Si on note D_n le nombre de points fixes de σ_n, on a

$$\mathbb{P}(D_n = k) = \frac{1}{k!}\frac{d_{n-k}}{(n-k)!}$$

où d_n est le nombre de permutations de S_n sans point fixe. En particulier, comme $d_n \sim \frac{1}{e}n!$, on a

$$D_n \xrightarrow{(d)} \mathscr{P}(1)$$

266 Utilisation de la notion d'indépendance en probabilités.

Soit $(\Omega, \mathscr{A}, \mathbb{P})$ un espace probabilisé.

I - Indépendance en probabilités

1. Indépendance d'événements

Définition 1. On dit que deux événements A et B sont **indépendants** (sous $\mathbb{P}$) si

$$\mathbb{P}(A \cap B) = \mathbb{P}(A)\mathbb{P}(B)$$

[G-K] p. 52

Définition 2. On dit que les événements d'une famille $(A_i)_{i\in I}$ sont **mutuellement indépendants** si

$$\forall J \subseteq I, J \text{ fini}, \mathbb{P}\left(\bigcap_{j\in J} A_j\right) = \prod_{j\in J} \mathbb{P}(A_j)$$

Proposition 3. Soient A, B deux événements. Alors,

$$A \text{ et } B \text{ sont indépendants} \iff \mathbb{P}(A \setminus B) = \mathbb{P}(A) \iff \mathbb{P}(B \setminus A) = \mathbb{P}(B)$$

[DAN] p. 425

Proposition 4. Soient $A_1, \dots, A_n$ des événements mutuellement indépendants. Alors, pour tout $k \in [\![1, n]\!]$, $A_1^c, \dots, A_k^c, A_{k+1}, \dots, A_n$ sont mutuellement indépendants.

Exemple 5. On considère deux gênes a et b tels que la redondance de l'un d'entre eux entraîne l'acquisition d'un caractère d'un caractère $\mathscr{C}$. Anselme et Colette possèdent chacun la combinaison ab et attendant un enfant : elles lui transmettront chacun et indépendamment soit le gêne a, soit le gêne b avec la même probabilité de $\frac{1}{2}$. On considère les événements :

— A : Colette transmet le gêne a.

— B : Anselme transmet le gêne b.

— C : l'enfant présent le caractère $\mathscr{C}$.

A, B et C sont indépendants deux à deux, mais non mutuellement indépendants.

Application 6 (Indicatrice d'Euler)**.** On note φ l'indicatrice d'Euler. Alors,

$$\forall n \geq 2, \varphi(n) = n \prod_{\substack{p \text{ premier} \\ p|n}} \left(1 - \frac{1}{p}\right)$$

2. Indépendance de tribus

Définition 7. On dit que deux sous-tribus $\mathscr{A}_1$ et $\mathscr{A}_2$ de $\mathscr{A}$ sont **indépendantes** (sous $\mathbb{P}$) si

$$\forall A \in \mathscr{A}_1, \forall B \in \mathscr{A}_2, \mathbb{P}(A \cap B) = \mathbb{P}(A)\mathbb{P}(B)$$

[G-K] p. 52

Définition 8. On dit qu'une famille de sous-tribus $(\mathscr{A}_i)_{i\in I}$ de $\mathscr{A}$ sont **indépendantes** (sous $\mathbb{P}$) si

$$\forall J \subseteq I, J \text{ fini}, \forall (A_j)_{j\in J} \in \prod_{j\in J} \mathscr{A}_j, \mathbb{P}\left(\bigcap_{j\in J} A_j\right) = \prod_{j\in J} \mathbb{P}(A_j)$$

Remarque 9.
- Pour tout $A, B \in \mathscr{A}$, A est indépendante de B si et seulement si $\sigma(A)$ est indépendante de $\sigma(B)$.
- Si deux tribus $\mathscr{A}$ et $\mathscr{B}$ sont indépendantes, toute sous tribu de $\mathscr{A}$ est indépendante de toute sous tribu de $\mathscr{B}$.

3. Indépendance de variables aléatoires

a. Variables aléatoires indépendantes

Définition 10. Soit X une variable aléatoire réelle définie sur $(\Omega, \mathscr{A}, \mathbb{P})$. On note

$$\sigma(X) = \{X^{-1}(A) \mid A \in \mathscr{B}(\mathbb{R})\}$$

Cette famille est la **tribu engendrée** par X.

p. 125

Définition 11. On dit que deux variables aléatoires X et Y sont **indépendantes** si les tribus qu'elles engendrent sont indépendantes.

Exemple 12. Si X et Y sont deux variables aléatoires indépendantes, on a

$$\forall A, B \in \mathscr{B}(\mathbb{R}), \mathbb{P}(\{X \in A\} \cap \{Y \in B\}) = \mathbb{P}(X \in A)\mathbb{P}(Y \in B)$$

Proposition 13. Si X et Y sont deux variables aléatoires indépendantes, alors $f(X)$ et $g(Y)$ sont indépendantes pour toutes fonctions mesurables f et g.

Proposition 14. Soient X et Y deux vecteurs aléatoires indépendants. On suppose que X admet une densité f et Y admet une densité g. Alors, (X,Y) admet comme densité $(x,y) \mapsto f(x)g(y)$. p. 136

Proposition 15. Soient X et Y deux vecteurs aléatoires indépendants intégrables. Alors, p. 175

$$\mathbb{E}(XY) = \mathbb{E}(X)\mathbb{E}(Y)$$

b. Variables aléatoires non corrélées

Définition 16. On dit que deux variables aléatoires X et Y sont **non corrélées** si p. 174

$$\text{Covar}(X,Y) = \mathbb{E}(X - \mathbb{E}(X))\mathbb{E}(Y - \mathbb{E}(Y)) = 0$$

Proposition 17. Soient X et Y deux variables aléatoires indépendantes intégrables. Alors X et Y ne sont pas corrélées.

Contre-exemple 18. La réciproque est fausse. Ainsi, soient X et Y deux variables aléatoires vérifiant

$$\begin{aligned}\mathbb{P}(\{X=1\} \cap \{Y=1\}) &= \mathbb{P}(\{X=1\} \cap \{Y=-1\}) \\ &= \mathbb{P}(\{X=-1\} \cap \{Y=0\}) \\ &= \frac{1}{3}\end{aligned}$$

alors, X et Y sont non corrélées mais pas indépendantes.

II - Étude de variables aléatoires indépendantes

1. Critères d'indépendance

Théorème 19. Soient X et Y deux variables aléatoires. Alors, X et Y sont indépendantes si et seulement si $\mathbb{P}_{(X,Y)} = \mathbb{P}_X \otimes \mathbb{P}_Y$. p. 128

Corollaire 20. Soient X et Y deux variables aléatoires indépendantes. Alors, $\mathbb{P}_{X+Y} = \mathbb{P}_X * \mathbb{P}_Y$.

Proposition 21. Soient X et Y deux variables aléatoires définies sur $(\Omega, \mathscr{A}, \mathbb{P})$. On suppose que (X,Y) admet une densité $h : (x,y) \mapsto f(x)g(y)$ à variables séparées. Alors, X et Y sont indépendantes. De plus, X et Y admettent respectivement pour densité

$$x \mapsto \frac{f(x)}{\int_{\mathbb{R}} f(t)\,\mathrm{d}t} \text{ et } y \mapsto \frac{g(y)}{\int_{\mathbb{R}} g(t)\,\mathrm{d}t}$$

par rapport à la mesure de Lebesgue.

p. 136

2. Sommes de variables aléatoires indépendantes

Théorème 22. Soient X et Y deux variables aléatoires réelles indépendantes de densités respectives f et g. Alors, $X+Y$ admet comme densité la fonction $f * g : x \mapsto \int_{\mathbb{R}} f(x-t)g(t)\,\mathrm{d}t$.

p. 179

Application 23. Soient X et Y deux variables aléatoires indépendantes telles que $X \sim \Gamma(a,\gamma)$ et $Y \sim \Gamma(b,\gamma)$. Alors $Z = X+Y \sim \Gamma(a+b,\gamma)$.

Application 24.

$$\frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)} = \int_0^1 \theta^{a-1}(1-\theta)^{b-1}\,\mathrm{d}\theta$$

où Γ désigne la fonction Γ d'Euler.

Définition 25. Soit X une variable aléatoire à valeurs dans $\mathbb{N}$. On appelle **fonction génératrice** de X la fonction

$$G_X : \begin{array}{ccc} [-1,1] & \to & \mathbb{R} \\ z & \mapsto & \sum_{k=0}^{+\infty} \mathbb{P}(X=k) z^k \end{array}$$

p. 235

Proposition 26. Soient X et Y deux variables aléatoires à valeurs dans $\mathbb{N}$ indépendantes. Alors,

$$G_{X+Y} = G_X G_Y$$

Théorème 27. Sur $[0,1]$, la fonction G_X est infiniment dérivable et ses dérivées sont toutes positives, avec

$$G_X^{(n)}(s) = \mathbb{E}(X(X-1)\dots(X-n+1)s^{X-n})$$

En particulier,

$$\mathbb{P}(X=n) = \frac{G_X^{(n)}(0)}{n!}$$

ce qui montre que la fonction génératrice caractérise la loi.

Exemple 28. Si $X_1 \sim \mathscr{P}(\lambda)$ et $X_2 \sim \mathscr{P}(\mu)$ sont indépendantes, alors $X_1 + X_2 \sim \mathscr{P}(\lambda+\mu)$.

Exemple 29. Si $X_1 \sim \mathscr{B}(n,p)$ et $X_2 \sim \mathscr{B}(m,p)$ sont indépendantes, alors $X_1 + X_2 \sim \mathscr{B}(n+m,p)$. [GOU21] p. 346

Définition 30. On appelle **fonction caractéristique** de X la fonction ϕ_X définie sur $\mathbb{R}^d$ par [G-K] p. 239

$$\phi_X : t \mapsto \mathbb{E}\left(e^{i\langle t,X\rangle}\right)$$

Théorème 31. Si deux variables (ou vecteurs) aléatoires ont la même fonction caractéristique, alors elles ont même loi.

Proposition 32. Si deux variables aléatoires réelles sont indépendantes, alors $\phi_{X+Y} = \phi_X \phi_Y$.

III - Indépendance et théorèmes limites

1. Lemmes de Borel-Cantelli

Théorème 33 (1^{er} lemme de Borel-Cantelli)**.** Soit (A_n) une suite d'événements. Si $\sum \mathbb{P}(A_n)$ converge, alors p. 272

$$\mathbb{P}\left(\limsup_{n\to+\infty} A_n\right) = 0$$

Remarque 34. Cela signifie que presque sûrement, seul un nombre fini d'événements A_n se réalisent.

Corollaire 35. Si $\sum \mathbb{P}(|X_n - X| > \epsilon)$ converge pour tout $\epsilon > 0$, alors $X_n \xrightarrow{(ps.)} X$.

Exemple 36. Si (X_n) est telle que $\forall n \geq 1$, $\mathbb{P}(X_n = n) = \mathbb{P}(X_n = \pm n) = \frac{1}{2n^2}$ et $\mathbb{P}(X_n = 0) = 1 - \frac{1}{2n^2}$, alors la suite (S_n) définie pour tout $n \geq 1$ par $S_n = \sum_{k=1}^{n} X_k$ est constante à partir d'un certain rang. p. 285

Théorème 37 (2^{e} lemme de Borel-Cantelli)**.** Soit (A_n) une suite d'événements indépendants. p. 273

Si $\sum \mathbb{P}(A_n)$ diverge, alors

$$\mathbb{P}\left(\limsup_{n\to+\infty} A_n\right) = 1$$

Remarque 38. Cela signifie que presque sûrement, un nombre infini d'événements A_n se réalisent.

Exemple 39. On fait une infinité de lancers d'une pièce de monnaie équilibrée. Alors, la probabilité de l'événement "on obtient une infinité de fois deux "Face" consécutifs" est 1.

p. 286

Corollaire 40 (Loi du 0-1 de Borel)**.** Soit (A_n) une suite d'événements indépendants, alors

$$\mathbb{P}\left(\limsup_{n\to+\infty} A_n\right) = 0 \text{ ou } 1$$

et elle vaut 1 si et seulement si $\sum \mathbb{P}(A_n)$ diverge.

2. Lois des grands nombres

Théorème 41 (Loi faible des grands nombres)**.** Soit (X_n) une suite de variables aléatoires deux à deux indépendantes de même loi et $\mathscr{L}_1$. On pose $M_n = \frac{X_1+\cdots+X_n}{n}$. Alors,

$$M_n \xrightarrow{(p)} \mathbb{E}(X_1)$$

p. 270

Théorème 42 (Loi forte des grands nombres)**.** Soit (X_n) une suite de variables aléatoires mutuellement indépendantes de même loi. On pose $M_n = \frac{X_1+\cdots+X_n}{n}$. Alors,

$$X_1 \in \mathscr{L}_1 \iff M_n \xrightarrow{(ps.)} \ell \in \mathbb{R}$$

Dans ce cas, on a $\ell = \mathbb{E}(X_1)$.

[Z-Q] p. 532

Application 43 (Théorème de Bernstein)**.** Soit $f : [0,1] \to \mathbb{R}$ continue. On note

$$\forall n \in \mathbb{N}^*, B_n(f) : x \mapsto \sum_{k=0}^{n} \binom{n}{k} f\left(\frac{k}{n}\right) x^k (1-x)^{n-k}$$

le n-ième polynôme de Bernstein associé à f. Alors la suite de fonctions $(B_n(f))$ converge uniformément vers f.

[G-K] p. 195

[DEV]

Corollaire 44 (Théorème de Weierstrass)**.** Toute fonction continue $f : [a,b] \to \mathbb{R}$ (avec $a, b \in \mathbb{R}$ tels que $a \leq b$) est limite uniforme de fonctions polynômiales sur $[a,b]$.

3. Théorème central limite

Théorème 45 (Lévy)**.** Soient (X_n) une suite de variables aléatoires réelles et X une variable aléatoire réelle. Alors : [Z-Q] p. 544

$$X_n \xrightarrow{(d)} X \iff \phi_{X_n} \text{ converge simplement vers } \phi_X$$

Théorème 46 (Central limite)**.** On suppose que (X_n) est une suite de variables aléatoires réelles indépendantes de même loi admettant un moment d'ordre 2. On note m l'espérance et σ^2 la variance commune à ces variables. On pose $S_n = X_1 + \cdots + X_n - nm$. Alors, [G-K] p. 307

$$\left(\frac{S_n}{\sqrt{n}}\right) \xrightarrow{(d)} \mathcal{N}(0, \sigma^2)$$

Application 47 (Théorème de Moivre-Laplace)**.** On suppose que (X_n) est une suite de variables aléatoires indépendantes de même loi $\mathcal{B}(p)$. Alors,

$$\frac{\sum_{k=1}^{n} X_k - np}{\sqrt{n}} \xrightarrow{(d)} \mathcal{N}(0, p(1-p))$$

Application 48 (Formule de Stirling)**.** p. 556

$$n! \sim \sqrt{2n\pi}\left(\frac{n}{e}\right)^n$$

[DEV]

Application 49 (Théorème des événements rares de Poisson)**.** Soit $(N_n)_{n\geq 1}$ une suite d'entiers tendant vers l'infini. On suppose que pour tout n, $A_{n,N_1}, \ldots, A_{n,N_n}$ sont des événements indépendants avec $\mathbb{P}(A_{n,N_k}) = p_{n,k}$. On suppose également que : p. 390

(i) $\lim_{n\to+\infty} s_n = \lambda > 0$ où $\forall n \in \mathbb{N}, s_n = \sum_{k=1}^{N_n} p_{n,k}$.

(ii) $\lim_{n\to+\infty} \sup_{k\in[\![1,N_n]\!]} p_{n,k} = 0$.

Alors, la suite de variables aléatoires (S_n) définie par

$$\forall n \in \mathbb{N}^*, S_n = \sum_{k=1}^{n} \mathbb{1}_{A_{n,k}}$$

converge en loi vers la loi de Poisson de paramètre λ.

Annexes

Loi	**Somme** (indépendantes de même loi)
de Bernoulli	$\sum_{k=1}^{n} \mathscr{B}(p) \sim \mathscr{B}(n,p)$
Binomiale	$\sum_{k=1}^{n} \mathscr{B}(n_k,p) \sim \mathscr{B}\left(\sum_{k=1}^{n} n_k, p\right)$
de Poisson	$\sum_{k=1}^{n} \mathscr{P}(\lambda_k) \sim \mathscr{P}\left(\sum_{k=1}^{n} \lambda_k\right)$

[G-K] p. 137
p. 236

FIGURE I.31 – Sommes de variables aléatoires à lois discrètes.

Loi	**Somme** (indépendantes de même loi)
Normale	$\sum_{k=1}^{n} \mathscr{N}(\mu_k,\sigma_k^2) \sim \mathscr{N}\left(\sum_{k=1}^{n} \mu_k, \sum_{k=1}^{n} \sigma_k^2\right)$
Exponentielle	$\sum_{k=1}^{n} \mathscr{E}(\lambda) \sim \mathscr{E}(n\lambda)$
Gamma	$\sum_{k=1}^{n} \Gamma(a_k,\gamma) \sim \Gamma\left(\sum_{k=1}^{n} a_k, \gamma\right)$

p. 142
p. 247
p. 178

FIGURE I.32 – Sommes de variables aléatoires à densité.

II Développements

1 Caractérisation réelle de la fonction Γ

On montre que la fonction Γ *d'Euler est la seule fonction log-convexe sur* $\mathbb{R}^+$ *prenant la valeur* 1 *en* 1 *et vérifiant* $\Gamma(x+1) = x\Gamma(x)$ *pour tout* $x > 0$.

[ROM19-1] p. 364

Lemme 1. La fonction Γ définie pour tout $x > 0$ par $\Gamma(x) = \int_0^{+\infty} t^{x-1} e^{-t}\,\mathrm{d}t$ vérifie :

(i) $\forall x \in \mathbb{R}_*^+, \Gamma(x+1) = x\Gamma(x)$.

(ii) $\Gamma(1) = 1$.

(iii) Γ est log-convexe sur $\mathbb{R}_*^+$.

Démonstration. (i) Soit $x \in \mathbb{R}_*^+$. Alors :

$$\begin{aligned}\Gamma(x+1) &= \int_0^{+\infty} t^x e^{-t}\,\mathrm{d}t \\ &= \left[-e^{-t}t^x\right]_0^{+\infty} + x\int_0^{+\infty} t^{x-1}e^{-t}\,\mathrm{d}t \\ &= x\Gamma(x)\end{aligned}$$

(ii) Comme $t \mapsto e^{-t}\mathbb{1}_{\mathbb{R}^+}(t)$ est la densité de probabilité d'une loi exponentielle de paramètre 1, on a

$$\underbrace{\int_0^{+\infty} e^{-t}\,\mathrm{d}t}_{=\Gamma(1)} = 1$$

(iii) Soient $x, y \in \mathbb{R}_*^+$ et $\lambda \in]0,1[$. On applique l'inégalité de Hölder en posant $\lambda = \frac{1}{p}$ et $1-\lambda = \frac{1}{q}$:

$$\begin{aligned}\Gamma(\lambda x + (1-\lambda)y) &= \int_0^{+\infty} e^{-t}t^{\lambda x}t^{(1-\lambda)y}\,\mathrm{d}t \\ &= \int_0^{+\infty} (e^{-t}t^{x-1})^{\frac{1}{p}}(e^{-t}t^{y-1})^{\frac{1}{q}}\,\mathrm{d}t \\ &\leq \left(\int_0^{+\infty} e^{-t}t^{x-1}\right)^{\frac{1}{p}}\left(\int_0^{+\infty} e^{-t}t^{y-1}\right)^{\frac{1}{q}} \\ &= \Gamma(x)^{\lambda}\Gamma(y)^{1-\lambda}\end{aligned}$$

Donc $\ln\circ\Gamma$ vérifie bien l'inégalité de convexité sur $\mathbb{R}_*^+$ et ainsi, Γ est log-convexe.

□

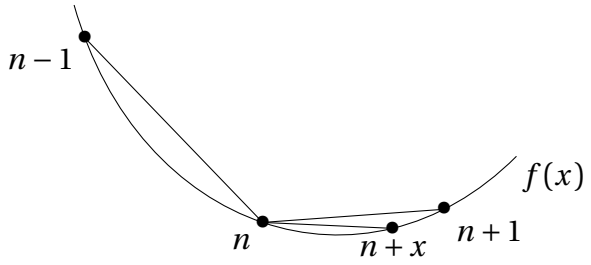
Théorème 2 (Bohr-Mollerup)**.** Soit $f : \mathbb{R}_*^+ \to \mathbb{R}^+$ vérifiant le Point (i), le Point (ii) et le Point (iii) du Théorème 1. Alors $f = \Gamma$.

Démonstration. Par récurrence, on a d'après le Point (i) :

$$\forall n \in \mathbb{N}^*, \forall x \in]0,1], f(x+n) = (x+n-1)\dots(x+1)xf(x) \qquad (*)$$

Donc les valeurs prises par f sur $\mathbb{R}_*^+$ sont entièrement déterminées par ses valeurs prises sur $]0,1]$. Ainsi, pour démontrer le théorème, il suffit de vérifier $\forall x \in]0,1], f(x) = \Gamma(x)$.

Soient donc $x \in]0,1]$ et $n \in \mathbb{N}^*$; on applique le lemme des trois pentes à la fonction convexe $\ln \circ f$ (d'après le Point (iii) appliqué aux points $n-1$, n, $n+x$ et $n+1$:



$$\frac{(\ln\circ f)(n)-(\ln\circ f)(n-1)}{n-(n-1)} \leq \frac{(\ln\circ f)(n+x)-(\ln\circ f)(n)}{n+x-n} \leq \frac{(\ln\circ f)(n+1)-(\ln\circ f)(n)}{n+1-n}$$

Mais, d'après $(*)$ et le Point (ii), on a $f(n) = (n-1)!$. D'où :

$$\begin{aligned} &\ln(n-1) \leq \frac{(\ln\circ f)(n+x)-\ln((n-1)!)}{x} \leq \ln(n) \\ \Longrightarrow\ &\ln((n-1)^x) \leq (\ln\circ f)(n+x)-\ln((n-1)!) \leq \ln(n^x) \\ \Longrightarrow\ &\ln((n-1)^x(n-1)!) \leq (\ln\circ f)(n+x) \leq \ln(n^x(n-1)!) \end{aligned}$$

Par croissance de la fonction ln, cela donne :

$$(n-1)^x(n-1)! \leq f(n+x) \leq n^x(n-1)!$$

Et en appliquant $(*)$, on obtient :

$$\frac{(n-1)^x(n-1)!}{(x+n-1)\dots(x+1)x} \leq f(x) \leq \frac{n^x(n-1)!}{(x+n-1)\dots(x+1)x}$$

En ne considérant que la première inégalité, on peut remplacer n par $n+1$ (car les deux inégalités sont vraies pour tout $n \in \mathbb{N}^*$) :

$$\frac{n^x n!}{(x+n)\dots(x+1)x} \leq f(x)$$

Or, $\frac{n^x(n-1)!}{(x+n-1)\dots(x+1)x} = \frac{n^x n!}{(x+n)\dots(x+1)x}\frac{x+n}{n}$, donc :

$$\begin{aligned}
&\frac{n^x n!}{(x+n)\dots(x+1)x} \leq f(x) \leq \frac{n^x n!}{(x+n)\dots(x+1)x}\frac{x+n}{n} \\
\Longrightarrow\ & f(x)\frac{n}{x+n} \leq \frac{n^x n!}{(x+n)\dots(x+1)x} \leq f(x) \\
\Longrightarrow\ & f(x) = \lim_{n\to+\infty} \frac{n^x n!}{(x+n)\dots(x+1)x}
\end{aligned}$$

en faisant $n \longrightarrow +\infty$ dans la deuxième implication. Comme Γ vérifie le Point (i), le Point (ii), et le Point (iii) ; le raisonnement précédent est a fortiori vrai aussi pour Γ. Donc

$$\Gamma(x) = \lim_{n\to+\infty} \frac{n^x n!}{(x+n)\dots(x+1)x} = f(x)$$

ie. f et Γ coïncident bien sur $]0,1]$. □

Remarque 3. À la fin de la preuve, on obtient une formule due à Gauss :

$$\forall x \in]0,1], \Gamma(x) = \lim_{n\to+\infty} \frac{n^x n!}{(x+n)\dots(x+1)x}$$

que l'on peut aisément étendre à $\mathbb{R}_*^+$ entier.

La preuve, telle qu'elle est écrite ici, est issue d'un livre de Walter Rudin. Elle est également disponible (sous une forme un peu différente) comme l'indique la référence, dans **[ROM19-1]**.

2 Connexité des valeurs d'adhérence d'une suite dans un compact

On montre que l'ensemble des valeurs d'adhérence d'une suite d'un espace métrique compact est connexe en raisonnant par l'absurde, puis on utilise ce résultat pour démontrer le lemme des grenouilles.

Soit (E,d) un espace métrique.

[I-P] p. 116

Théorème 1. On suppose E compact. Soit (u_n) une suite de E telle que $d(u_n,u_{n-1}) \longrightarrow 0$. Alors l'ensemble Γ des valeurs d'adhérence de (u_n) est connexe.

Démonstration. Pour tout $p \in \mathbb{N}$, on note $A_p = \{u_n \mid n \geq p\}$. On a $\Gamma = \bigcap_{p\in\mathbb{N}} \overline{A_p}$. Γ est fermé (en tant qu'intersection de fermés) dans E qui est compact, donc Γ est compact.Supposons que Γ soit non connexe ; on peut alors écrire $\Gamma = A \sqcup B$, où A et B sont deux fermés disjoints de Γ. Comme Γ est compact, A et B le sont aussi. Notons $\alpha = d(A,B) > 0$ (car $A \cap B = \emptyset$). Posons :

$$A' = \left\{x \in E \mid d(x,A) < \frac{\alpha}{3}\right\} \text{ et } B' = \left\{x \in E \mid d(x,B) < \frac{\alpha}{3}\right\}$$

A' et B' sont ouverts (en tant qu'images réciproques d'ouverts par des application continues), donc $K = E \setminus (A' \cup B')$ est fermé dans E, donc compact.

Montrons que (u_n) admet une valeur d'adhérence dans K, ce qui serait absurde car $\Gamma \cap K = \emptyset$. Comme $\lim_{n\to+\infty} d(u_n,u_{n-1}) = 0$,

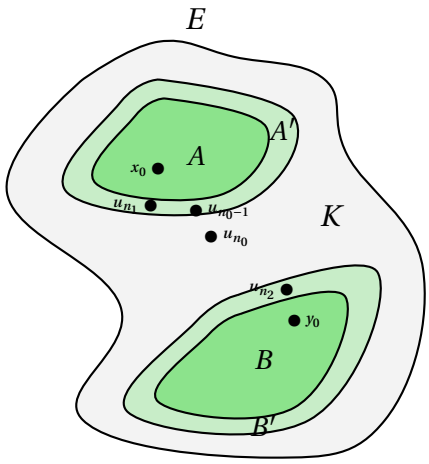
$$\exists N_0 \in \mathbb{N} \text{ tel que } \forall n \geq N_0,\ d(u_n,u_{n-1}) < \frac{\alpha}{3} \qquad (*)$$

Soit $N \geq N_0$.

— Soit $x_0 \in A$. Comme x_0 est valeur d'adhérence de (u_n), $\exists n_1 > N$ tel que $d(x_0,u_{n_1}) < \frac{\alpha}{3}$. Donc $u_{n_1} \in A'$.

— Soit $y_0 \in B$. De même, $\exists n_2 > n_1$ tel que $d(y_0,u_{n_2}) < \frac{\alpha}{3}$. Donc $u_{n_2} \in B'$.

Soit maintenant n_0 le premier entier supérieur à n_1 tel que $u_{n_0} \notin A'$ (un tel entier existe car $u_{n_2} \notin A'$). On a alors $u_{n_0-1} \in A'$.



D'après $(*)$, en appliquant l'inégalité triangulaire,

$$\begin{aligned} d(u_{n_0}, B) &\geq d(u_{n_0-1}, B) - d(u_{n_0-1}, u_{n_0}) \\ &\geq d(A, B) - d(u_{n_0-1}, A) - d(u_{n_0-1}, u_{n_0}) \\ &> \frac{\alpha}{3} \end{aligned}$$

ce qui prouve que $u_{n_0} \notin B'$. Comme $u_{n_0} \notin A'$, on a $u_{n_0} \in K$. On vient de montrer que,

$$\forall N \geq N_0, \exists n_0 \geq N \text{ tel que } u_{n_0} \in K$$

On peut créer comme cela une sous-suite de (u_n) dans K. Or K est compact, donc (u_n) admet une valeur d'adhérence dans K. □

Application 2 (Lemme de la grenouille)**.** Soient $f : [0,1] \to [0,1]$ continue et (x_n) une suite de $[0,1]$ telle que

$$\begin{cases} x_0 \in [0,1] \\ x_{n+1} = f(x_n) \end{cases}$$

Alors (x_n) converge si et seulement si $\lim_{n\to+\infty} x_{n+1} - x_n = 0$.

Démonstration. Le sens direct est évident. Montrons la réciproque. On suppose donc que $\lim_{n\to+\infty} x_{n+1} - x_n = 0$ et on note Γ l'ensemble des valeurs d'adhérence de (x_n). Γ est non vide (car (x_n) est bornée, donc admet une valeur d'adhérence par le théorème de Bolzano-Weierstrass) et est un connexe de $\mathbb{R}$ (par le Théorème 1), donc Γ est un intervalle non vide.

Soit $a \in \Gamma$. Il existe $\varphi : \mathbb{N} \to \mathbb{N}$ strictement croissante (on dit que φ est une extractrice) telle que $x_{\varphi(n)} \longrightarrow a$. Mais alors,

$$x_{\varphi(n)+1} - x_{\varphi(n)} = f(x_{\varphi(n)}) - x_{\varphi(n)} \longrightarrow f(a) - a$$

et par hypothèse, le membre de gauche converge vers 0. Donc $f(a) - a = 0$ ie. a est un point fixe de f.

Supposons par l'absurde que (x_n) diverge. Alors Γ n'est pas un singleton, donc est un intervalle

d'intérieur non vide : on peut trouver $c \in \Gamma$ et $h > 0$ tel que $[c-h, c+h] \subseteq \Gamma$.

Or, $c \in \Gamma$, donc

$$\exists N \geq 0 \text{ tel que } |x_N - c| \leq \frac{h}{2} \implies x_N \in \Gamma$$

et en particulier, x_N est un point fixe de f. Ainsi, $x_{n+1} = f(x_n) = x_n$ pour tout $n \geq N$: absurde. □

3 Critère d'Eisenstein

Ici, nous démontrons le célèbre critère d'Eisenstein que l'on utilise énormément en pratique pour montrer qu'un polynôme est irréductible.

Soit A un anneau commutatif et unitaire.

Notation 1. Soit $P \in A[X]$. On note $\gamma(P)$ le contenu du polynôme P.

Lemme 2. Soit $p \in A$ tel que (p) est premier. Alors $A/(p)$ est intègre. [ULM18] p. 32

Démonstration. Soient $\overline{a}, \overline{b} \in A/(p)$. On suppose $\overline{a}\overline{b} = 0$. Comme $\overline{a}\overline{b} = \overline{ab}$, on a $ab \in (p)$. Donc par hypothèse,

$$\begin{aligned} & a \in (p) \text{ ou } b \in (p) \\ \Longrightarrow\ & \overline{a} = 0 \text{ ou } \overline{b} = 0 \end{aligned}$$

et ainsi $A/(p)$ est bien intègre. □

Lemme 3. Si A est intègre, alors $A[X]$ l'est aussi. p. 22

Démonstration. Soient $P, Q \in A[X]$ non nuls, de degrés respectifs n et m que l'on écrit $P = \sum_{i=0}^{n} a_i X^i$ et $Q = \sum_{j=0}^{m} b_j X^j$. Alors, le coefficient de X^{n+m} dans le produit PQ est $a_n b_m$. Comme $a_n \neq 0$, $b_m \neq 0$ et A est intègre, ce coefficient est non nul. Donc en particulier, le produit PQ est non nul. □

Lemme 4. On suppose A factoriel. Soit $a \in A$ irréductible. Alors (a) est premier. p. 64

Démonstration. On suppose que $a \mid bc$ avec $b, c \in A$. Alors, il existe $d \in A$ tel que

$$ad = bc \qquad (*)$$

Si b est inversible, alors $a \mid c$. De même, si c est inversible, alors $a \mid b$. Supposons donc que b et c ne sont pas inversibles. Comme a est irréductible, on en déduit que d est un élément non nul et non inversible de A. Il existe donc des décompositions en irréductibles

$$b = \beta_1 \dots \beta_n,\ c = \gamma_1 \dots \gamma_m \text{ et } d = \delta_1 \dots \delta_k$$

avec $n, m, k \in \mathbb{N}^*$. Par conséquent, en injectant dans $(*)$:

$$a\delta_1 \dots \delta_k = \beta_1 \dots \beta_n \gamma_1 \dots \gamma_m$$

Comme la factorisation en irréductibles est unique à l'ordre près, il existe β_i ou γ_j qui est associé à a. Si bien que a divise b ou c ; c'est ce que l'on voulait démontrer. □

Lemme 5 (Gauss)**.** On suppose A factoriel. Alors :

(i) Le produit de deux polynômes primitifs est primitif.

(ii) $\forall P, Q \in A[X] \setminus \{0\}, \gamma(PQ) = \gamma(P)\gamma(Q)$.

[GOZ] p. 10

Démonstration. (i) Soient $P, Q \in A[X]$ tels que $\gamma(P) = \gamma(Q) = 1$. Supposons $\gamma(PQ) \neq 1$. Alors, il existe $p \in A$ irréductible tel que p divise tous les coefficients de PQ. Donc, dans $A/(p)$, $\overline{PQ} = \overline{P}\,\overline{Q} = 0$.

Mais, par le Théorème 4, (p) est premier. Donc par le Théorème 2 $A/(p)$ est intègre, et en particulier, $A/(p)[X]$ l'est aussi par le Théorème 3. Ainsi, $\overline{P} = 0$ ou $\overline{Q} = 0$: absurde.

(ii) En factorisant, on écrit $P = \gamma(P)R$ et $Q = \gamma(Q)S$ où $R, S \in A[X]$ avec $\gamma(R) = \gamma(S) = 1$. D'où $PQ = \gamma(P)\gamma(Q)RS$ avec $\gamma(RS) = 1$ par le Point (i). Ainsi, $\gamma(PQ) = \gamma(P)\gamma(Q)$.

□

Théorème 6 (Critère d'Eisenstein)**.** Soient $\mathbb{K}$ le corps des fractions de A et $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ de degré $n \geq 1$. On suppose que A est factoriel et qu'il existe $p \in A$ irréductible tel que :

(i) $p \mid a_i$, $\forall i \in [\![0, n-1]\!]$.

(ii) $p \nmid a_n$.

(iii) $p^2 \nmid a_0$.

Alors P est irréductible dans $\mathbb{K}[X]$.

Démonstration. Par l'absurde, on suppose $P = UV$ avec $U, V \in \mathbb{K}[X]$ de degré supérieur ou égal à 1. Soit a un multiple commun à tous les dénominateurs des coefficients non nuls de U et V. On a

$$a^2 P = \underbrace{aU}_{\substack{=U_1 \\ \in A[X]}} \underbrace{aV}_{\substack{=V_1 \\ \in A[X]}}$$

On applique le Théorème 5 pour obtenir :

$$a^2\gamma(P) = \gamma(U_1)\gamma(V_1) \qquad (*)$$

En factorisant, on écrit $U_1 = \gamma(U_1)U_2$ et $V_1 = \gamma(V_1)V_2$ avec $U_2, V_2 \in A[X]$. Il vient :

$$a^2 P = \gamma(U_1)\gamma(V_1)U_2V_2 \overset{(*)}{=} a^2\gamma(P)U_2V_2$$

Et comme $a \in A \setminus \{0\}$ et que A est intègre, on a $P = \gamma(P)U_2V_2 = U_3V_3$ avec $U_3 = \gamma(P)U_2 \in A[X]$ et $V_3 = V_2 \in A[X]$ (dans un souci de symétrie des notations) qui sont de degré supérieur ou égal à 1.

On pose $U_3 = \sum_{i=0}^{r} b_i X^i$ et $V_3 = \sum_{j=0}^{s} c_j X^j$ avec $b_r c_s = a_n \neq 0$ par définition de P. Dans $A/(p)$, on a

$$\underbrace{\overline{P}}_{=\overline{a_n}X^n} = \overline{U_3V_3} = \overline{U_3}\,\overline{V_3}$$

et en particulier, le terme de degré 0, $\overline{b_0 c_0} = \overline{b_0}\,\overline{c_0}$ est nul. Mais, p est irréductible et A est factoriel, donc au vu du Théorème 4, (p) est premier et $A/(p)$ est intègre par le Théorème 2. Donc par le Théorème 3, $A/(p)[X]$ est aussi intègre. D'où $\overline{b_0} = 0$ ou $\overline{c_0} = 0$ (mais pas les deux car sinon $p^2 \mid b_0 c_0 = a_0$, ce qui serait en contradiction avec le Point (iii)).

On suppose donc $\overline{b_0} = 0$ et $\overline{c_0} \neq 0$. Si on avait $\forall i \in [\![0, r]\!]$, $\overline{b_i} = 0$, on aurait en particulier $\overline{b_r} = 0$, et donc $\overline{b_r}\,\overline{c_s} = \overline{a_n} = 0$ (exclu par le Point (ii)). Donc,

$$\exists i \in [\![0, r-1]\!] \text{ tel que } \overline{b_0} = \cdots = \overline{b_i} = 0 \text{ et } b_{i+1} \neq 0$$

Ainsi,

$$\overline{a_{i+1}} = \sum_{k=0}^{i+1} \overline{b_k}\,\overline{c_{i+1-k}} = \underbrace{\overline{b_{i+1}}}_{\neq 0}\,\underbrace{\overline{c_0}}_{\neq 0} \neq 0$$

ce qui est absurde au vu du Point (i) car $i \in [\![0, r-1]\!]$ avec $r - 1 \leq n - 1$. □

Application 7. Soit $n \in \mathbb{N}^*$. Il existe des polynômes irréductibles de degré n sur $\mathbb{Z}$.

[PER] p. 67

Démonstration. On applique le Théorème 6 au polynôme $P = X^n - 2$ avec le premier $p = 2$ qui nous donne l'irréductibilité du polynôme sur $\mathbb{Q}$. Reste à montrer qu'il est irréductible sur $\mathbb{Z}$.

Or, en supposant P réductible sur $\mathbb{Z}$, on peut écrire $P = QR$ avec $Q, R \in \mathbb{Z}[X]$ de degré supérieur ou égal à 1 car P est primitif. Mais à fortiori, $Q, R \in \mathbb{Q}[X]$ et ne sont pas inversibles donc P est réductible sur $\mathbb{Q}$: absurde. □

4 Décomposition de Dunford

On démontre l'existence et l'unicité de la décomposition de Dunford pour tout endomorphisme d'un espace vectoriel de dimension finie.

Soit E un espace vectoriel de dimension finie sur un corps commutatif $\mathbb{K}$.

[GOU21] p. 203

Théorème 1 (Décomposition de Dunford)**.** Soit $f \in E$ un endomorphisme tel que son polynôme minimal π_f soit scindé sur $\mathbb{K}$. Alors il existe un unique couple d'endomorphismes (d, n) tel que :

- $f = d + n$.
- d est diagonalisable et n est nilpotent.
- $d \circ n = n \circ d$.

Démonstration. On écrit $\pi_f = (-1)^n \prod_{i=1}^{s} (X - \lambda_i)^{\alpha_i}$ et pour tout i, on note $N_i = \mathrm{Ker}((f - \lambda_i \mathrm{id}_E)^{\alpha_i})$ le i-ième sous-espace caractéristique de f.

Construction : Comme $E = N_1 \oplus \cdots \oplus N_s$, il suffit de définir d et n sur chaque N_i. On les définit pour tout i et pour tout $x \in N_i$ comme tels :

- $d(x) = \lambda_i x \implies d_{|N_i} = \lambda_i \mathrm{id}_{N_i}$
- $n(x) = f(x) - \lambda_i x = f(x) - d(x) \implies n = f - d$.

Vérification :

- Les restrictions de d et n à N_i sont bien des endomorphismes car les espaces N_i sont stables par f et par d (cf. définition de d), donc aussi par $n = f - d$.
- d est diagonalisable et pour tout i, $n_{|N_i}^{\alpha_i} = 0$ (car $\forall x \in N_i$, $(f - \lambda_i)^{\alpha_i}(x) = 0$ par définition de N_i). On pose donc $\alpha = \max_i\{\alpha_i\}$ et on a $n_{|N_i}^{\alpha} = 0$ pour tout i, donc $n^{\alpha} = 0$ par somme directe. Ainsi, n est nilpotent.
- Pour tout i, on a $d_{|N_i} = \lambda_i \mathrm{id}_E$, donc $n_{|N_i} \circ d_{|N_i} = d_{|N_i} \circ n_{|N_i}$ i.e. d et n commutent sur chaque N_i donc sur E tout entier.

Unicité : Soit (d', n') un autre couple d'endomorphismes de E vérifiant les hypothèses. On remarque d'abord que d' et f commutent (car d' commute avec d' et n', donc avec $f = d' + n'$ aussi). Pour tout i, N_i est stable par d' (car $\forall x \in N_i$, $(f - \lambda_i \mathrm{id}_E)^{\alpha_i}(d'(x)) = d' \circ (f - \lambda_i \mathrm{id}_E)^{\alpha_i}(x) = 0$). Comme $d_{|N_i} = \lambda_i \mathrm{id}_{N_i}$, on en déduit que $d \circ d' = d' \circ d$ sur N_i. Donc c'est également vrai sur E tout entier. Ainsi, d et d' sont diagonalisables dans une même base, donc $d - d'$ est diagonalisable.

D'autre part, comme $n = f - d$, $n' = f - d'$ et que d et d' commutent, n et n' commutent. Si on choisit p et q tels que $n^p = n'^q = 0$, alors :

$$(n - n')^{p+q} = \sum_{i=0}^{p+q} \binom{p+q}{i} n^i (-1)^{p+q-i} n'^{p+q-i} = 0$$

(dans chaque terme de la somme, soit $i \geq p$, soit $p + q - i \geq q$). Donc $n - n' = d' - d$ est nilpotent. Or nous avions montré que $d' - d$ est diagonalisable, donc $d' - d = 0$. Finalement, on a $d = d'$ et $n = n'$. □

Remarque 2. On peut démontrer que les endomorphismes d et n sont des polynômes en f. En effet, si on note p_i la projection sur N_i parallèlement à $\bigoplus_{\substack{j=1\\j\neq i}}^{s} N_j$, alors, le lemme des noyaux nous indique que p_i est la restriction à N_i d'un endomorphisme en f. Comme $d = \sum_{i=1}^{s} \lambda_i p_i$, d est également un polynôme en f ; et $n = f - d$ aussi.

5 Décomposition polaire

On montre que toute matrice $M \in \mathrm{GL}_n(\mathbb{R})$ peut s'écrire de manière unique $M = OS$ avec $O \in \mathcal{O}_n(\mathbb{R})$ et $S \in \mathcal{S}_n^{++}(\mathbb{R})$, et que l'application $(O,S) \mapsto M$ est un homéomorphisme.

Lemme 1. Soit $S \in \mathcal{S}_n(\mathbb{R})$. Alors $S \in \mathcal{S}_n^{++}(\mathbb{R})$ si et seulement si toutes ses valeurs propres sont strictement positives.

Démonstration. Par le théorème spectral, on peut écrire $S = {}^tP\,\mathrm{Diag}(\lambda_1,\dots,\lambda_n)P$ avec $P \in \mathcal{O}_n(\mathbb{R})$. Si on suppose $\lambda_1,\dots,\lambda_n > 0$, on a $\forall x \neq 0$,

$$ {}^txSx = {}^t(Px)\,\mathrm{Diag}(\lambda_1,\dots,\lambda_n)(Px) > 0 \text{ car } \mathrm{Diag}(\lambda_1,\dots,\lambda_n) \in \mathcal{S}_n^{++}(\mathbb{R})$$

d'où le résultat.

Réciproquement, on suppose $\forall x \neq 0$, ${}^txSx > 0$. Avec $x = {}^tPe_1$ (où e_1 désigne le vecteur dont la première coordonnée vaut 1 et les autres sont nulles),

$$ {}^txSx = {}^t(Px)\,\mathrm{Diag}(\lambda_1,\dots,\lambda_n)(Px) = {}^te_1De_1 = \lambda_1 > 0$$

Et on peut faire de même pour montrer que $\forall i \in [\![1,n]\!]$, $\lambda_i > 0$. □

Lemme 2. $\mathcal{S}_n^+(\mathbb{R})$ est un fermé de $\mathcal{M}_n(\mathbb{R})$ et $\mathrm{GL}_n(\mathbb{R}) \cap \mathcal{S}_n^+(\mathbb{R}) \subseteq \mathcal{S}_n^{++}(\mathbb{R})$.

Démonstration. Pour la première assertion, il suffit de constater que

$$\mathcal{S}_n^+(\mathbb{R}) = \{M \in \mathcal{M}_n(\mathbb{R}) \mid {}^tM = M\} \cap \left(\bigcap_{x\in\mathbb{R}^n} \{M \in \mathcal{M}_n(\mathbb{R}) \mid {}^txMx \geq 0\} \right)$$

qui est une intersection de fermés (par image réciproque). Maintenant, si $M \in \mathrm{GL}_n(\mathbb{R}) \cap \mathcal{S}_n^+(\mathbb{R})$, alors M est diagonalisable avec des valeurs propres positives ou nulles (par le théorème spectral). Mais comme $\det(M) \neq 0$, toutes les valeurs propres de M sont strictement positives. Donc par le Théorème 1, $M \in \mathcal{S}_n^{++}(\mathbb{R})$. □

Théorème 3 (Décomposition polaire)**.** L'application

$$\mu : \begin{array}{ccc} \mathcal{O}_n(\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R}) & \to & \mathrm{GL}_n(\mathbb{R}) \\ (O,S) & \mapsto & OS \end{array}$$

est un homéomorphisme.

[C-G] p. 376

Démonstration. Montrer qu'une application est un homéomorphisme se fait en 4 étapes : on montre qu'elle est continue, injective, surjective, et que la réciproque est elle aussi continue.

— L'application est bien définie et continue : Si $O \in \mathcal{O}_n(\mathbb{R})$ et $S \in \mathcal{S}_n^{++}(\mathbb{R})$, alors $OS \in \mathrm{GL}_n(\mathbb{R})$. De plus, μ est continue en tant que restriction de la multiplication matricielle.

— L'application est surjective : Soit $M \in \mathrm{GL}_n(\mathbb{R})$. Si $x \neq 0$, on a

$$ {}^t x({}^t MM)x = {}^t(Mx)(Mx) = \|Mx\|_2^2 > 0 $$

En particulier, ${}^t MM \in \mathcal{S}_n^{++}(\mathbb{R})$. Par le théorème spectral, il existe $P \in \mathcal{O}_n(\mathbb{R})$ et $\lambda_1, \dots, \lambda_n > 0$ tels que ${}^t MM = P\,\mathrm{Diag}(\lambda_1, \dots, \lambda_n)P^{-1}$. On pose alors

$$ D = \mathrm{Diag}\left(\sqrt{\lambda_1}, \dots, \sqrt{\lambda_n}\right) \text{ et } S = PDP^{-1} $$

de sorte que $S^2 = {}^t MM$. Mais de plus,

$$ {}^t S = {}^t P^{-1}\,{}^t D\,{}^t P = S \implies S \in \mathcal{S}_n(\mathbb{R}) $$

et par le Théorème 1,

$$ \forall i \in [\![1, n]\!],\ \sqrt{\lambda_i} > 0 \implies S \in \mathcal{S}_n^{++}(\mathbb{R}) $$

On pose donc $O = MS^{-1}$ (ie. $M = OS$), et on a

$$ {}^t OO = {}^t(MS^{-1})MS^{-1} = {}^t S^{-1}\,{}^t MMS^{-1} = S^{-1}S^2S^{-1} = I_n \implies O \in \mathcal{O}_n(\mathbb{R}) $$

Donc $\mu(O, S) = M$ et μ est surjective.

— L'application est injective : Soit $M = OS \in \mathrm{GL}_n(\mathbb{R})$ (avec O et S comme précédemment). Soit $M = O'S'$ une autre décomposition polaire de M. Alors il vient,

$$ S^2 = {}^t MM = {}^t(O'S')O'S' = {}^t S'\,{}^t O'O'S' = S'^2 $$

Soit Q un polynôme tel que $\forall i \in [\![1, n]\!]$, $Q(\lambda_i) = \sqrt{\lambda_i}$ (les polynômes d'interpolation de Lagrange conviennent parfaitement). Alors,

$$ S = PD\,{}^t P = PQ\left(D^2\right){}^t P = Q\left(PD^2\,{}^t P\right) = Q\left({}^t MM\right) = Q\left(S^2\right) = Q\left(S'^2\right) $$

Mais S' commute avec S'^2, donc avec $S = Q\left(S'^2\right)$. En particulier, S et S' sont codiagonalisables, il existe $P_0 \in \mathrm{GL}_n(\mathbb{R})$ et $\mu_1, \dots, \mu_n, \mu'_1, \dots, \mu'_n \in \mathbb{R}$ tels que

$$ S = P_0\,\mathrm{Diag}(\mu_1, \dots, \mu_n)P_0^{-1} \text{ et } S' = P_0\,\mathrm{Diag}\left(\mu'_1, \dots, \mu'_n\right)P_0^{-1} $$

d'où :

$$ \begin{aligned} S^2 = S'^2 &\implies P_0\,\mathrm{Diag}\left(\mu_1^2, \dots, \mu_n^2\right)P_0^{-1} = P_0\,\mathrm{Diag}\left(\mu_1'^2, \dots, \mu_n'^2\right)P_0^{-1} \\ &\implies \mu_i^2 = \mu_i'^2 \qquad \forall i \in [\![1, n]\!] \\ &\implies \mu_i = \mu'_i \qquad \forall i \in [\![1, n]\!] \text{ car } \forall i \in [\![1, n]\!],\ \mu_i > 0 \\ &\implies S = S' \end{aligned} $$

Ainsi, $O = MS^{-1} = MS'^{-1} = O'$. Donc μ est injective.

— L'application inverse est continue : Soit $(M_p) \in \mathrm{GL}_n(\mathbb{R})^{\mathbb{N}}$ qui converge vers $M \in \mathrm{GL}_n(\mathbb{R})$. Il

s'agit de montrer que la suite $\left(\mu^{-1}\left(M_p\right)\right) = (O_p, S_p)$ converge vers $\mu^{-1}(M) = (O, S)$. Comme $\mathcal{O}_n(\mathbb{R})$ est compact, il existe $\varphi : \mathbb{N} \to \mathbb{N}$ strictement croissante telle que la suite extraite $(O_{\varphi(p)})$ converge vers une valeur d'adhérence $\overline{O} \in \mathcal{O}_n(\mathbb{R})$. Ainsi, la suite $(S_{\varphi(p)})$ converge vers $\overline{S} = \overline{O}^{-1}M$.

Mais, $\overline{S} = \overline{O}^{-1}M \in \mathrm{GL}_n(\mathbb{R}) \cap \overline{\mathcal{S}_n^{++}(\mathbb{R})}$. Donc par le Théorème 1,

$$\overline{S} \in \mathrm{GL}_n(\mathbb{R}) \cap \mathcal{S}_n^{+}(\mathbb{R})$$

et par le Théorème 2,

$$\overline{S} \in \mathcal{S}_n^{++}(\mathbb{R})$$

On a $M = \overline{OS}$, d'où, par unicité de la décomposition polaire, $\overline{O} = O$ et $\overline{S} = S$.

□

Remarque 4. La preuve vaut encore dans le cas complexe (pour le groupe unitaire et les matrices hermitiennes).

6 Densité des polynômes orthogonaux

On montre que la famille des polynômes orthogonaux associée à une fonction poids ρ vérifiant certaines hypothèses forme une base hilbertienne de $L_2(I,\rho)$ (où I est un intervalle de $\mathbb{R}$).

Soient I un intervalle de $\mathbb{R}$ et ρ une fonction poids. On considère (P_n) la famille des polynômes orthogonaux associée à ρ sur I. **[BMP]** p. 140

Lemme 1. On suppose que $\forall n \in \mathbb{N}$, $g_n : x \mapsto x^n \in L_1(I,\rho)$. Alors $\forall n \in \mathbb{N}$, $g_n \in L_2(I,\rho)$. En particulier, l'algorithme de Gram-Schmidt a bien du sens et (P_n) est bien définie.

Démonstration. On a $\forall n \in \mathbb{N}$,

$$\int_I |x^n|^2 \rho(x)\,\mathrm{d}x = \int_I |x^{2n}|\rho(x)\,\mathrm{d}x = \|g_{2n}\|_1 < +\infty$$

□

Théorème 2. On suppose qu'il existe $a > 0$ tel que

$$\int_I e^{a|x|}\rho(x)\,\mathrm{d}x < +\infty$$

alors (P_n) est une base hilbertienne de $L_2(I,\rho)$ pour la norme $\|.\|_2$.

Démonstration. Soit $f \in \mathrm{Vect}(g_n)^\perp = \mathrm{Vect}(P_n)^\perp$. On définit

$$\forall x \in \mathbb{R}, \quad \varphi(x) = \begin{cases} f(x)\rho(x) & \text{si } x \in I \\ 0 & \text{sinon} \end{cases}$$

Montrons que $\varphi \in L_1(\mathbb{R})$. Remarquons tout d'abord que $\forall t \geq 0$, $t \leq \frac{1+t^2}{2}$. Ainsi, on a

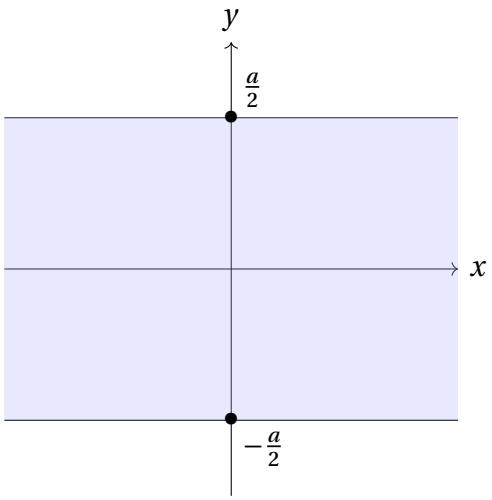
$$\forall x \in I, \quad |f(x)|\rho(x) \leq \frac{1+|f(x)|^2}{2}\rho(x)$$

Comme ρ et ρf^2 sont intégrables sur I, on en déduit que $\varphi \in L_1(\mathbb{R})$. On peut donc considérer sa transformée de Fourier

$$\widehat{\varphi} : \xi \mapsto \int_I f(x)e^{-i\xi x}\rho(x)\,\mathrm{d}x$$

Montrons que $\widehat{\varphi}$ se prolonge en une fonction F holomorphe sur

$$B_a = \left\{ z \in \mathbb{C} \mid |\mathrm{Im}(z)| < \frac{a}{2} \right\}$$



Définissons à présent $g : (z,x) \mapsto e^{-izx} f(x)\rho(x)$. Pour $z \in B_a$, on a

$$\int_I |g(z,x)|\,\mathrm{d}x \leq \int_I e^{\frac{a|x|}{2}} |f(x)|\rho(x)\,\mathrm{d}x$$

En utilisant l'inégalité de Cauchy-Schwarz pour $\|.\|_2$, on obtient de plus

$$\int_I e^{\frac{a|x|}{2}} |f(x)|\rho(x)\,\mathrm{d}x \leq \left(\int_I e^{a|x|}\rho(x)\,\mathrm{d}x\right)^{\frac{1}{2}} \left(\int_I |f(x)|^2\rho(x)\,\mathrm{d}x\right)^{\frac{1}{2}} < +\infty \qquad (*)$$

On définit la fonction F par

$$\forall z \in B_a, \quad F(z) = \int_I e^{-izx} f(x)\rho(x)\,\mathrm{d}x = \int_I g(z,x)\,\mathrm{d}x$$

L'inégalité $(*)$ montre que cette fonction est bien définie. De plus :

— $\forall z \in B_a$, $x \mapsto g(z,x)$ est mesurable.

— pp. en $x \in I$, $z \mapsto g(z,x)$ est holomorphe.

— $\forall z \in B_a$, $\forall x \in I$,
$$|g(z,x)| \leq h(x) = e^{\frac{a|x|}{2}} |f(x)|\rho(x)$$
et l'inégalité $(*)$ montre que $h \in L_1(I)$.

Donc par le théorème d'holomorphie sous l'intégrale, la fonction F est holomorphe sur B_a, et coïncide sur $\mathbb{R}$ avec $\widehat{\varphi}$.Ce théorème nous dit de plus que

$$\forall n \in \mathbb{N}, \forall z \in B_a, F^{(n)}(z) = (-i)^n \int_I x^n e^{-izx} f(x)\rho(x)\,\mathrm{d}x$$

Ce qui donne, une fois évalué en 0 :

$$\forall n \in \mathbb{N}, F^{(n)}(0) = (-i)^n \int_I x^n f(x)\rho(x)\,\mathrm{d}x = (-i)^n \langle g_n, f\rangle = 0$$

L'unicité du développement en série entière d'une fonction holomorphe montre que $F = 0$ sur un voisinage de 0. Le théorème du prolongement analytique implique alors que $F = 0$ sur le connexe B_a tout entier, et donc en particulier, sur $\mathbb{R}$. Ainsi, $\widehat{\varphi} = 0$. Comme φ est une fonction

intégrable, l'injectivité de la transformée de Fourier implique que $\varphi = 0$. Comme $\rho(x) > 0$, on en déduit que $f(x) = 0$ pp. en $x \in I$. On vient donc de montrer qu'une fonction orthogonale à tous les polynômes est nulle i.e. $\text{Vect}(g_n)^\perp = \{0\}$.En ajoutant le Théorème 1 à ceci, on a bien que les polynômes orthogonaux forment une base hilbertienne de $L_2(I, \rho)$. □

Contre-exemple 3. On considère, sur $I = \mathbb{R}_*^+$, la fonction poids $\rho : x \mapsto x^{-\ln(x)}$. On pose $\forall x \in I$, $f(x) = \sin(2\pi \ln(x))$. On calcule

$$\begin{aligned}
\langle f, g_n \rangle &= \int_I x^n \sin(2\pi \ln(x)) x^{-\ln(x)} \, \mathrm{d}x \\
&\overset{y=\ln(x)}{=} \int_{\mathbb{R}} e^{(n+1)y} \sin(2\pi y) e^{-y^2} \, \mathrm{d}y \\
&= e^{\frac{(n+1)^2}{4}} \int_{\mathbb{R}} e^{-\left(y-\frac{n+1}{2}\right)^2} \sin(2\pi y) \, \mathrm{d}y \\
&= (-1)^{n+1} e^{\frac{(n+1)^2}{4}} \int_{\mathbb{R}} \sin(2\pi t) e^{-t^2} \, \mathrm{d}t, \text{ avec } t = y - \frac{n+1}{2} \\
&\overset{f \text{ impaire}}{=} 0
\end{aligned}$$

Ainsi, la famille des g_n n'est pas totale. La famille des polynômes orthogonaux associée à ce poids particulier n'est donc pas totale non plus : ce n'est pas une base hilbertienne.

7 Développement asymptotique de la série harmonique

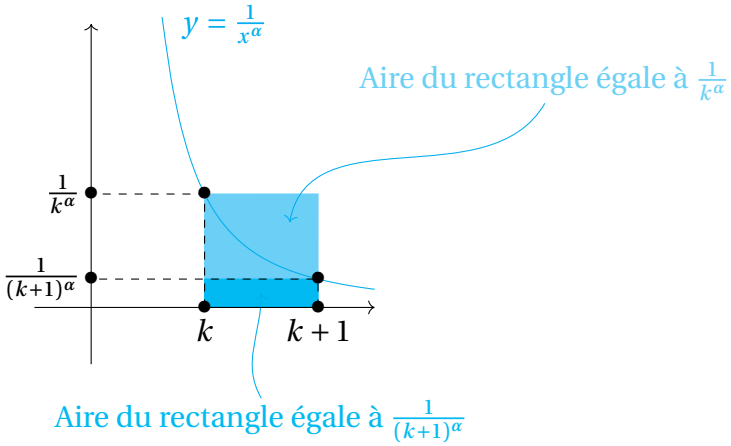
On effectue un développement asymptotique à l'ordre 2 de la série harmonique $\sum \frac{1}{n}$.

Lemme 1. Soit $\alpha > 1$. Lorsque n tend vers $+\infty$, on a

$$\sum_{k=n+1}^{+\infty} \frac{1}{n^\alpha} \sim \frac{1}{\alpha-1}\frac{1}{n^{\alpha-1}}$$

[I-P] p. 380

Démonstration. La fonction $x \mapsto \frac{1}{x}^\alpha$ est décroissante sur $\mathbb{R}_*^+$, nous allons faire une comparaison série / intégrale.



On a

$$\forall k \geq 1,\ \frac{1}{(k+1)^\alpha} \leq \int_k^{k+1} \frac{1}{x^\alpha}\,\mathrm{d}x \leq \frac{1}{k^\alpha}$$

D'où :

$$\forall k \geq 2,\ \int_k^{k+1} \frac{1}{x^\alpha}\,\mathrm{d}x \leq \frac{1}{k^\alpha} \leq \int_{k-1}^{k} \frac{1}{x^\alpha}\,\mathrm{d}x$$

Soit $N \geq 2$. Pour tout $n \in [\![2, N]\!]$,

$$\begin{aligned}
&\int_n^{N+1} \frac{1}{x^\alpha}\,\mathrm{d}x \leq \sum_{k=n}^{N} \frac{1}{k^\alpha} \leq \int_{n-1}^{N} \frac{1}{x^\alpha}\,\mathrm{d}x \\
\iff &\left[\frac{-1}{\alpha-1}\frac{1}{x^{\alpha-1}}\right]_n^{N+1} \leq \sum_{k=n}^{N} \frac{1}{k^\alpha} \leq \left[\frac{-1}{\alpha-1}\frac{1}{x^{\alpha-1}}\right]_{n-1}^{N} \\
\iff &\frac{1}{\alpha-1}\left(\frac{1}{n^{\alpha-1}} - \frac{1}{(N+1)^{\alpha-1}}\right) \leq \sum_{k=n}^{N} \frac{1}{k^\alpha} \leq \frac{1}{\alpha-1}\left(\frac{1}{(n-1)^{\alpha-1}} - \frac{1}{N^{\alpha-1}}\right)
\end{aligned}$$

La suite $\left(\sum_{k=n}^{N} \frac{1}{k^\alpha}\right)$ est donc convergente, car elle est croissante et majorée par $\frac{1}{\alpha-1}\left(\frac{1}{(n-1)^{\alpha-1}}\right)$. Lorsque N tend vers $+\infty$, on a donc

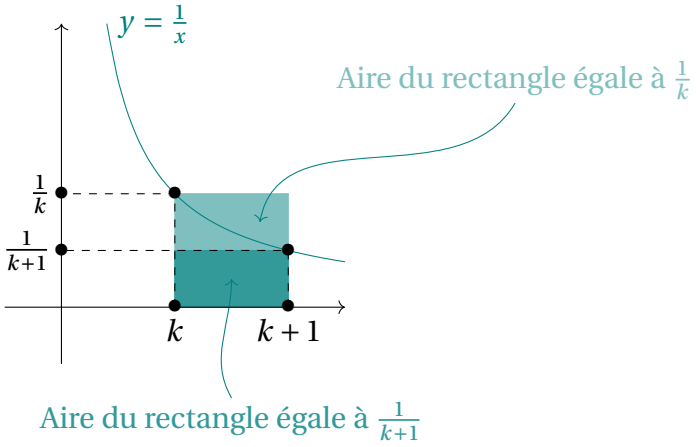
$$\frac{1}{\alpha-1}\left(\frac{1}{n^{\alpha-1}}\right) \leq \sum_{k=n}^{+\infty} \frac{1}{k^\alpha} \leq \frac{1}{\alpha-1}\left(\frac{1}{(n-1)^{\alpha-1}}\right)$$

Or, comme $n^{\alpha-1} \sim (n-1)^{\alpha-1}$ quand n tend vers $+\infty$, on en conclut l'équivalent annoncé. □

Théorème 2 (Développement asymptotique de la série harmonique)**.** On note $\forall n \in \mathbb{N}^*, H_n = \sum_{k=1}^{n} \frac{1}{k}$. Alors, quand n tend vers $+\infty$,

$$H_n = \ln(n) + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + o\left(\frac{1}{n^2}\right)$$

Démonstration. La fonction $x \mapsto \frac{1}{x}$ est décroissante sur $\mathbb{R}_*^+$, cela invite à faire une comparaison série / intégrale.



On a

$$\forall k \geq 1, \frac{1}{k+1} \leq \int_k^{k+1} \frac{1}{x}\,\mathrm{d}x \leq \frac{1}{k}$$

Traitons les deux morceaux séparément.

— $\forall k \geq 1, \int_k^{k+1} \frac{1}{x}\,\mathrm{d}x \leq \frac{1}{k}$ par l'inégalité de droite. Donc, en sommant entre 1 et $n \in \mathbb{N}^*$:

$$\ln(n+1) = \int_1^{n+1} \frac{1}{x}\,\mathrm{d}x \leq H_n$$

— $\forall k \geq 2, \frac{1}{k} \leq \int_{k-1}^{k} \frac{1}{x}\,\mathrm{d}x$ par l'inégalité de gauche avec un changement de variable. Donc, en sommant entre 2 et $n \in \mathbb{N}^*$:

$$\sum_{k=2}^{n} \frac{1}{k} \leq \int_1^n \frac{1}{x}\,\mathrm{d}x = \ln(n)$$

et en ajoutant 1 :

$$H_n \leq \ln(n) + 1$$

On peut tout regrouper pour obtenir les inégalités suivantes :

$$\ln(n+1) \leq H_n \leq \ln(n) + 1$$

et donc, quand n tend vers $+\infty$,

$$H_n \sim \ln(n)$$

Pour la suite, on pose pour tout $n \geq 1$, $u_n = H_n - \ln(n)$ et pour tout $n \geq 2$, $v_n = H_{n-1} - \ln(n)$. On a :

— $\forall n \geq 2$, $u_n - v_n = \frac{1}{n} \geq 0$ et converge vers 0 quand n tend vers $+\infty$.

— $\forall n \geq 1$,

$$\begin{aligned} u_n - u_{n+1} &= -\frac{1}{n+1} - \ln(n) + \ln(n+1) \\ &= -\frac{1}{n+1} - \ln\left(1 - \frac{1}{n+1}\right) \\ &\geq 0 \end{aligned}$$

car $\ln(1+x) \leq x$ pour $x \in]-1, +\infty[$.

— $\forall n \geq 2$,

$$\begin{aligned} v_{n+1} - v_n &= \frac{1}{n} + \ln(n) - \ln(n+1) \\ &= \frac{1}{n} - \ln\left(1 + \frac{1}{n}\right) \\ &\geq 0 \end{aligned}$$

les suites (u_n) et (v_n) sont adjacentes, elles convergent donc vers un réel $\gamma \in \mathbb{R}$. Posons maintenant

$$\forall n \geq 1,\ t_n = u_n - \gamma = H_n - \ln(n) - \gamma$$

Nous allons utiliser le lien entre séries et suites : cherchons un équivalente de la suite $(t_n - t_{n-1})$ pour obtenir un équivalent de la somme partielle de la série de terme général $(t_n - t_{n-1})$ qui n'est autre que la suite (t_n). À l'aide du développement limité de $\ln(1+x)$ en 0 on obtient

$$\begin{aligned} t_n - t_{n-1} &= \ln(n-1) - \ln(n) + \frac{1}{n} \\ &= \ln\left(1 - \frac{1}{n}\right) + \frac{1}{n} \\ &\sim -\frac{1}{2n^2} \end{aligned}$$

D'après le critère de Riemann, la série de terme général $t_k - t_{k-1}$ converge. Le théorème de sommation des équivalents donne l'équivalence des restes. Or, un équivalent du reste de la série de Riemann $\sum \frac{1}{n^2}$ est donné par le Théorème 1 et vaut $\frac{1}{n}$:

$$\sum_{k=n+1}^{+\infty} t_k - t_{k-1} = -t_n \sim \sum_{k=n+1}^{+\infty} -\frac{1}{2k^2} \sim -\frac{1}{2n}$$

D'où $t_n \sim \frac{1}{2n}$ et $H_n = \ln(n) + \gamma + \frac{1}{2n} + o\left(\frac{1}{n}\right)$. On pose alors $\forall n \geq 1$, $w_n = t_n - \frac{1}{2n}$ et on procède de

manière similaire pour obtenir, pour tout $n \geq 2$:

$$\begin{aligned} w_n - w_{n-1} &= \frac{1}{n} + \ln\left(1 - \frac{1}{n}\right) + \frac{1}{2n-2} - \frac{1}{2n} \\ &= \frac{1}{n} - \frac{1}{n} - \frac{1}{2n^2} - \frac{1}{3n^3} + \frac{1}{2n}\frac{1}{1-\frac{1}{n}} - \frac{1}{2n} + o\left(\frac{1}{n^3}\right) \\ &= -\frac{1}{2n^2} + \frac{1}{2n}\left(1 + \frac{1}{n} + \frac{1}{n^2}\right) - \frac{1}{2n} + o\left(\frac{1}{n^3}\right) \\ &= \frac{1}{6n^3} + o\left(\frac{1}{n^3}\right) \end{aligned}$$

On a donc

$$\sum_{k=n+1}^{+\infty} w_k - w_{k-1} = -w_n \sim \frac{1}{2}\frac{1}{6n^2} = \frac{1}{12n^2}$$

d'où le résultat. □

8 Dimension du commutant

Dans ce développement, on montre en se ramenant à la résolution d'un système d'équations linéaires homogène que la dimension du commutant d'une matrice est plus grande que celle de l'espace de départ. On applique ensuite ce résultat pour donner une condition nécessaire et suffisante qui permettant de calculer le commutant de cette matrice.

Soient $\mathbb{K}$ un corps, $n \geq 1$ et $A \in \mathcal{M}_n(\mathbb{K})$.

Notation 1. — On note $\mathcal{T}_n(\mathbb{K})$ l'ensemble des matrices carrées triangulaires supérieures d'ordre n à coefficients dans le corps $\mathbb{K}$.

— On note $\mathscr{C}(A)$ le commutant de A.

Remarque 2. On considère acquis le fait que si $\pi_A = \chi_A$, alors A est cyclique : [GOU21] p. 289

$$\exists x \in \mathbb{K}^n \setminus \{0\} \text{ tel que } (x, Ax, \dots, A^{n-1}x) \text{ est une base de } \mathbb{K}^n$$

Lemme 3. [FGN2] p. 160

$$\dim_{\mathbb{K}}(\mathscr{C}(A)) \geq n$$

Démonstration. Commençons par poser le système d'équations linéaires homogène

$$AX - XA = 0$$

d'inconnue $X = (x_{i,j})_{i,j \in [\![1,n]\!]} \in \mathcal{M}_n(\mathbb{K})$. On note $\mathscr{S}$ l'espace des solutions de ce système.

Plaçons-nous d'abord dans le cas où $A = (a_{i,j})_{i,j \in [\![1,n]\!]} \in \mathcal{T}_n(\mathbb{K})$. Considérons ce système d'équations pour $X \in \mathcal{T}_n(\mathbb{K})$; on a alors $\frac{n(n+1)}{2}$ inconnues dans $\mathbb{K}$. Comme $AX - XA$ est triangulaire supérieure, dire que X est solution revient à écrire $\frac{n(n+1)}{2}$ équations correspondant à la nullité des coefficients de $AX - XA$ dans la partie supérieure. Mais, de ces équations, on peut en retirer n qui sont triviales (celles situées sur la diagonale, de la forme $a_{i,i}x_{i,i} - x_{i,i}a_{i,i}$). Ce système a donc $\frac{n(n+1)}{2} - n$ équations pour seulement $\frac{n(n+1)}{2}$ inconnues. Ainsi,

$$\dim_{\mathbb{K}}(\mathscr{C}(A)) = \dim_{\mathbb{K}}(\mathscr{S}) \geq \dim_{\mathbb{K}}(\mathscr{S} \cap \mathcal{T}_n(\mathbb{K})) \geq \frac{n(n+1)}{2} - \left(\frac{n(n+1)}{2} - n\right) = n$$

Si A n'est pas triangulaire mais est tout de même trigonalisable, il existe $P \in \mathrm{GL}_n(\mathbb{K})$ et $T \in \mathcal{T}_n(\mathbb{K})$ telles que $A = PTP^{-1}$. Ainsi,

$$\begin{aligned} X \in \mathscr{C}(A) &\iff AX = XA \\ &\iff (PTP^{-1})X = X(PTP^{-1}) \\ &\iff T(P^{-1}XP) = (P^{-1}XP)T \\ &\iff P^{-1}XP \in \mathscr{C}(T) \end{aligned}$$

et puisque $X \mapsto P^{-1}XP$ est un isomorphisme de $\mathcal{M}_n(\mathbb{K})$, on a

$$\dim_{\mathbb{K}}(\mathcal{C}(A)) = \dim_{\mathbb{K}}(\mathcal{C}(T))$$

donc on peut tout à fait se ramener au cas où A est triangulaire supérieure.

Enfin, si A n'est pas trigonalisable, on considère $\mathbb{L}$ une extension de $\mathbb{K}$ sur laquelle χ_A est scindé. L'application

$$\varphi : \begin{array}{ccc} \mathcal{M}_n(\mathbb{K}) & \to & \mathcal{M}_n(\mathbb{K}) \\ X & \mapsto & AX - XA \end{array}$$

est linéaire, donc on peut considérer sa matrice $B \in \mathcal{M}_{n^2}(\mathbb{K})$ dans la base canonique de $\mathcal{M}_n(\mathbb{K})$ (il s'agit de la matrice associée au système d'équations linéaires). Alors $\mathcal{S} = \mathrm{Ker}(B)$. Le rang est invariant par extension de corps, donc

$$\mathrm{rang}_{\mathbb{K}}(B) = \mathrm{rang}_{\mathbb{L}}(B)$$

d'où

$$\begin{aligned} \dim_{\mathbb{K}}(\mathcal{S}) &= \dim_{\mathbb{K}}(\mathrm{Ker}(B)) \\ &= n^2 - \mathrm{rang}_{\mathbb{K}}(B) \\ &= n^2 - \mathrm{rang}_{\mathbb{L}}(B) \\ &= \dim_{\mathbb{L}}(\mathrm{Ker}(B)) \\ &\geq n \end{aligned}$$

car A est trigonalisable dans $\mathbb{L}$. D'où le résultat. □

Théorème 4.

$$\mathbb{K}[A] = \mathcal{C}(A) \iff \pi_A = \chi_A$$

Démonstration. Sens direct : Supposons $\mathbb{K}[A] = \mathcal{C}(A)$. Le Théorème 3 entraîne que

$$\deg(\pi_A) = \dim(\mathbb{K}[A]) \geq n$$

Mais comme $\deg(\pi_A) \leq n$, on a $\deg(\pi_A) = n$. Par le théorème de Cayley-Hamilton, on conclut

$$\pi_A = \chi_A$$

Réciproque : On suppose $\pi_A = \chi_A$. Par la Théorème 2, on peut trouver $x \in\in \mathbb{K}^n \setminus \{0\}$ tel que $(x, Ax, \dots, A^{n-1}x)$ est une base de $\mathbb{K}^n$. Ainsi, l'application

$$\varphi : \begin{array}{ccc} \mathcal{C}(A) & \to & \mathbb{K}^n \\ B & \mapsto & Bx \end{array}$$

est linéaire injective. En effet, si $B \in \mathrm{Ker}(\varphi)$, alors

$$\forall k \in [\![0, n-1]\!],\ BA^k x = A^k Bx = 0 \implies B = 0$$

car B s'annule sur une base de $\mathbb{K}^n$. D'où $\dim(\mathscr{C}(A)) \leq \dim(\mathbb{K}^n) = n$. On déduit à l'aide du Théorème 3 que

$$\dim(\mathscr{C}(A)) = n$$

Notons de plus que

$$\dim(\mathbb{K}[A]) = \deg(\pi_A) = \deg(\chi_A) = n$$

et comme $\mathbb{K}[A] \subseteq \mathscr{C}(A)$ (car tout polynôme en A commute avec A), on a bien le résultat. □

9 Dual de L_p

Avec les propriétés hilbertiennes de L_2 couplées à certaines propriétés des espaces L_p, on montre que le dual d'un espace L_p est L_q pour $\frac{1}{p}+\frac{1}{q}=1$, dans le cas où $p\in]1,2[$ et où l'espace est de mesure finie.

Soit $(X,\mathscr{A},\mu)$ un espace mesuré de mesure finie.

Notation 1. On note $\forall p\in]1,2[$, $L_p = L_p(X,\mathscr{A},\mu)$.

Lemme 2. Soient $p\in]1,2[$ et $f\in L_2$. Alors $f\in L_p$ telle que $\|f\|_p \leq M\|f\|_2$ où $M\geq 0$.

Démonstration. Comme $p\in]1,2[$, on a $\frac{2}{p}>1$. Soit r tel que $\frac{p}{2}+\frac{1}{r}=1$. On applique l'inégalité de Hölder à $g=|f|^p\mathbb{1}_X$ de sorte que

$$\int_X |f|^p\,\mathrm{d}\mu = \||f|^p\mathbb{1}_X\|_1 \leq \||f|^p\|_{\frac{2}{p}}\|\mathbb{1}_X\|_r \leq \mu(X)^{\frac{1}{r}}\|f\|_2^p$$

d'où le résultat. □

Lemme 3. Soit $p\in]1,2[$. Alors L_2 est dense dans L_p pour la norme $\|.\|_p$.

Démonstration. Soit $f\in L_p$. On considère la suite de fonction (f_n) définie par

$$\forall n\in\mathbb{N},\ f_n = f\mathbb{1}_{|f|\leq n}$$

Clairement, (f_n) est une suite de L_2. On va chercher à appliquer le théorème de convergence dominée à la suite de fonctions (g_n) définie pour tout $n\in\mathbb{N}$ par $g_n=|f_n-f|^p$:

— $\forall n\in\mathbb{N}$, g_n est mesurable.

— (g_n) converge presque partout vers la fonction nulle.

— Par convexité de la fonction $x\mapsto x^p$, on a

$$|f_n-f|^p = 2^p\left|\frac{f_n}{2}-\frac{f}{2}\right|^p \leq 2^{p-1}(|f|^p+|f_n|^p) \leq 2^p|f|^p\in L_1$$

On peut donc conclure

$$\|f-f_n\|_p^p = \int_X |f-f_n|^p\,\mathrm{d}\mu \longrightarrow 0$$

ce qu'il fallait démontrer. □

Théorème 4. L'application

$$\varphi : \begin{array}{ccc} L_q & \to & (L_p)' \\ g & \mapsto & \left(\varphi_g : f\mapsto \int_X f\overline{g}\,\mathrm{d}\mu\right)\end{array} \qquad \text{où } \frac{1}{p}+\frac{1}{q}=1$$

[Z-Q] p. 222

est une isométrie linéaire surjective. C'est donc un isomorphisme isométrique.

Démonstration. Soient $g \in L_q$ et $f \in L_p$. L'inégalité de Hölder donne

$$|\varphi_g(f)| \leq \|g\|_q \|f\|_p$$

donc $\varphi_g \in (L_p)'$ et $|||\varphi_g||| \leq \|g\|_q$. De plus, si $g = 0$, alors $|||\varphi_g||| = \|g\|_q = 0$. On peut donc supposer $g \neq 0$.

Soit u une fonction mesurable de module 1, telle que $g = u|g|$. On pose $h = \overline{u}|g|^{q-1}$. Comme $q = p(q-1)$, on a

$$\int_X |h|^p \,\mathrm{d}\mu = \int_X |g|^{(q-1)p} \,\mathrm{d}\mu = \int_X |g|^q \,\mathrm{d}\mu < +\infty$$

d'où $h \in L_p$ et $\|h\|_p^p = \|g\|_q^q = |\varphi_g(h)|$. Comme, $\frac{|\varphi_g(h)|}{\|h\|_p} \leq |||\varphi_g|||$, on a en particulier,

$$\underbrace{\int_X |g|^q \,\mathrm{d}\mu}_{=|\varphi_g(h)|} \leq |||\varphi_g||| \underbrace{\left(\int_X |g|^q \,\mathrm{d}\mu\right)^{\frac{1}{p}}}_{=\|h\|_p}$$

et ainsi,

$$|||\varphi_g||| \geq \left(\int_X |g|^q \,\mathrm{d}\mu\right)^{1-\frac{1}{p}} = \left(\int_X |g|^q \,\mathrm{d}\mu\right)^{\frac{1}{q}} = \|g\|_q$$

donc $|||\varphi_g||| = \|g\|_q$ et φ est une isométrie.

Montrons qu'elle est surjective. Soit $\ell \in (L_p)'$. D'après le Théorème 2, on a $L_2 \subseteq L_p$, donc on peut considérer la restriction $\widetilde{\ell} = \ell_{|L_2}$.

$$\forall f \in L_2, \quad |\widetilde{\ell}(f)| \leq |||\ell||| \|f\|_p \leq M \|\ell\| \|f\|_2 \implies \widetilde{\ell} \in (L_2)'$$

Comme L_2 est un espace de Hilbert, on peut appliquer le théorème de représentation de Riesz à $\widetilde{\ell}$. Il existe $g \in L_2$ telle que

$$\forall f \in L_2, \quad \widetilde{\ell}(f) = \int_X f\overline{g} \,\mathrm{d}\mu$$

Pour conclure, il reste à montrer que $g \in L_q$ et que l'égalité précédente est vérifiée sur L_p. Comme précédemment, on considère u de module 1 telle que $g = u|g|$ et on pose $f_n = \overline{u}|g|^{q-1}\mathbb{1}_{|g|\leq n} \in L_\infty \subseteq L_2$. On a

$$\int_X |g|^q \mathbb{1}_{|g|\leq n} \,\mathrm{d}\mu = |\ell(f_n)| \leq \|\ell\| \|f_n\|_p = \|\ell\| \left(\int_X |g|^q \mathbb{1}_{|g|\leq n} \,\mathrm{d}\mu\right)^{\frac{1}{p}}$$

D'où

$$\left(\int_X |g|^q \mathbb{1}_{|g|\leq n} \,\mathrm{d}\mu\right)^{\frac{1}{q}} = \left(\int_X |g|^q \mathbb{1}_{|g|\leq n} \,\mathrm{d}\mu\right)^{1-\frac{1}{p}} \leq |||\ell|||$$

D'après le théorème de convergence monotone, on a

$$\lim_{n\to+\infty} \left(\int_X |g|^q \mathbb{1}_{|g|\leq n} \,\mathrm{d}\mu\right)^{\frac{1}{q}} = \left(\int_X |g|^q \,\mathrm{d}\mu\right)^{\frac{1}{q}} \leq |||\ell|||$$

Et en particulier, $g \in L_q$ de norme inférieure ou égale à $|||\ell|||$. Ainsi, on a $\forall f \in L_2$, $\ell(f) = \varphi_g(f)$. Les applications ℓ et φ_g sont continues sur L_p et L_2 est dense dans L_p (par le Théorème 3), donc on a bien $\ell = \varphi_g = \varphi(g)$. □

Remarque 5. Plus généralement, si l'on identifie g et φ_g :

— L_q est le dual topologique de L_p pour $p \in]1, +\infty[$.

— L_∞ est le dual topologique de L_1 si μ est σ-finie.

[LI] p. 140

10 Équation de Sylvester

On montre que l'équation $AX + XB = C$ d'inconnue X admet une unique solution pour tout $C \in \mathcal{M}_n(\mathbb{C})$ et pour tout $A, B \in \mathcal{M}_n(\mathbb{C})$ dont les valeurs propres sont de partie réelle strictement négative.

Lemme 1. Soit $\|.\|$ une norme d'algèbre sur $\mathcal{M}_n(\mathbb{C})$, et soit $A \in \mathcal{M}_n(\mathbb{C})$ une matrice dont les valeurs propres sont de partie réelle strictement négative. Alors il existe une fonction polynômiale $P : \mathbb{R} \to \mathbb{R}$ et $\lambda > 0$ tels que $\|e^{tA}\| \leq e^{-\lambda t} P(t)$. [GOU21] p. 200

Démonstration. On fait la décomposition de Dunford de A : $A = D+N$. Comme D et N commutent, on a $e^{tA} = e^{tD}e^{tN}$. Soient P la matrice de passage donnée par la base de diagonalisation de D et $\lambda_1, \dots, \lambda_n$ ses valeurs propres. En notant $|||.|||$ la norme subordonnée à $\|.\|_\infty$ sur $\mathbb{C}^n$, on a $\forall t \geq 0$,

$$\begin{aligned}
|||e^{tD}||| &= |||e^{tP\,\mathrm{Diag}(\lambda_1,\dots,\lambda_n)P^{-1}}||| \\
&= |||Pe^{t\,\mathrm{Diag}(\lambda_1,\dots,\lambda_n)}P^{-1}||| \\
&\leq \underbrace{|||P|||\,|||P^{-1}|||}_{=\alpha} \sup_{\|x\|_\infty=1} \|\mathrm{Diag}(e^{t\lambda_1},\dots,e^{t\lambda_n})x\|_\infty \\
&\leq \alpha \sup_{i\in[\![1,n]\!]} |e^{t\lambda_i}| \\
&\leq \alpha e^{-\lambda t}
\end{aligned}$$

où $\lambda > 0$ par hypothèse. En dimension finie, toutes les normes sont équivalentes, donc il existe $\beta > 0$ tel que $|||e^{tD}||| \leq \beta e^{-\lambda t}$.

Pour conclure, en notant r l'indice de nilpotence de N,

$$\begin{aligned}
\|e^{tA}\| &\leq \|e^{tD}\|\,\|e^{tN}\| \\
&\leq e^{-\lambda t} \underbrace{\sum_{k=0}^{r-1} \beta \frac{\|N\|^k t^k}{k}}_{=P(t)}
\end{aligned}$$

□

Théorème 2 (Équation de Sylvester)**.** Soient A et $B \in \mathcal{M}_n(\mathbb{C})$ deux matrices dont les valeurs propres sont de partie réelle strictement négative. Alors pour tout $C \in \mathcal{M}_n(\mathbb{C})$, l'équation $AX + XB = C$ admet une unique solution X dans $\mathcal{M}_n(\mathbb{C})$. [I-P] p. 177

Démonstration. Comme l'application $\varphi : X \mapsto AX + XB$ est un endomorphisme de $\mathcal{M}_n(\mathbb{C})$, qui est un espace vectoriel de dimension finie, il suffit de montrer qu'elle est surjective pour obtenir l'injectivité (et donc l'unicité de la solution). Soit $C \in \mathcal{M}_n(\mathbb{C})$. On considère le problème de Cauchy suivant d'inconnue $Y : \mathbb{R} \to \mathcal{M}_n(\mathbb{C})$:

$$\begin{cases} Y' = AY + YB \\ Y(0) = C \end{cases} \tag{E}$$

Il s'agit d'une équation différentielle linéaire à coefficients constants (on peut voir cela notamment en calculant les produits AY et YB et en effectuant la somme ; l'égalité matricielle avec Y' donnant le système d'équations voulu). D'après le théorème de Cauchy-Lipschitz linéaire, (E) admet une unique solution définie sur $\mathbb{R}$ tout entier, que l'on note Y.

On vérifie que la solution est définie $\forall t \in \mathbb{R}$ par $Y(t) = \exp(tA)C\exp(tB)$. En effet pour tout $t \in \mathbb{R}$, on a :

$$Y'(t) = A\exp(tA)C\exp(tB) + \exp(tA)CB\exp(tB) = AY + YB$$

car toute matrice M commute avec son exponentielle (puisque $\exp(M)$ est limite d'un polynôme en M) et donc M commute aussi avec $\exp(tM)$ pour tout $t \in \mathbb{R}$.

On va maintenant montrer que $X = -\int_0^{+\infty} Y(s)\,\mathrm{d}s$ est la solution de l'équation de Sylvester. Pour tout $t \geq 0$, on intègre Y' entre 0 et t pour obtenir :

$$Y(t) - C = \int_0^t Y'(s)\,\mathrm{d}s = A \times \int_0^t Y(s)\,\mathrm{d}s + \int_0^t Y(s)\,\mathrm{d}s \times B$$

Il ne reste donc plus qu'à montrer que $Y(t) \longrightarrow 0$ et que Y est intégrable pour conclure. Par le Théorème 1, il existe $\lambda_1, \lambda_2 > 0$ et $P_1, P_2 : \mathbb{R} \to \mathbb{R}$ polynômiales tels que $\|e^{tA}\| \leq e^{-\lambda_1 t}P_1(t)$ et $\|e^{tB}\| \leq e^{-\lambda_2 t}P_2(t)$ pour tout $t \geq 0$. Ainsi, en posant $\lambda = \max(\lambda_1, \lambda_2)$ et $P = P_1P_2$, comme $\|.\|$ est une norme d'algèbre :

$$\|Y(t)\| = \|e^{tA}Ce^{tB}\| \leq \|C\|P(t)e^{-2\lambda t}$$

En particulier, on a bien $Y(t) \longrightarrow 0$. De plus, comme $\|C\|P(t)e^{-2\lambda t}$ est intégrable sur $[0, +\infty[$ et domine $\|Y(t)\|$, alors Y est aussi intégrable $[0, +\infty[$. Finalement, en faisant $t \longrightarrow +\infty$, on obtient :

$$-C = A \times \int_0^{+\infty} Y(s)\,\mathrm{d}s + \int_0^{+\infty} Y(s)\,\mathrm{d}s \times B$$

Donc $\varphi(X) = C$: φ est surjective et X est bien la solution de l'équation de Sylvester. □

Remarque 3. Pour dire que toute matrice M commute avec $\exp(M)$, on aurait simplement pu dire que $\exp(M)$ est un polynôme en M ie. $\forall M \in \mathcal{M}_n(\mathbb{C}), \exists P \in \mathbb{C}[X]$ tel que $\exp(M) = P(M)$.

[GOU21] p. 189

Démonstration. Soit $M \in \mathcal{M}_n(\mathbb{C})$. L'ensemble $\mathbb{C}[M] = \{P(M) \mid P \in \mathbb{C}[X]\}$ est un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{C})$ qui est de dimension finie, donc $\mathbb{C}[M]$ l'est aussi et est en particulier fermé.

Pour tout $n \in \mathbb{N}$, on pose $P_n = \sum_{k=0}^{n} \frac{M^k}{k!} \in \mathbb{C}[M]$ de sorte que $P_n \longrightarrow_{n\to+\infty} \exp(M)$. Comme $\mathbb{C}[M]$ est fermé, on en déduit que $\exp(M) \in \mathbb{C}[M]$. Donc $\exists P \in \mathbb{C}[X]$ tel que $\exp(M) = P(M)$. □

11 Équivalence des normes en dimension finie et théorème de Riesz

On montre l'équivalence des normes en dimension finie ainsi que le théorème de Riesz sur la compacité de la boule unité fermée toujours en dimension finie, qui sont deux résultats fondamentaux sur les espaces vectoriels normés.

Lemme 1. Les compacts de $(\mathbb{R}^n, \|.\|_\infty)$ sont les fermés bornés.

[I-P] p. 422

Démonstration. Soit X une partie fermée bornée de $\mathbb{R}^n$. Soit (x_n) une suite de X. On note $\forall k \in \mathbb{N}$, $\forall i \in [\![1,n]\!]$, x_k^i la i-ième composante du vecteur x_k. Comme X est bornée, alors $(\|x_n\|_\infty)$ est une suite réelle bornée. Montrons par récurrence que, pour tout $k \in [\![1,n]\!]$, il existe des extractrices $\varphi_1, \dots, \varphi_i$ telle que la suite réelle $(x^i_{\varphi_1 \circ \dots \circ \varphi_i(n)})$ converge pour tout $i \in [\![1,k]\!]$.

— Pour $k = 1$, c'est une réécriture du théorème de Bolzano-Weierstrass.

— Pour $k > 1$, supposons avoir construit $\varphi_1, \dots, \varphi_k$ telles que $(x^i_{\varphi_1 \circ \dots \circ \varphi_k(n)})$ converge pour tout $i \in [\![1,k]\!]$. Comme

$$|x_n^{k+1}| \leq \|x_n\|_\infty$$

$(x^{k+1}_{\varphi_1 \circ \dots \circ \varphi_k(n)})$ est une suite réelle bornée. Toujours par le théorème de Bolzano-Weierstrass, il existe une extractrice φ_{k+1} telle que $(x^{k+1}_{\varphi_1 \circ \dots \circ \varphi_{k+1}}(n))$ converge. D'où l'hérédité.

La propriété est en particulier vraie pour $k = n$. En posant $\varphi = \varphi_1 \circ \dots \circ \varphi_n$, on obtient une extractrice telle que

$$\forall i \in [\![1,n]\!], (x^i_{\varphi(n)}) \text{ converge}$$

et on en déduit que $(x_{\varphi(n)})$ converge vers un réel $x \in \mathbb{R}^n$. Comme X est fermé, $x \in X$. X est donc séquentiellement compact, donc compact. □

Proposition 2. Soient (E, d_E), (F, d_F) deux espaces métriques et $f : E \to F$ continue. Si E est compact, alors $f(E)$ est compact dans F.

Démonstration. Soit (y_n) une suite d'éléments de $f(E)$. On pose $\forall n \in \mathbb{N}$, $x_n = f(y_n)$. E est compact, donc il existe une extractrice $\varphi : \mathbb{N} \to \mathbb{N}$ telle que $x_{\varphi(n)} \longrightarrow_{n \to +\infty} x$ où $x \in E$. Par continuité,

$$y_{\varphi(n)} = f(x_{\varphi(n)}) \longrightarrow_{n \to +\infty} f(x) \in f(E)$$

$f(E)$ est ainsi séquentiellement compact, donc est compact. □

Théorème 3. Soit E un espace vectoriel sur le corps $\mathbb{R}$ de dimension finie $n \in \mathbb{N}$. Alors, toutes les normes sur E sont équivalentes.

Démonstration. Soient $\mathcal{B} = (e_1, \dots, e_n)$ une base de E. On définit la norme infinie $\mathcal{N}_\infty$ associée à

la base $\mathscr{B}$ pour tout $x = \sum_{i=1}^{n} x_i e_i \in E$ par

$$\mathcal{N}_\infty : x \mapsto \max_{i \in [\![1,n]\!]} |x_i|$$

Si $\mathcal{N}$ est une norme sur E, on a :

$$\mathcal{N}(x) \leq \underbrace{\left(\sum_{i=1}^{n} \mathcal{N}(e_i)\right)}_{=\alpha} \mathcal{N}_\infty(x)$$

Donc $\mathcal{N}_\infty$ est plus fine que $\mathcal{N}$.

Définissons l'isomorphisme suivant :

$$f : \begin{array}{ccc} (\mathbb{R}^n, \|.\|_\infty) & \to & (E, \mathcal{N}) \\ (x_1, \dots, x_n) & \mapsto & \sum_{i=1}^{n} x_i e_i \end{array}$$

La fonction f vérifie

$$\forall x \in \mathbb{R}^n, \mathcal{N}(f(x)) \leq \alpha \|x\|_\infty$$

c'est une application linéaire bornée, qui est donc continue. On considère l'ensemble

$$S_E = f(S)$$

où S désigne la sphère unité de $(\mathbb{R}^n, \|.\|_\infty)$ qui est compacte d'après le Théorème 1. D'après le Théorème 2, S_E est compacte comme image d'un compact par une application continue.

Montrons que S_E est la sphère unité de $(E, \mathcal{N}_\infty)$. Déjà, si $x \in S$, alors $\mathcal{N}_\infty(f(x)) = \|x\|_\infty = 1$, d'où l'inclusion directe. Pour l'inclusion réciproque, si $y \in S_E$, par bijectivité de f, on peut écrire $y = f^{-1}(x)$ avec $x \in \mathbb{R}^n$ et ainsi $\|x\|_\infty = \mathcal{N}_\infty(f(x)) = 1$.

L'application $\mathcal{N} : E \to \mathbb{R}$ est continue car lipschitzienne ($\forall x, y \in E, |\mathcal{N}(x) - \mathcal{N}(y)| \leq \mathcal{N}(x - y)$), donc est bornée et atteint ses bornes sur la sphère S_E. On note $x_0 \in E$ ce minimum :

$$\forall x \in E \text{ tel que } \mathcal{N}_\infty(x) = 1, \text{ on a } \mathcal{N}(x) \geq \underbrace{\mathcal{N}(x_0)}_{=\beta}$$

Ainsi,

$$\forall x \in E, \mathcal{N}\left(\frac{x}{\mathcal{N}_\infty(x)}\right) \geq \beta \text{ ie. } \mathcal{N}(x) \geq \beta \mathcal{N}_\infty(x)$$

Donc $\mathcal{N}$ est plus fine que $\mathcal{N}_\infty$: les normes $\mathcal{N}$ et $\mathcal{N}_\infty$ sont équivalentes. Comme la relation d'équivalence sur les normes d'un espace vectoriel est transitive, on en déduit que toutes les normes sur E sont équivalentes. □

Théorème 4 (Riesz)**.** Soit $(E, \|.\|)$ un espace vectoriel normé sur le corps $\mathbb{R}$. Alors, E est de dimension finie si et seulement si sa boule unité fermée est compacte.

Démonstration. Notons $\overline{B}$ la boule unité fermée de E et supposons E de dimension finie $n \in \mathbb{N}$. Comme dans la démonstration du théorème précédent, $\overline{B}$ est compacte comme image de la

boule unité fermée de $(\mathbb{R}^n, \|.\|_\infty)$ par l'application continue f. Réciproquement, supposons E de dimension finie et, par l'absurde, également que $\overline{B}$ est compacte. On a,

$$\overline{B} \subseteq \bigcup_{x \in E} B(x,1)$$

où $B(x,1)$ désigne la boule ouverte centrée en x de rayon 1. Par la propriété de Borel-Lebesgue, il existe $x_1, \dots, x_n \in E$ tels que

$$\overline{B} \subseteq \bigcup_{i=1}^{n} B(x_i,1)$$

On définit $F = \text{Vect}(x_1, \dots, x_n)$. Comme F est de dimension finie et E de dimension infinie, on peut trouver $y \in E \setminus F$. Soit $x_0 \in F$ le projeté de y sur F :

$$d(y,F) = \|y - x_0\| > 0$$

On pose

$$u = \frac{y - x_0}{\|y - x_0\|}$$

On a u de norme 1, donc $u \in \overline{B}$ et il existe $i \in [\![1,n]\!]$ tel que $\|u - x_i\| < 1$. Or,

$$\begin{aligned}
\|u - x_i\| &= \frac{\|y - x_0 - \|y - x_0\| x_i\|}{\|y - x_0\|} \\
&= \frac{\|y - (x_0 - \|y + x_0\| x_i)\|}{\|y - x_0\|} \\
&\geq \frac{d(y,F)}{\|y - x_0\|} \\
&= 1
\end{aligned}$$

car $x_0 + \|y - x_0\| x_i \in F$: absurde. □

12 Formes de Hankel

Le but de ce développement est de construire une forme quadratique permettant de dénombrer les racines réelles distinctes d'un polynôme en fonction de ses racines complexes.

Soit $P \in \mathbb{R}[X]$ un polynôme de degré n.

[C-G] p. 356

Théorème 1 (Formes de Hankel)**.** On note $x_1, \dots, x_t$ les racines complexes de P de multiplicités respectives $m_1, \dots, m_t$. On pose

$$s_0 = n \text{ et } \forall k \geq 1,\ s_k = \sum_{i=1}^{t} m_i x_i^k$$

Alors :

(i) $\sigma = \sum_{i,j \in [\![0,n-1]\!]} s_{i+j} X_i X_j$ définit une forme quadratique sur $\mathbb{C}^n$ ainsi qu'une forme quadratique $\sigma_{\mathbb{R}}$ sur $\mathbb{R}^n$.

(ii) Si on note (p,q) la signature de $\sigma_{\mathbb{R}}$, on a :

— $t = p + q$.

— Le nombre de racines réelles distinctes de P est $p - q$.

Démonstration. σ est un polynôme homogène de degré 2 sur $\mathbb{C}$ (car la somme des exposants est 2 pour chacun des monômes), qui définit donc une forme quadratique sur $\mathbb{C}^n$. De plus, on peut écrire :

$$\forall k \geq 1,\ s_k = \sum_{\substack{x_i \text{ racine de P} \\ x_i \in \mathbb{R}}} m_i x^i + \sum_{\substack{x \text{ racine de P} \\ x_i \in \mathbb{C}}} m_i (x^i + \overline{x}^k)$$

donc $s_k = \overline{s_k}$ ie. $s_k \in \mathbb{R}$. Donc σ définit une forme quadratique $\sigma_{\mathbb{R}}$ sur $\mathbb{R}^n$. D'où le premier point.

Soit φ_k la forme linéaire sur $\mathbb{C}^n$ définie par le polynôme homogène de degré 1

$$P_k(X_0, \dots, X_{n-1}) = X_0 + x_k X_1 + \cdots + x_k^{n-1} X_{n-1}$$

pour $k \in [\![0,t]\!]$. Dans la base duale $(e_i^*)_{i \in [\![0,n-1]\!]}$ de la base canonique $(e_i)_{i \in [\![0,n-1]\!]}$ de $\mathbb{C}^n$, on a

$$\varphi_k = e_0^* + x_k e_1^* + \cdots + x_k^{n-1} e_{n-1}^*$$

Et comme

$$\det((\varphi_k)_{k \in [\![0,t]\!]}) = \begin{vmatrix} 1 & 1 & \dots & 1 \\ x_0 & x_1 & \dots & x_t \\ \vdots & \ddots & \ddots & \vdots \\ x_0^{n-1} & x_1^{n-1} & \dots & x_t^{n-1} \end{vmatrix} \overset{\text{Vandermonde}}{\neq} 0$$

la famille $(\varphi_k)_{k \in [\![0,t]\!]}$ est de rang t sur $\mathbb{C}$. Or, le coefficient de $X_i X_j$ dans $\sum_{k=1}^t m_k P_k^2$ vaut

$$\begin{cases} \sum_{k=1}^t m_k x_k^{2i} = s_{i+j} & \text{si } i = j \\ \sum_{k=1}^t 2 m_k x_k^i x_k^j = \sum_{k=1}^t 2 m_k x_k^{i+j} = 2 s_{i+j} & \text{sinon} \end{cases}$$

donc, $\sigma = \sum_{k=1}^{t} m_k \varphi_k^2$. En particulier, $\operatorname{rang}(\sigma) = t$ par indépendance des φ_k. On en déduit,

$$p + q = \operatorname{rang}(\sigma_{\mathbb{R}}) = \operatorname{rang}(\sigma) = t$$

(le rang est invariant par extension de corps).

Soit $k \in [\![0, t]\!]$. Calculons la signature de la forme quadratique $\varphi_k^2 + \overline{\varphi_k}^2$:

— Si $x_k \in \mathbb{R}$, on a $\varphi_k^2 + \overline{\varphi_k}^2 = 2\varphi_k^2$, qui est de signature $(1,0)$ car $\varphi_k \neq 0$.

— Si $x_k \notin \mathbb{R}$, on a $\varphi_k^2 + \overline{\varphi_k}^2 = 2\operatorname{Re}(\varphi_k)^2 - 2\operatorname{Im}(\varphi_k)^2$ qui est bien une forme quadratique réelle. Et $x_k \neq \overline{x_k}$, donc la matrice

$$\begin{pmatrix} 1 & 1 \\ x_k & \overline{x_k} \\ \vdots & \vdots \\ x_k^{n-1} & \overline{x_k}^{n-1} \end{pmatrix}$$

est de rang 2 (cf. le mineur correspondant aux deux premières lignes). Donc φ_k et $\overline{\varphi_k}$ sont indépendantes. Ainsi, $\operatorname{rang}(\varphi_k^2 + \overline{\varphi_k}^2) = 2$ sur $\mathbb{C}$, donc sur $\mathbb{R}$ aussi (toujours par invariance du rang par extension de corps). Donc la signature de $\varphi_k^2 + \overline{\varphi_k}^2$ est $(1,1)$.

Maintenant, regroupons les φ_k conjuguées entre elles lorsqu'elles ne sont pas réelles :

$$\sigma = \sum_{\substack{k=1 \\ x_k \in \mathbb{R}}}^{t} m_k \varphi_k^2 + \sum_{\substack{k=1 \\ x_k \notin \mathbb{R}}}^{t} m_k (\varphi_k^2 + \overline{\varphi_k}^2)$$

En passant à la signature, on obtient :

$$(p,q) = (r,0) + \left(\frac{t-r}{2}, \frac{t-r}{2}\right) = \left(\frac{t+r}{2}, \frac{t-r}{2}\right)$$

où r désigne le nombre de racines réelles distinctes de P. Par unicité de la signature d'une forme quadratique réelle, on a bien $p - q = r$. D'où le point (ii). □

Remarque 2. Tout l'intérêt de ces formes quadratiques est qu'on peut calculer les s_k par récurrence en utilisant les polynômes symétriques élémentaires, sans avoir besoin des racines.

Proposition 3 (Sommes de Newton)**.** On pose $P = \sum_{k=0}^{n} a_k X^k$. Les sommes de Newton vérifient les relations suivantes :

(i) $s_0 = n$.

(ii) $\forall k \in [\![1, n-1]\!]$, $s_k = -k a_{n-k} \sum_{i=1}^{k-1} s_i a_{n-k+i}$.

(iii) $\forall p \in \mathbb{N}$, $s_{p+n} = \sum_{i=1}^{n} s_i a_{p+n-i}$.

[GOU21] p. 86

13 Formule de Stirling

Dans ce développement un peu technique, nous démontrons la formule de Stirling $n! \sim \sqrt{2n\pi}\left(\frac{n}{e}\right)^n$ *à l'aide du théorème central limite et de la fonction* Γ *d'Euler.*

Lemme 1. Soit Y une variable aléatoire réelle à densité. Alors $\forall n \geq 1$, $\frac{Y-n}{\sqrt{n}}$ est à densité et,

$$f_{\frac{Y-n}{\sqrt{n}}}(x) = \sqrt{n} f_Y(n + x\sqrt{n}) \text{ pp. en } x \in \mathbb{R}$$

Démonstration. $\forall x \in \mathbb{R}$,

$$\begin{aligned} F_{\frac{Y-n}{\sqrt{n}}}(x) &= \mathbb{P}\left(\frac{Y-n}{\sqrt{n}} \leq x\right) \\ &= \mathbb{P}(Y \leq x\sqrt{n} + n) \\ &= F_Y(x\sqrt{n} + n) \end{aligned}$$

Or, la fonction de répartition d'une variable aléatoire réelle à densité est dérivable presque partout, et sa dérivée est presque partout égale à sa densité. Donc :

$$f_{\frac{Y-n}{\sqrt{n}}}(x) = \sqrt{n} f_Y(x\sqrt{n} + n) \text{ pp. en } x \in \mathbb{R}$$

□

Remarque 2. Il ne s'agit ni plus ni moins qu'une version affaiblie du théorème de changement de variable.

Lemme 3. Soient X et Y deux variables aléatoires indépendantes telles que $X \sim \Gamma(a,\gamma)$ et $Y \sim \Gamma(b,\gamma)$. Alors $Z = X + Y \sim \Gamma(a+b,\gamma)$.

[G-K] p. 180

Démonstration. Soit $f_{a,\gamma} : x \mapsto \frac{\gamma^a}{\Gamma(a)} x^{a-1} e^{-\gamma x} \mathbb{1}_{\mathbb{R}^+}(x)$ la densité de la loi $\Gamma(a,\gamma)$. $\forall x \geq 0$, on a :

$$\begin{aligned} f_Z(x) &= \int_0^x f_{a,\gamma}(t) f_{b,\gamma}(x-t)\,\mathrm{d}t \\ &= \int_0^x \frac{\gamma^a}{\Gamma(a)} t^{a-1} e^{-\gamma t} \frac{\gamma^b}{\Gamma(b)} (x-t)^{b-1} e^{-\gamma(x-t)}\,\mathrm{d}t \\ &= \frac{\gamma^{a+b} e^{-\gamma x}}{\Gamma(a)\Gamma(b)} \int_0^x t^{a-1}(x-t)^{b-1}\,\mathrm{d}t \\ &\overset{t=ux}{=} \frac{\gamma^{a+b} e^{-\gamma x}}{\Gamma(a)\Gamma(b)} x^{a+b-1} \int_0^1 u^{a-1}(1-u)^{b-1}\,\mathrm{d}t \\ &= K_{a,b} f_{a+b,\gamma}(x) \end{aligned}$$

où $K_{a,b} = \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)} \int_0^1 u^{a-1}(1-u)^{b-1}\,\mathrm{d}u$. Notons par ailleurs que f_Z est nulle sur $\mathbb{R}^-$ et coïncide donc avec $K_{a,b} f_{a+b,\gamma}$ sur $\mathbb{R}^-$.

Pour conclure, on utilise la condition de normalisation :

$$1 = \int_{\mathbb{R}} f_Z(x)\,\mathrm{d}x = K_{a,b} \int_{\mathbb{R}} f_{a+b,\gamma}(x)\,\mathrm{d}x = K_{a,b}$$

On obtient ainsi $f_Z = f_{a+b,\gamma}$, ce que l'on voulait. □

p. 556

Théorème 4 (Formule de Stirling)**.**

$$n! \sim \sqrt{2n\pi}\left(\frac{n}{e}\right)^n$$

Démonstration. Soit (X_n) une suite de variable aléatoires indépendantes de même loi $\mathscr{E}(1)$. On pose $S_n = \sum_{k=0}^n X_k$. Montrons par récurrence que $S_n \sim \Gamma(n+1,1)$.

— Pour $n = 0$: c'est clair car $\mathscr{E}(1) = \Gamma(1,1)$.

— On suppose le résultat vrai à un rang $n \geq 0$. Pour montrer qu'il reste vrai au rang $n+1$, il suffit d'appliquer le Théorème 3 à $S_n \sim \Gamma(n,1)$ et $X_{n+1} \sim \Gamma(1,1)$ (qui sont bien indépendantes).

Par le Théorème 1 appliqué à S_n, pp. en $x \in \mathbb{R}$,

$$\begin{aligned}
\overbrace{f_{\frac{S_n-n}{\sqrt{n}}}(x)}^{=g_n(x)} &= \sqrt{n} f_{S_n}(n + x\sqrt{n}) \\
&= \frac{\sqrt{n}}{\Gamma(n+1)} n^n \left(1 + \frac{x}{\sqrt{n}}\right)^n e^{-(n+x\sqrt{n})} \mathbb{1}_{[-\sqrt{n},+\infty[}(x) \\
&= a_n h_n(x)
\end{aligned}$$

avec :

— $a_n = \frac{n^{n+\frac{1}{2}} e^{-n}\sqrt{2\pi}}{\Gamma(n+1)}$ (ce qui nous intéresse).

— $h_n : x \mapsto \frac{e^{-\sqrt{n}x}}{\sqrt{2\pi}} \left(1 + \frac{x}{\sqrt{n}}\right)^n \mathbb{1}_{[-\sqrt{n},+\infty[}(x)$ (ce qui nous intéresse moins).

Montrons maintenant que $\frac{S_n-n}{\sqrt{n}}$ converge en loi vers $\mathscr{N}(0,1)$. D'après le théorème central limite,

$$\frac{S_n - \mathbb{E}(S_n)}{\sqrt{\mathrm{Var}(S_n)}} \xrightarrow{(d)} \mathscr{N}(0,1)$$

où :

— $\mathbb{E}(S_n) = (n+1)\mathbb{E}(X_0) = n+1$.

— $\mathrm{Var}(S_n) = (n+1)\,\mathrm{Var}(X_0) = n+1$ par indépendance.

On applique maintenant le théorème de Slutsky :

$$\frac{S_n - n}{\sqrt{n}} = \underbrace{\frac{\sqrt{n+1}}{\sqrt{n}}}_{\longrightarrow 1}\left(\underbrace{\frac{S_n-(n+1)}{\sqrt{n+1}}}_{\xrightarrow{(d)}\mathcal{N}(0,1)} + \underbrace{\frac{1}{\sqrt{n+1}}}_{\longrightarrow 0}\right) \xrightarrow{(d)} \mathcal{N}(0,1)$$

Tout cela pour dire que,

$$\int_0^1 g_n(x)\,\mathrm{d}x = \mathbb{P}\left(\frac{S_n-n}{\sqrt{n}} \in [0,1]\right) \longrightarrow \int_0^1 \frac{e^{-\frac{x^2}{2}}}{\sqrt{2\pi}}\,\mathrm{d}x$$

De plus :

— $\forall n \in \mathbb{N}$, h_n est mesurable.

— $\forall x \in \mathbb{R}$, $h_n(x) = \frac{e^{-x^2\varphi\left(\frac{x}{\sqrt{n}}\right)}}{\sqrt{2\pi}} \mathbb{1}_{]-1,+\infty[}\left(\frac{x}{\sqrt{n}}\right)$ où $\forall x > -1$, $\varphi(x) = \frac{x-\ln(1+x)}{x^2}$. Par développement limité, on a $\lim_{x\to 0}\varphi(x) = \frac{1}{2}$. Donc $\forall x \in \mathbb{R}$, $h_n(x) \longrightarrow \frac{e^{-\frac{x^2}{2}}}{\sqrt{2\pi}}$.

— Comme $\forall x > -1$, $\varphi(x) \geq 0$, alors h_n est dominée par $x \mapsto \frac{1}{\sqrt{2\pi}}$.

Donc par le théorème de convergence dominée,

$$\int_0^1 h_n(x)\,\mathrm{d}x \longrightarrow \int_0^1 \frac{e^{-\frac{x^2}{2}}}{\sqrt{2\pi}}\,\mathrm{d}x$$

Pour conclure, on écrit :

$$\int_0^1 g_n(x)\,\mathrm{d}x = a_n \int_0^1 h_n(x)\,\mathrm{d}x \implies \lim_{n\to+\infty} a_n = \frac{\lim_{n\to+\infty}\int_0^1 g_n(x)\,\mathrm{d}x}{\lim_{n\to+\infty}\int_0^1 h_n(x)\,\mathrm{d}x} = 1$$

et comme $\Gamma(n+1) = n!$, par définition de a_n :

$$1 = \lim_{n\to+\infty} a_n = \lim_{n\to+\infty} \frac{n^{n+\frac{1}{2}}e^{-n}\sqrt{2\pi}}{n!}$$

□

14 Formule sommatoire de Poisson

On démontre la formule sommatoire de Poisson en utilisant principalement la théorie des séries de Fourier.

Théorème 1 (Formule sommatoire de Poisson)**.** Soit $f : \mathbb{R} \to \mathbb{C}$ une fonction de classe $\mathscr{C}^1$ telle que $f(x) = O\left(\frac{1}{x^2}\right)$ et $f'(x) = O\left(\frac{1}{x^2}\right)$ quand $|x| \longrightarrow +\infty$. Alors :

$$\forall x \in \mathbb{R},\ \sum_{n\in\mathbb{Z}} f(x+n) = \sum_{n\in\mathbb{Z}} \widehat{f}(2\pi n) e^{2i\pi nx}$$

où $\widehat{f}$ désigne la transformée de Fourier de f.

[GOU20] p. 284

Démonstration. Comme $f(x) = O\left(\frac{1}{x^2}\right)$, il existe $M > 0$ et $A > 0$ tel que

$$\forall |x| > A,\ |f(x)| \leq \frac{M}{x^2} \qquad (*)$$

Soit $K > 0$. On a $\forall x \in [-K, K]$, $\forall n \in \mathbb{Z}$ tel que $|n| > K + A$:

$$|f(x+n)| \overset{(*)}{\leq} \frac{M}{(x+n)^2} \leq \frac{M}{(|n| - |x|)^2} \leq \frac{M}{(|n| - K)^2}$$

Donc $\sum_{n\in\mathbb{Z}} f(x+n)$ converge normalement sur tout segment de $\mathbb{R}$ donc converge simplement sur $\mathbb{R}$. On note F la limite simple en question.

On montre de même que $\sum_{n\in\mathbb{Z}} f'(x+n)$ converge normalement sur tout segment de $\mathbb{R}$. Donc par le théorème de dérivation des suites de fonctions, F est de classe $\mathscr{C}^1$ sur tout segment de $\mathbb{R}$, donc sur $\mathbb{R}$ tout entier (la continuité et la dérivabilité sont des propriétés locales).

Soit $x \in \mathbb{R}$. On a :

$$\begin{aligned} &\forall N \in \mathbb{N},\ \sum_{n=-N}^{N} f(x+1+n) = \sum_{n=-N-1}^{N+1} f(x+n) \\ &\overset{N\longrightarrow+\infty}{\Longrightarrow} F(x+1) = F(x) \end{aligned}$$

ie. F est 1-périodique. On peut calculer ses coefficients de Fourier. $\forall n \in \mathbb{Z}$,

$$c_n(F) = \int_0^1 F(t) e^{-2i\pi nt}\,\mathrm{d}t = \int_0^1 \sum_{n=-\infty}^{+\infty} f(t+n) e^{-2i\pi nt}\,\mathrm{d}t$$

Par convergence uniforme sur un segment, on peut échanger somme et intégrale :

$$c_n(F) = \sum_{n=-\infty}^{+\infty} \int_n^{n+1} f(t) e^{-2i\pi nt}\,\mathrm{d}t$$

Or, la transformée de Fourier d'une fonction L_1 est convergente. On peut donc écrire :

$$c_n(F) = \int_{-\infty}^{+\infty} f(t) e^{-2i\pi nt}\,\mathrm{d}t = \widehat{f}(2\pi n)$$

Comme F est de classe $\mathscr{C}^1$, sa série de Fourier converge uniformément vers F. D'où le résultat. □

Application 2 (Identité de Jacobi)**.**

$$\forall s>0,\ \sum_{n=-\infty}^{+\infty} e^{-\pi n^2 s} = \frac{1}{\sqrt{s}} \sum_{n=-\infty}^{+\infty} e^{-\frac{\pi n^2}{s}}$$

Démonstration. Soit $\alpha>0$. On définit $G_\alpha : x \mapsto e^{-\alpha x^2}$ et on connaît sa transformée de Fourier :

$$\forall \xi \in \mathbb{R},\ \widehat{G_\alpha}(\xi) = \sqrt{\frac{\pi}{\alpha}} e^{-\frac{\xi^2}{4\alpha}}$$

Soit $s>0$. Appliquons le Théorème 1 à la fonction $G_{\pi s}$:

$$\begin{aligned} \sum_{n\in\mathbb{Z}} e^{-\pi s(x+n)^2} &= \frac{1}{\sqrt{s}} \sum_{n\in\mathbb{Z}} e^{-\frac{(2\pi n)^2}{4\pi s}} e^{2i\pi nx} \\ \overset{x=0}{\Longrightarrow} \sum_{n\in\mathbb{Z}} e^{-\pi s n^2} &= \frac{1}{\sqrt{s}} \sum_{n\in\mathbb{Z}} e^{-\frac{\pi n^2}{s}} \end{aligned}$$

□

15 $\exp : \mathcal{S}_n(\mathbb{R}) \to \mathcal{S}_n^{++}(\mathbb{R})$ est un homéomorphisme

Dans ce développement, on démontre que l'exponentielle de matrices induit un homéomorphisme de $\mathcal{S}_n(\mathbb{R})$ sur $\mathcal{S}_n^{++}(\mathbb{R})$.

Lemme 1. $\mathcal{S}_n(\mathbb{R})$ est un fermé de $\mathcal{M}_n(\mathbb{R})$.

Démonstration. Il suffit d'écrire

$$\mathcal{S}_n(\mathbb{R}) = \{M \in \mathcal{M}_n(\mathbb{R}) \mid {}^tM = M\} = f^{-1}\{0\}$$

où $f : M \mapsto {}^tM - M$ est continue, donc $\mathcal{S}_n(\mathbb{R})$ est fermé en tant qu'image réciproque d'un fermé par une application continue. □

Lemme 2. Une suite bornée d'un espace métrique qui admet une seule valeur d'adhérence converge vers cette valeur d'adhérence.

Démonstration. Soit (x_n) une suite bornée d'un espace métrique (E,d) qui n'admet qu'une seule valeur d'adhérence $\ell \in E$. On suppose par l'absurde que (x_n) ne converge pas vers ℓ :

$$\exists \epsilon > 0 \text{ tel que } \forall N \in \mathbb{N}, \exists n \geq N \text{ tel que } d(x_n, \ell) > \epsilon \qquad (*)$$

On va construire une sous-suite qui converge vers une valeur d'adhérence différente de ℓ.

Par $(*)$ appliqué à $N = 0$, $\exists n_0 \geq 0$ tel que $d(x_{n_0}, \ell) > \epsilon$. On définit donc $\varphi(0) = n_0$.

Supposons construite $\varphi(i)$ jusqu'à un rang k telle que $\forall i \leq k$, $\varphi(i+1) > \varphi(i)$ (lorsque cela à un sens) et $d(x_{\varphi(i)}, \ell) > \epsilon$. Il suffit alors d'appliquer $(*)$ à $N = \varphi(n) + 1$ pour obtenir un $n_k \geq \varphi(n) + 1 > \varphi(n)$ tel que $d(x_{n_k}, \ell) > \epsilon$; on définit alors $\varphi(k+1) = n_k$.

Nous venons donc de construire par récurrence une application $\varphi : \mathbb{N} \to \mathbb{N}$ strictement croissante et telle que $\forall n \in \mathbb{N}$, $d(x_{\varphi(n)}, \ell) > \epsilon$. La suite $(x_{\varphi(n)})$ est bornée (par hypothèse) : elle est contenue dans un compact et admet une valeur d'adhérence ℓ' (par le théorème de Bolzano-Weierstrass). Soit donc $\phi : \mathbb{N} \to \mathbb{N}$ strictement croissante telle que $(x_{(\varphi\circ\psi)(n)})$ converge vers ℓ'.

On a $\forall n \in \mathbb{N}$, $d(x_{(\varphi\circ\psi)(n)}, \ell) > \epsilon$, qui donne $d(\ell', \ell) \geq \epsilon$ après un passage à la limite. Donc $\ell \neq \ell'$. Et ℓ' est clairement valeur d'adhérence de (x_n) : absurde. □

Lemme 3. Soit $S \in \mathcal{S}_n(\mathbb{R})$. Alors,

$$|||S|||_2 = \rho(S)$$

où ρ est l'application qui a une matrice y associe son rayon spectral.

[I-P] p. 182

Démonstration. D'après le théorème spectral, il existe $(e_1, \dots, e_n)$ une base orthonormée de $\mathbb{R}^n$ formée de vecteurs propres de S associés aux valeurs propres $\lambda_1, \dots, \lambda_n$ de S, qui sont réelles car S

est symétrique. Soit $x \in \mathbb{R}^n$ dont on note $(x_1, \dots, x_n)$ ses coordonnées dans cette base. On a

$$\|Sx\|_2^2 = \left\| \sum_{i=1}^n \lambda_i x_i e_i \right\|_2^2 = \sum_{i=1}^n \lambda_i^2 x_i^2 \leq \rho(S)^2 \|x\|_2^2$$

D'où $|||S|||_2 \leq \rho(S)$. Pour obtenir l'inégalité inverse, il suffit de considérer $\lambda \in \mathbb{R}$ une valeur propre de S telle que $|\lambda| = \rho(S)$ et $x \in \mathbb{R}^n$ un vecteur propre associé à λ. On a alors

$$\|Sx\|_2 = |\lambda| \|x\|_2$$

et on a bien $\rho(S) \leq |||S|||_2$. □

Théorème 4. L'application exp : $\mathcal{S}_n(\mathbb{R}) \to \mathcal{S}_n^{++}(\mathbb{R})$ est un homéomorphisme.

Démonstration. Montrer qu'une application est un homéomorphisme se fait en 4 étapes : on montre qu'elle est continue, injective, surjective, et que la réciproque est elle aussi continue.

— L'application est bien définie et continue : Soit $S \in \mathcal{S}_n(\mathbb{R})$. D'après le théorème spectral,

$$\exists P \in \mathcal{O}_n(\mathbb{R}) \text{ telle que } S = P^{-1} \underbrace{\operatorname{Diag}(\lambda_1, \dots, \lambda_n)}_{=D} P$$

où $\lambda_1, \dots, \lambda_n$ désignent les valeurs propres de S. On a donc

$$\begin{aligned} \exp(S) &= P^{-1} \exp(D) P \\ &= P^{-1} \operatorname{Diag}(e^{\lambda_1}, \dots, e^{\lambda_n}) P \end{aligned}$$

Or, $P^{-1} = {}^tP$, donc ${}^t\exp(S) = \exp(S)$ et $\exp(S) \in \mathcal{S}_n(\mathbb{R})$. De plus, $\forall x \in \mathbb{R}^n$,

$${}^t x S x = {}^t(Px) D (Px) > 0$$

car $D \in \mathcal{S}_n^{++}(\mathbb{R})$. Donc $S \in \mathcal{S}_n^{++}(\mathbb{R})$. Elle est de plus continue en tant que restriction de l'exponentielle définie sur $\mathcal{M}_n(\mathbb{K})$ (qui est la somme d'une série normalement convergente sur toute boule ouverte de $\mathcal{M}_n(\mathbb{K})$).

— L'application est surjective : Soit $S \in \mathcal{S}_n^{++}(\mathbb{R})$. On peut écrire

$$S = P \operatorname{Diag}(\mu_1, \dots, \mu_n) P^{-1}$$

Il suffit alors de poser $U = P^{-1} \operatorname{Diag}(\ln(\mu_1), \dots, \ln(\mu_n)) P \in \mathcal{S}_n(\mathbb{R})$ pour avoir $\exp(U) = S$; d'où la surjectivité.

— L'application est injective : Soient $S, S' \in \mathcal{S}_n(\mathbb{R})$ telles que $\exp(S) = \exp(S')$. Montrons que $S = S'$. Comme avant, $\exists P, P' \in \mathcal{O}_n(\mathbb{R})$ telles que

$$S = P \operatorname{Diag}(\lambda_1, \dots, \lambda_n) P^{-1} \text{ et } S' = P' \operatorname{Diag}(\lambda_1', \dots, \lambda_n') P'^{-1}$$

Soit $L \in \mathbb{R}[X]$ tel que $\forall i \in [\![1, n]\!]$, $L(e^{\lambda_i}) = \lambda_i$ et $L(e^{\lambda_i'}) = \lambda_i'$ (les polynômes d'interpolation de Lagrange conviennent parfaitement et sont bien définis dans le cas présent car $e^{\lambda_i} =$

$e^{\lambda_j} \implies \lambda_i = \lambda_j$ par injectivité de l'exponentielle). D'où

$$\begin{aligned} L(\exp(S)) &= L(P\,\mathrm{Diag}(\lambda_1,\dots,\lambda_n)P^{-1}) \\ &= PL(\exp(\mathrm{Diag}(\lambda_1,\dots,\lambda_n)))P^{-1} \\ &= P\,\mathrm{Diag}(\lambda_1,\dots,\lambda_n)P^{-1} \\ &= S \end{aligned}$$

et de même, $L(\exp(S')) = S'$. D'où $S = S'$ car on a supposé $\exp(S) = \exp(S')$.

— L'application inverse est continue : Soit (A_k) une suite de $\mathscr{S}_n^{++}(\mathbb{R})$ qui converge vers $A \in \mathscr{S}_n^{++}(\mathbb{R})$. Il s'agit de montrer que la suite (B_k) de terme général $B_k = \exp^{-1}(A_k)$ converge vers $B = \exp^{-1}(A)$. Supposons tout d'abord (B_k) non bornée. Comme sur $\mathscr{S}_n(\mathbb{R})$, $|||.|||_2 = \rho(.)$ (par le Théorème 3), il existe $\varphi : \mathbb{N} \to \mathbb{N}$ strictement croissante telle que $\rho(B_{\varphi(k)}) \longrightarrow +\infty$. On peut donc extraire une suite de valeurs propres (λ_k) telle que $|\lambda_k| \longrightarrow +\infty$. Encore une fois, quitte à extraire, on peut supposer $\lambda_k \longrightarrow +\infty$ ou $\lambda_k \longrightarrow -\infty$.

  — Si $\lambda_k \longrightarrow +\infty$, $e^{\lambda_k} \longrightarrow +\infty$. Mais $\forall k \in \mathbb{N}$, e^{λ_k} est valeur propre de A_k, donc $\rho(A_k) \longrightarrow +\infty$: absurde car (A_k) converge.

  — Si $\lambda_k \longrightarrow -\infty$, $e^{-\lambda_k} \longrightarrow +\infty$. Mais $\forall k \in \mathbb{N}$, $e^{-\lambda_k}$ est valeur propre de A_k^{-1}, donc $\rho(A_k^{-1}) \longrightarrow +\infty$: absurde car (A_k^{-1}) converge par continuité de $M \mapsto M^{-1}$.

  Donc la suite (B_k) est bornée. Par le théorème de Bolzano-Weierstrass, (B_k) admet une valeur d'adhérence $\widetilde{B_0}$. Comme $\mathscr{S}_n(\mathbb{R})$ est fermé (c'est le Théorème 1), $\widetilde{B_0} \in \mathscr{S}_n(\mathbb{R})$.

  Soit $\widetilde{B} \in \mathscr{S}_n(\mathbb{R})$ une valeur d'adhérence de (B_k) et soit $\varphi : \mathbb{N} \to \mathbb{N}$ strictement croissante telle que $B_{\varphi(k)} \longrightarrow \widetilde{B}$. Alors,

$$\exp(B) = A \longleftarrow A_{\varphi(k)} = \exp(B_{\varphi(k)}) \longrightarrow \exp(\widetilde{B})$$

  ie. $\exp(B) = \exp(\widetilde{B})$; donc $B = \widetilde{B} = \widetilde{B_0}$ par injectivité de exp. Donc par le Théorème 2, $B_k \longrightarrow B$.

□

16 Intégrale de Dirichlet

Il s'agit ici de calculer l'intégrale de Dirichlet en utilisant les théorèmes classiques d'intégration.

Lemme 1.

$$\forall y, t \in \mathbb{R}^+, |e^{-(y-i)t}| \leq 1$$

Démonstration. Soient $y, t \in \mathbb{R}^+$. On a :

$$|e^{-(y-i)t}| = |e^{-yt}e^{it}| = |e^{-yt}||e^{it}|$$

Or, e^{it} est un complexe de module 1 et $yt \geq 0$, donc $e^{-yt} \leq 1$. D'où le résultat. □

Théorème 2 (Intégrale de Dirichlet)**.** On pose $\forall x \geq 0$,

$$F(x) = \int_0^{+\infty} \frac{\sin(t)}{t} e^{-xt}\,\mathrm{d}t$$

alors :

(i) F est bien définie et est continue sur $\mathbb{R}^+$.

(ii) F est dérivable sur $\mathbb{R}_*^+$ et $\forall x \in \mathbb{R}_*^+, F'(x) = -\frac{1}{1+x^2}$.

(iii) $F(0) = \int_0^{+\infty} \frac{\sin(t)}{t}\,\mathrm{d}t = \frac{\pi}{2}$.

[G-K] p. 107

Démonstration. Posons $\forall x \in \mathbb{R}^+$ et $\forall t \in \mathbb{R}_*^+, f(x,t) = \frac{\sin(t)}{t}e^{-xt}$ ainsi que $\forall n \geq 1, F_n(x) = \int_0^n f(x,t)\,\mathrm{d}t$. [p. 478]
On a :

— $\forall x \geq 0$, $t \mapsto f(x,t)$ est mesurable.

— Presque partout en $t > 0$, $x \mapsto f(x,t)$ est continue.

— $\forall x \geq 0$ et presque partout en $t > 0$, $|f(x,t)| \leq 1$, et $t \mapsto 1$ est intégrable sur $[0,n]$.

On peut donc appliquer le théorème de continuité sous l'intégrale pour conclure que F_n est continue sur $\mathbb{R}^+$.

Soient $x \geq 0$ et $q \geq p \geq N \geq 0$. On a :

$$\begin{aligned}
|F_q(x) - F_p(x)| &= \left| \int_p^q f(x,t)\,\mathrm{d}t \right| \\
&= \left| \mathrm{Im}\left(\int_p^q e^{-xt} \frac{e^{it}}{t}\,\mathrm{d}t \right) \right| \\
&\leq \left| \int_p^q \frac{e^{-(x-i)t}}{t}\,\mathrm{d}t \right| \\
&= \frac{1}{|x-i|} \left| \int_p^q (x-i) \frac{e^{-(x-i)t}}{t}\,\mathrm{d}t \right| \\
&\leq \left| \int_p^q (x-i) \frac{e^{-(x-i)t}}{t}\,\mathrm{d}t \right| \\
&= \left| \int_p^q -(x-i) e^{-(x-i)t} \frac{1}{t}\,\mathrm{d}t \right|
\end{aligned}$$

Nous allons réaliser une intégration par parties. Pour cela, posons :

— $u'(t) = -(x-i)e^{-(x-i)t} \implies u(t) = e^{-(x-i)t}$

— $v(t) = \frac{1}{t} \implies v'(t) = -\frac{1}{t^2}$

Ce qui nous donne :

$$\begin{aligned}
\left| \int_p^q (x-i) \frac{e^{-(x-i)t}}{t}\,\mathrm{d}t \right| &= \left| [u(t)v(t)]_p^q - \int_p^q u(t)v'(t)\,\mathrm{d}t \right| \\
&= \left| \frac{e^{-(x-i)q}}{q} - \frac{e^{-(x-i)p}}{p} + \int_p^q \frac{e^{-(x-i)t}}{t^2}\,\mathrm{d}t \right|
\end{aligned}$$

On applique maintenant le Théorème 1 :

$$\begin{aligned}
\left| \frac{e^{-(x-i)q}}{q} - \frac{e^{-(x-i)p}}{p} + \int_p^q \frac{e^{-(x-i)t}}{t^2}\,\mathrm{d}t \right| &\leq \frac{1}{p} + \frac{1}{q} + \int_p^q \frac{1}{t^2}\,\mathrm{d}t \\
&= \frac{1}{q} + \frac{1}{p} - \left[\frac{1}{t} \right]_p^q \\
&\leq \frac{2}{N}
\end{aligned}$$

D'où :

$$|F_q(x) - F_p(x)| \leq \frac{2}{N}$$

Donc la suite de fonctions continues (F_n) vérifie le critère de Cauchy uniforme, et converge ainsi vers F uniformément. En particulier, F est continue sur $\mathbb{R}^+$.

Soit $a > 0$. f est dérivable par rapport à x et pour tout $x \in]a, +\infty|$ et $t \in \mathbb{R}^+$:

$$\left| \frac{\partial f}{\partial x}(x,t) \right| = |-\sin(t)e^{-xt}| \leq e^{-at}$$

On applique le théorème de dérivation sous l'intégrale, qui donne :

$$\forall x \in]a, +\infty[, F'(x) = \int_0^{+\infty} -\sin(t)e^{-xt}\,\mathrm{d}t$$

En particulier, c'est vrai sur $\mathbb{R}_*^+$ car la dérivabilité est une propriété locale. Or $\forall A > 0$, on a :

$$\begin{aligned}
&\int_0^A e^{-(i+x)t}\,\mathrm{d}t = \frac{1-e^{-(i+x)A}}{i+x} \\
\implies &\lim_{A\to+\infty}\int_0^A e^{-(i+x)t}\,\mathrm{d}t = \frac{1}{i+x} = \frac{-i+x}{1+x^2} \\
\implies &\mathrm{Im}\left(\lim_{A\to+\infty}\int_0^A e^{-(i+x)t}\,\mathrm{d}t\right) = \mathrm{Im}\left(\frac{-i+x}{1+x^2}\right) = -\frac{1}{1+x^2}
\end{aligned}$$

Or,

$$\mathrm{Im}\left(\lim_{A\to+\infty}\int_0^A e^{-(i+x)t}\,\mathrm{d}t\right) = \lim_{A\to+\infty}\int_0^A \mathrm{Im}\left(e^{-(i+x)t}\right)\mathrm{d}t = \int_0^{+\infty} -\sin(t)e^{-xt}\,\mathrm{d}t = F'(x)$$

En recollant les deux morceaux :

$$F'(x) = -\frac{1}{1+x^2} \qquad (*)$$

Soient $x, y \in \mathbb{R}_*^+$. En intégrant $(*)$ entre x et y, on obtient :

$$F(x) - F(y) = \arctan(x) - \arctan(y)$$

Mais,

$$\begin{aligned}
|F(y)| &= \left|\int_0^{+\infty} \frac{\sin(t)}{t}e^{-yt}\,\mathrm{d}t\right| \\
&\leq \int_0^{+\infty}\left|\frac{\sin(t)}{t}e^{-yt}\right|\mathrm{d}t \\
&\leq \int_0^{+\infty} e^{-yt}\,\mathrm{d}t \\
&= \frac{1}{y} \\
&\longrightarrow_{y\to+\infty} 0
\end{aligned}$$

Il suffit donc de faire tendre y vers $+\infty$ pour obtenir :

$$\forall x > 0, F(x) = \frac{\pi}{2} - \arctan(x)$$

Ce qui, en faisant tendre x vers 0, donne :

$$F(0) = \int_0^{+\infty} \frac{\sin(t)}{t}\,\mathrm{d}t = \frac{\pi}{2}$$

□

17 Lemme de Morse

En usant (certains diront plutôt "en abusant") du théorème d'inversion locale, on montre le lemme de Morse et on l'applique à l'étude de la position d'une surface par rapport à son plan tangent.

Notation 1. Si $f : \mathbb{R}^n \to \mathbb{R}$ est une application dont toutes les dérivées secondes existent, on note $\mathrm{Hess}(f)_a$ la hessienne de f au point a.

Lemme 2. Soit $A_0 \in \mathcal{S}_n(\mathbb{R})$ inversible. Alors il existe un voisinage V de A_0 dans $\mathcal{S}_n(\mathbb{R})$ et une application $\psi : V \to \mathrm{GL}_n(\mathbb{R})$ de classe $\mathcal{C}^1$ telle que

$$\forall A \in V,\ A = {}^t\psi(A) A_0 \psi(A)$$

[ROU] p. 209

Démonstration. On définit l'application

$$\varphi : \begin{array}{ccc} \mathcal{M}_n(\mathbb{R}) & \to & \mathcal{S}_n(\mathbb{R}) \\ M & \mapsto & {}^tMA_0M \end{array}$$

qui est une application polynômiale en les coefficients de M, donc de classe $\mathcal{C}^1$. Soit $H \in \mathcal{M}_n(\mathbb{R})$. On calcule :

$$\begin{aligned} \varphi(I_n + H) - \varphi(I_n) &= {}^tHA_0 + A_0H + {}^tHA_0 + H \\ &= {}^t(A_0H) + A_0H + o(\|H\|^2) \end{aligned}$$

où $(\|.\|$ désigne une quelconque norme d'algèbre sur $\mathcal{M}_n(\mathbb{R}))$. Ainsi, on a $\mathrm{d}\varphi_{I_n}(H) = {}^t(A_0H) + A_0H$. D'où

$$\mathrm{Ker}(\mathrm{d}\varphi_{I_n}) = \{M \in \mathcal{M}_n(\mathbb{R}) \mid A_0M \in \mathcal{A}_n(\mathbb{R})\} = A_0^{-1}\mathcal{A}_n(\mathbb{R})$$

On définit donc

$$F = \{M \in \mathcal{M}_n(\mathbb{R}) \mid A_0M \in \mathcal{S}_n(\mathbb{R})\} = A_0^{-1}\mathcal{S}_n(\mathbb{R})$$

et on a $\mathcal{M}_n(\mathbb{R}) = F \oplus \mathrm{Ker}(\mathrm{d}\varphi_{I_n})$. Ainsi, la différentielle $\mathrm{d}(\varphi_{|F})_{I_n}$ est bijective (car $\mathrm{Ker}(\mathrm{d}(\varphi_{|F})_{I_n}) = \mathrm{Ker}(\mathrm{d}\varphi_{I_n}) \cap F = \{0\}$).

On peut donc appliquer le théorème d'inversion locale à $\varphi_{|F}$: il existe U un voisinage ouvert de I_n dans F tel que $(\varphi_{|U})$ soit $\mathcal{C}^1$-difféomorphisme de U sur $V = \varphi(U)$. De plus, on peut supposer $U \subseteq \mathrm{GL}_n(\mathbb{R})$ (quitte à considérer $U \cap U'$ où U' est un voisinage ouvert de I_n dans $\mathrm{GL}_n(\mathbb{R})$; qui existe par continuité de det).

Ainsi, V est un voisinage ouvert de $A_0 = \varphi(I_n)$ dans $\mathcal{S}_n(\mathbb{R})$ vérifiant :

$$\forall A \in V,\ A = {}^t(\varphi_{|U})^{-1}(A) A_0 (\varphi_{|U})^{-1}(A)$$

Il suffit alors de poser $\psi = (\varphi_{|U})^{-1}$ (qui est bien une application de classe $\mathcal{C}^1$) pour avoir le résultat demandé. □

p. 354

Lemme 3 (Morse)**.** Soit $f : U \to \mathbb{R}$ une fonction de classe $\mathscr{C}^3$ (où U désigne un ouvert de $\mathbb{R}^n$ contenant l'origine). On suppose :

— $\mathrm{d}f_0 = 0$.

— La matrice symétrique $\mathrm{Hess}(f)_0$ est inversible.

— La signature de $\mathrm{Hess}(f)_0$ est $(p, n-p)$.

Alors il existe un difféomorphisme $\phi = (\phi_1, \dots, \phi_n)$ de classe $\mathscr{C}^1$ entre deux voisinage de l'origine de $\mathbb{R}^n$ $V \subseteq U$ et W tel que $\varphi(0) = 0$ et

$$\forall x \in U,\ f(x) - f(0) = \sum_{k=1}^{p} \phi_k^2(x) - \sum_{k=p+1}^{n} \phi_k^2(x)$$

Démonstration. On écrit la formule de Taylor à l'ordre 1 avec reste intégral au voisinage de 0, qui donne :

$$\begin{aligned} f(x) &= f(0) + \mathrm{d}f_0(x) + \int_0^1 (1-t)\mathrm{d}^2 f_{tx}(x,x)\,\mathrm{d}t \\ \iff f(x) - f(0) &= {}^t x Q(x) x \end{aligned} \tag{$*$}$$

où $Q(x)$ est la matrice symétrique définie par $Q(x) = \int_0^1 (1-t)\mathrm{Hess} f_{tx}\,\mathrm{d}t$ (qui est une application $\mathscr{C}^1$ sur U car f est $\mathscr{C}^3$ sur U).

Par hypothèse, $Q(0) = \frac{\mathrm{Hess}(f)_0}{2}$ est une matrice symétrique inversible, donc en vertu du Théorème 2, il existe un voisinage V_1 de $Q(0)$ dans $\mathscr{S}_n(\mathbb{R})$ et une application $\psi : V_1 \to \mathrm{GL}_n(\mathbb{R})$ de classe $\mathscr{C}^1$ tels que :

$$\forall A \in V_1,\ A = {}^t\psi(A) Q(0) \psi(A)$$

Mais, l'application $x \mapsto Q(x)$ est continue sur U (puisque f est de classe $\mathscr{C}^3$ sur U), donc il existe V_2 voisinage de 0 dans U tel que $\forall x \in V_2,\ Q(x) \in V_1$. On peut donc définir l'application $M = \psi \circ Q_{|V_2}$, qui nous permet d'écrire

$$\forall x \in V_2,\ Q(x) = {}^t M(x) Q(0) M(x) \tag{$**$}$$

Or, $Q(0)$ est de signature $(p, n-p)$, donc d'après la loi d'inertie de Sylvester, il existe $P \in \mathrm{GL}_n(\mathbb{R})$ telle que

$$Q(0) = {}^t P \underbrace{\begin{pmatrix} I_p & \\ & -I_{n-p} \end{pmatrix}}_{=D} P \tag{$***$}$$

Finalement en combinant $(*)$ avec $(**)$ et $(***)$, cela donne

$$\begin{aligned} &\forall x \in V_2,\ f(x) - f(0) = {}^t(PM(x)x) D (PM(x)x) \\ \overset{\varphi(x) = PM(x)x}{\iff} &\forall x \in V_2,\ f(x) - f(0) = {}^t\varphi(x) D \varphi(x) \end{aligned}$$

ce qui est bien l'expression voulue.

Il reste à montrer que φ définit bien un difféomorphisme de classe $\mathscr{C}^1$ entre deux voisinages de

l'origine. Notons déjà que φ est de classe $\mathscr{C}^1$ car M l'est. Calculons la différentielle en 0 de φ. Soit $h \in V_2$;

$$\begin{aligned}\varphi(h) - \varphi(0) &= PM(h)h \\ &= P(M(0) + \mathrm{d}M_0(h) + o(\|h\|))h \\ &= PM(0)h + o(\|h\|)\end{aligned}$$

d'où $\mathrm{d}\varphi_0(h) = PM(0)h$. Or, $PM(0)$ est inversible, donc en particulier, $\mathrm{d}\varphi_0$ l'est aussi. On peut appliquer le théorème d'inversion locale à φ, qui donne l'existence de deux ouverts V et W contenant l'origine (car $\varphi(0) = 0$) tel que $\phi = \varphi_{|V}$ soit un $\mathscr{C}^1$-difféomorphisme de V sur W. □

p. 341

Application 4. Soit S la surface d'équation $z = f(x,y)$ où f est de classe $\mathscr{C}^3$ au voisinage de l'origine. On suppose la forme quadratique $\mathrm{d}^2 f_0$ non dégénérée. Alors, en notant P le plan tangent à S en 0 :

(i) Si $\mathrm{d}^2 f_0$ est de signature $(2,0)$, alors S est au-dessus de P au voisinage de 0.

(ii) Si $\mathrm{d}^2 f_0$ est de signature $(0,2)$, alors S est en-dessous de P au voisinage de 0.

(iii) Si $\mathrm{d}^2 f_0$ est de signature $(1,1)$, alors S traverse P selon une courbe admettant un point double en $(0, f(0))$.

Démonstration. Une équation cartésienne de P est donnée par

$$z - 0 = f(0) + \mathrm{d}f_0(x,y)$$

La différence d'altitude entre la surface S et le plan tangent P au point $h \in \mathbb{R}^2$ est donc donnée par

$$\delta(h) = f(h) - (f(0) + \mathrm{d}f_0(h))$$

et le Théorème 3 permet d'écrire

$$\delta(h) = \alpha\phi_1(h)^2 + \beta\phi_2(h)^2$$

où (α,β) désigne la signature de $\mathrm{d}^2 f_0$ et $\phi = (\phi_1,\phi_2)$ est un $\mathscr{C}^1$-difféomorphisme entre deux voisinages de l'origine dans $\mathbb{R}^2$. En particulier, ϕ_1 et ϕ_2 ne s'annulent simultanément qu'en 0.

(i) Si $\mathrm{d}^2 f_a$ est de signature $(2,0)$, on a $\delta(h) > 0$ pour h voisin de 0 et $h \neq 0$.

(ii) Si $\mathrm{d}^2 f_a$ est de signature $(0,2)$, on a $\delta(h) < 0$ pour h voisin de 0 et $h \neq 0$.

(iii) Si $\mathrm{d}^2 f_a$ est de signature $(1,1)$, on a $\delta(h) = \phi_1(h)^2 - \phi_2(h)^2$ et S traverse P selon une courbe admettant un point double en $(0, f(0))$.

□

18 Loi d'inertie de Sylvester

Le but de ce développement est de montrer la très connue loi d'inertie de Sylvester qui donne l'existence (et une forme d'unicité) de la décomposition d'une forme quadratique réelle en carrés de formes linéaires indépendantes.

Soit E un espace vectoriel sur $\mathbb{R}$ de dimension finie $n \geq 1$. Soit Φ une forme quadratique sur E. [GOU21] p. 243

Notation 1. — On note φ la forme polaire associée à Φ.
— Si Γ est une partie de E^*, on note Γ° son orthogonal (ie. $\Gamma^\circ = \{x \in E \mid \forall f \in \Gamma, f(x) = 0\}$).

Lemme 2. Il existe une base de E qui soit Φ-orthogonale.

Démonstration. On procède par récurrence sur n.

— Si $n = 1$: il n'y a rien à montrer, tout base est Φ-orthogonale.

— On suppose le résultat vrai à un rang $n \geq 1$ et montrons le au rang $n+1$. Si $\Phi = 0$, alors tout base de E est Φ-orthogonale. Sinon, il existe $v \in E$ tel que $\Phi(v) \neq 0$. Dans ce cas, l'application $f = \varphi(v, .)$ est une forme linéaire non nulle sur E.

$H = \mathrm{Ker}(f)$ est un hyperplan de E et comme $v \notin H$, on a $E = H \oplus \mathrm{Vect}(v)$. Or, $\dim(H) = n-1$, donc on peut appliquer l'hypothèse de récurrence à $\Phi_{|H}$, et on obtient une base $\mathscr{B}$ de H qui est Φ-orthogonale. En particulier, $\mathscr{B} \cup \{v\}$ est une base Φ-orthogonale de E.

□

Théorème 3 (Loi d'inertie de Sylvester)**.**

$$\exists p, q \in \mathbb{N} \text{ et } \exists f_1, \dots, f_{p+q} \in E^* \text{ tels que } \Phi = \sum_{i=1}^{p} |f_i|^2 - \sum_{i=p+1}^{p+q} |f_i|^2$$

où les formes linéaires f_i sont linéairement indépendantes et où $p + q \leq n$. De plus, ces entiers ne dépendent que de Φ et pas de la décomposition choisie.

Le couple (p, q) est la **signature** de Φ et le rang Φ est égal à $p + q$.

Démonstration. Soit $\mathscr{B} = (e_1, \dots, e_n)$ une base Φ-orthogonale (dont l'existence est assurée par le Théorème 2). En posant $\forall i \in [\![1, n]\!]$, $\lambda_i = \Phi(e_i)$, on a

$$\forall x \in E \text{ que l'on écrit } x = x_1 e_1 + \cdots + x_n e_n, \ \Phi(x) = \sum_{i=1}^{n} |x_i|^2 \Phi(e_i) = \sum_{i=1}^{n} \lambda_i |x_i|^2$$

Chaque λ_i est strictement positif, strictement négatif, ou nul. Quitte à les réordonner, on peut supposer

$$\lambda_1, \dots, \lambda_p > 0, \lambda_{p+1}, \dots, \lambda_{p+q} < 0, \text{ et } \lambda_{p+q+1} = \cdots = \lambda_n = 0$$

Pour $i \in [\![1,p]\!]$, on peut écrire $\lambda_i = \omega_i^2$ et pour $i \in [\![p+1,p+q]\!]$, on peut écrire $\lambda_i = -\omega_i^2$ où les $\omega_i \in \mathbb{R}^*$. On définit :

$$\forall i \in [\![1,q]\!], f_i = \omega_i e_i^*$$

Ainsi définies, les formes linéaires f_i sont linéairement indépendantes et on obtient bien :

$$\Phi = \sum_{i=1}^{p} |f_i|^2 - \sum_{i=p+1}^{q} |f_i|^2 \qquad (*)$$

Reste maintenant à montrer l'indépendance de p et de q vis-à-vis de la décomposition choisie. Soit donc

$$\Phi = \sum_{i=1}^{p'} |g_i|^2 - \sum_{i=p'+1}^{q'} |g_i|^2 \qquad (**)$$

une autre écriture en carrés de formes linéaires indépendantes. Supposons $p' \neq p$ avec par exemple $p' > p$. Complétons $g_1, \dots, g_{p'+q'}$ en une base $g_1, \dots, g_n$ de E^*. Donc, la famille $\Gamma = (f_1, \dots, f_p, g_{p'+1}, \dots, g_n)$ est de cardinal $p + n - p' < n$. Elle ne peut donc pas former une base de E^*. Donc

$$\dim(\Gamma^\circ) = \dim(E^*) - \dim(\Gamma) \geq 1$$

Par conséquent,

$$\exists x \neq 0 \text{ tel que } f_1(x) = \cdots = f_p(x) = g_{p'+1}(x) = \cdots = g_n(x) = 0$$

Donc $\Phi(x) \leq 0$ par $(*)$. Supposons par l'absurde que

$$g_1(x) = \cdots = g_{p'}(x) = 0$$

Comme $(g_i)_{i \in [\![1,n]\!]}$ est une base de E^* et que x s'annule sur cette base, on a $x = 0$: c'est absurde. Donc, il existe $i \in [\![1,p']\!]$ tel que $g_i(x) \neq 0$. En particulier $\Phi(x) > 0$ par $(**)$: contradiction. Ainsi, $p = p'$. On montre de même que $q = q'$.

Dans la base Φ-orthogonale $(e_1, \dots, e_n)$, la matrice de Φ est

$$\begin{pmatrix} I_p & 0 & 0 \\ 0 & -I_q & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

d'où le rang de Φ. □

La preuve de **[GOU21]** est un peu décousue. Il faut savoir recoller les morceaux pour bien montrer existence et "unicité" de la décomposition.

19 Méthode de Newton

On démontre ici la méthode de Newton qui permet de trouver numériquement une approximation précise d'un zéro d'une fonction réelle d'une variable réelle.

Théorème 1 (Méthode de Newton)**.** Soit $f : [c,d] \to \mathbb{R}$ une fonction de classe $\mathscr{C}^2$ strictement croissante sur $[c,d]$. On considère la fonction

$$\varphi : \begin{array}{ccc} [c,d] & \to & \mathbb{R} \\ x & \mapsto & x - \frac{f(x)}{f'(x)} \end{array}$$

(qui est bien définie car $f' > 0$). Alors :

(i) $\exists! a \in [c,d]$ tel que $f(a) = 0$.

(ii) $\exists \alpha > 0$ tel que $I = [a-\alpha, a+\alpha]$ est stable par φ.

(iii) La suite (x_n) des itérés (définie par récurrence par $x_{n+1} = \varphi(x_n)$ pour tout $n \geq 0$) converge quadratiquement vers a pour tout $x_0 \in I$.

[ROU] p. 152

Démonstration. Soit $x \in [c,d]$. Comme $f(a) = 0$, on peut écrire :

$$\begin{aligned} \varphi(x) - a &= x - a - \frac{f(x) - f(a)}{f'(x)} \\ &= \frac{f(a) - f(x) - (a-x)f'(x)}{f'(x)} \end{aligned}$$

Or, la formule de Taylor-Lagrange à l'ordre 2 donne l'existence d'un $z \in]a,x[$ tel que

$$\begin{aligned} f(a) &= f(x) + f'(x)(a-x) + \frac{1}{2}f''(z)(a-x)^2 \\ \iff f(a) - f(x) - f'(x)(a-x) &= \frac{1}{2}f''(z)(a-x)^2 \end{aligned}$$

D'où :

$$\varphi(x) - a = \frac{f''(z)}{2f'(x)}(x-a)^2 \qquad (*)$$

Soit $C = \frac{\max_{x\in[c,d]} |f''(x)|}{2\min_{x\in[c,d]} |f'(x)|}$. Par $(*)$, on a :

$$\forall x \in [c,d],\ |\varphi(x) - a| \leq C|x-a|^2$$

Soit maintenant $\alpha > 0$ suffisamment petit pour que $C\alpha < 1$ et que $I = [a-\alpha, a+\alpha] \subseteq [c,d]$. Alors :

$$x \in I \implies |\varphi(x) - a| \leq C\alpha^2 < \alpha$$

(la première inégalité se voit en faisant un dessin, et la seconde vient du fait que $C\alpha < 1$). D'où

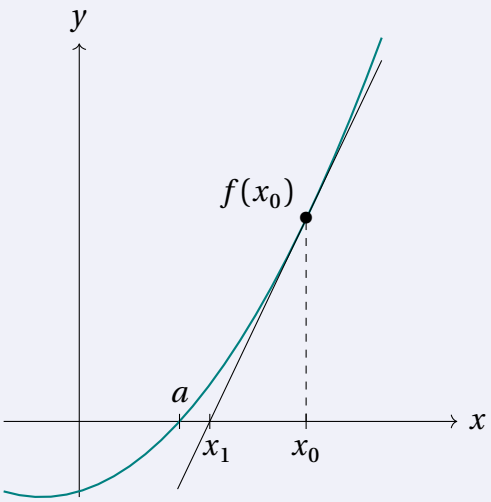
$\varphi(I) \subseteq I$. Et si $x_0 \in I$, on a donc $\forall n \in \mathbb{N}$, $x_n \in I$ et

$$\begin{aligned} |x_{n+1} - a| &= |\varphi(x_n) - a| \\ &\leq C|x_n - a|^2 \end{aligned}$$

D'où $C|x_n - a| \leq (C|x_0 - a|)^{2^n} \leq (C\alpha)^{2^n}$ où $C\alpha < 1$. On a donc bien convergence quadratique de la suite (x_n) vers le réel a. □

Remarque 2. On suppose que l'on connaisse une approximation grossière du point que l'on nomme x_0.

[DEM] p. 100



L'idée de la méthode est de remplacer la courbe représentative de f par sa tangente au point x_0 :

$$y = f'(x_0)(x - x_0) + f(x_0)$$

L'abscisse x_1 du point d'intersection de cette tangente avec l'axe des abscisses est donnée par

$$x_1 = x_0 - \frac{f(x_0)}{f'(x_0)}$$

d'où le fait d'itérer la fonction $\varphi : x \mapsto x - \frac{f(x)}{f'(x)}$.

Corollaire 3. En reprenant les hypothèses et notations du théorème précédent, et en supposant de plus f strictement convexe sur $[c,d]$, le résultat du théorème est vrai sur $I = [a,d]$. De plus :

(i) (x_n) est strictement décroissante (ou constante).

(ii) $x_{n+1} - a \sim \frac{f''(a)}{2f'(a)}(x_n - a)^2$ pour $x_0 > a$.

[ROU] p. 152

Démonstration. La dérivée f' est strictement croissante (car f est strictement convexe) sur $]c,d[$. Ainsi, soit $x \in [a,d]$. Si $x = a$, on a $\varphi(x) = x$, et la suite (x_n) est alors constante. Supposons

maintenant $x > a$. On a :

$$\varphi(x) = x - \frac{\overbrace{f(x)}^{>0}}{\underbrace{f'(x)}_{>0}} < x$$

Et par $(*)$ (de la démonstration précédente), $\exists z \in]a, x[$:

$$\varphi(x) - a = \frac{f''(z)}{2f'(z)}(x-a)^2 > 0 \iff \varphi(x) < a$$

Ainsi, $I = [a, d]$ est stable par φ et pour $x_0 \in]a, d]$, on a $x_n \in]a, d]$ pour tout $n \in \mathbb{N}$ et la suite (x_n) est strictement décroissante. La suite (x_n) admet donc une limite ℓ vérifiant $\varphi(\ell) = \ell \iff f(\ell) = 0$ ie. $\ell = a$ par unicité. Comme dans le théorème précédent, la convergence est quadratique :

$$0 \leq x_{n+1} - a \leq C(x_n - a)^2$$

Enfin, si $x_0 \in]a, d]$, on a comme dans $(*)$:

$$\forall n \in \mathbb{N},\ x_n > a \text{ et } \frac{x_{n+1} - a}{(x_n - a)^2} = \frac{f''(z_n)}{2f'(x_n)}$$

où $z_n \in]a, x_n[$ (d'après la démarche effectuée pour obtenir $(*)$). On fait tendre n vers l'infini et la fraction de droite tend vers $\frac{f''(a)}{2f'(a)}$; d'où le résultat. □

> *Remarque* 4. L'ajout de l'hypothèse de convexité à la méthode de Newton, nous permet de nous affranchir de l'intervalle I tout en gardant la même vitesse de convergence.

20 Nombres de Bell

En utilisant les propriétés des séries entières, nous calculons le nombre de partitions de l'ensemble $[\![1,n]\!]$.

Théorème 1 (Nombres de Bell)**.** Pour tout $n \in \mathbb{N}^*$, on note B_n le nombre de partitions de $[\![1,n]\!]$. Par convention on pose $B_0 = 1$. Alors,

$$\forall k \in \mathbb{N}^*, B_k = \frac{1}{e}\sum_{n=0}^{+\infty}\frac{n^k}{n!}$$

[GOU21] p. 314

Démonstration. Notons que clairement $B_1 = 1$. Soit $n \in \mathbb{N}^*$, exprimons B_{n+1} en fonction des termes précédents. Pour tout $k \leq n$, on note E_k l'ensemble des partitions P de $[\![1,n+1]\!]$ tel que la partie de P qui contient l'entier $n+1$ est de taille $k+1$. Choisir une partition dans E_k, c'est choisir k entiers de $[\![1,n]\!]$ (ceux de l'ensemble qui contient $n+1$ dans la partition), puis construire une partition des $n-k$ éléments restants. Donc $|E_k| = \binom{n}{k}B_{n-k}$.

Comme $E_0, \dots, E_n$ forment une partition de l'ensemble des partitions de $[\![1,n+1]\!]$, on obtient :

$$B_{n+1} = \sum_{k=0}^{n}\binom{n}{k}B_{n-k} = \sum_{k=0}^{n}\binom{n}{n-k}B_k = \sum_{k=0}^{n}\binom{n}{k}B_k \qquad (*)$$

À toute partition P de $[\![1,n]\!]$, on peut associer une permutation $\sigma_P \in S_n$, qui est le produit des cycles de supports les éléments de P. On construit ainsi une application $P \mapsto \sigma_P$ injective. D'où :

$$B_n \leq |S_n| = n!$$

On en déduit en particulier que $\frac{B_n}{n!} \leq 1$. En vertu du lemme d'Abel, le rayon de convergence R de la série entière $\sum \frac{B_n}{n!}x^n$ est supérieur ou égal à 1. On peut donc définir

$$B : \begin{array}{ccc}]-R,R[& \to & \mathbb{R} \\ x & \mapsto & \sum_{n=0}^{+\infty}\frac{B_n}{n!}x^n \end{array}$$

et en dérivant, $\forall x \in]-R,R[$:

$$\begin{aligned} B'(x) &= \sum_{n=0}^{+\infty}\frac{B_{n+1}}{n!}x^n \\ &\overset{(*)}{=} \sum_{n=0}^{+\infty}\frac{1}{n!}\left(\sum_{k=0}^{n}\binom{n}{k}B_k\right)x^n \\ &= \sum_{n=0}^{+\infty}\left(\sum_{k=0}^{n}\frac{B_k}{k!}\frac{1}{(n-k)!}\right)x^n \end{aligned}$$

On reconnaît là le produit de Cauchy suivant :

$$B'(x) = \sum_{n=0}^{+\infty}\left(\sum_{k=0}^{n}\frac{B_k}{k!}\frac{1}{(n-k)!}\right)x^n = \left(\sum_{n=0}^{+\infty}\frac{B_n}{n!}x^n\right)\left(\sum_{n=0}^{+\infty}\frac{x^n}{n!}\right) = B(x)e^x$$

Reste à résoudre cette équation différentielle linéaire homogène d'ordre 1 :

$$B(x) = \lambda e^{e^x}$$

Or, $B(0) = B_0 = 1 = \lambda e^1$. D'où $B(x) = \frac{1}{e} e^{e^x}$.

La série entière définissant l'exponentielle a un rayon de convergence infini. On peut écrire, pour tout $z \in \mathbb{C}$:

$$e^{e^z} = \sum_{n=0}^{+\infty} \frac{e^{nz}}{n!} = \sum_{n=0}^{+\infty} \sum_{k=0}^{+\infty} \underbrace{\frac{(nz)^k}{n!k!}}_{u_{n,k}(z)}$$

On va appliquer le théorème de Fubini-Lebesgue à $u_{n,k}(z)$ (où $z \in \mathbb{C}$ est fixé) :

$$\sum_{n=0}^{+\infty} \sum_{k=0}^{+\infty} |u_{n,k}(z)| = \sum_{n=0}^{+\infty} \frac{e^{n|z|}}{n!} = e^{e^{|z|}} < +\infty$$

Donc on peut intervertir les signes de sommations. Pour tout $x \in]-R, R[$,

$$\begin{aligned} B(x) &= \frac{1}{e} e^{e^x} \\ &= \frac{1}{e} \sum_{n=0}^{+\infty} \sum_{k=0}^{+\infty} u_{n,k}(x) \\ &= \frac{1}{e} \sum_{k=0}^{+\infty} \sum_{n=0}^{+\infty} u_{n,k}(x) \\ &= \frac{1}{e} \sum_{k=0}^{+\infty} \left(\sum_{n=0}^{+\infty} \frac{n^k}{n!} \right) \frac{x^k}{k!} \end{aligned}$$

Par unicité du développement en série entière d'une fonction, on en déduit, par identification des coefficients :

$$\forall k \in \mathbb{N}^*, B_k = \frac{1}{e} \sum_{n=0}^{+\infty} \frac{n^k}{n!}$$

□

La partie sur le dénombrement (au début de la preuve) est un peu technique. N'hésitez pas à passer du temps dessus et à y réfléchir en faisant des exemples.

21 Projection sur un convexe fermé

On montre le théorème de projection sur un convexe fermé dans un espace de Hilbert réel en utilisant les suites de Cauchy et des propriétés du produit scalaire.

Soit H un espace de Hilbert réel de norme $\|.\|$ et dont on note $\langle .,. \rangle$ le produit scalaire associé.

Lemme 1 (Identité du parallélogramme)**.** Soient $x, y \in H$. Alors :

$$\|x+y\|^2 + \|x-y\|^2 = 2(\|x\|^2 + \|y\|^2)$$

[LI] p. 32

Démonstration. D'une part,

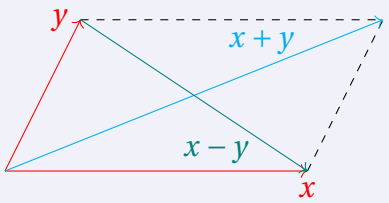
$$\|x+y\|^2 = \langle x+y, x+y\rangle = \|x\|^2 + \|y\|^2 + 2\langle x, y\rangle$$

D'autre part,

$$\|x-y\|^2 = \langle x-y, x-y\rangle = \|x\|^2 + \|y\|^2 - 2\langle x, y\rangle$$

En additionnant les deux lignes, on obtient bien l'égalité voulue. □

Remarque 2. L'interprétation géométrique de cette égalité est que dans le parallélogramme formé par les vecteurs x et y, la somme des carrés des diagonales est égale à la somme des carrés des côtés.



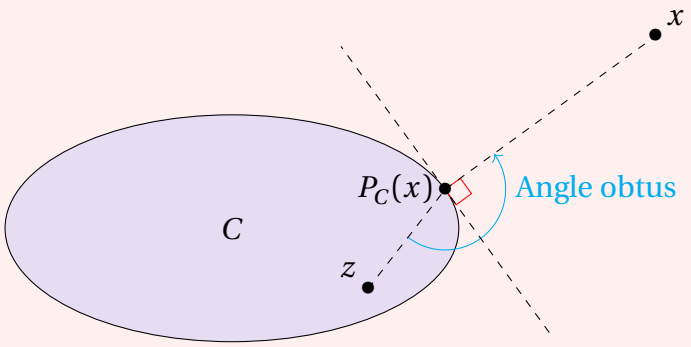
Théorème 3 (Projection sur un convexe fermé)**.** Soit $C \subseteq H$ un convexe fermé non-vide. Alors :

$$\forall x \in H, \exists! y \in C \text{ tel que } d(x,C) = \inf_{z \in C} \|x-z\| = d(x,y)$$

[GOU20] p. 427

On peut donc noter $y = P_C(x)$, le **projeté orthogonal de** x **sur** C. Il s'agit de l'unique point de C vérifiant

$$\forall z \in C, \langle x - P_C(x), z - P_C(x)\rangle \leq 0 \qquad (*)$$



Démonstration. Soit $x \in H$. Posons $\delta = d(x,C)$. Par la caractérisation séquentielle de la borne inférieure, il existe (y_n) une suite de C telle que $\|x-y_n\| \longrightarrow \delta$. Montrons que (y_n) est une suite de Cauchy. On applique le Théorème 1 :

$$\forall p,q \in \mathbb{N},\ \|(x-y_p)+(x-y_q)\|^2 + \|y_p-y_q\|^2 = 2(\|x-y_p\|^2 + \|x-y_q\|^2) \qquad (**)$$

Or, C est convexe. Donc $\forall p,q \in \mathbb{N},\ \frac{y_p+y_q}{2} \in C$.Par définition,

$$\begin{aligned} &\left\| x - \frac{y_p+y_q}{2} \right\| \geq \delta \\ \iff &\frac{1}{2}\|(x-y_p)+(x-y_q)\| \geq \delta \\ \iff &\|(x-y_p)+(x-y_q)\|^2 \geq 4\delta^2 \end{aligned}$$

Par $(**)$, quand $p,q \longrightarrow +\infty$:

$$\|y_p-y_q\| \leq 2((\underbrace{\|x-y_p\|^2}_{\longrightarrow \delta^2} - \delta^2) + (\underbrace{\|x-y_q\|^2}_{\longrightarrow \delta^2} - \delta^2)) \longrightarrow 0$$

Ainsi (y_n) est une suite de Cauchy de H qui est complet, donc (y_n) converge vers $y \in H$. Mais, C est fermé et (y_n) est une suite de C, donc $y \in C$.

Montrons maintenant que y est unique. Soit $z \in C$ tel que $\delta = \|x-z\|$. On définit la suite (z_n) par

$$\forall n \in \mathbb{N},\ z_n = \begin{cases} y & \text{si } n \text{ est pair} \\ z & \text{si } n \text{ est impair} \end{cases}$$

Cette suite vérifie $\forall n \in \mathbb{N},\ \|x-z_n\| = \delta$ donc en particulier $\|x-z_n\| \longrightarrow \delta$, et on peut tout-à-fait refaire le raisonnement précédent pour montrer que (z_n) converge (vers $y=z$, donc). Ainsi, on a bien existence et unicité du projeté.

Soit $y \in C$ vérifiant $(*)$. Montrons que $y = P_C(x)$. $\forall z \in C$,

$$\begin{aligned} \|z-x\|^2 &= \|(z-y)-(x-y)\|^2 \\ &= \|z-y\|^2 + \|x-y\|^2 - 2\langle z-y, x-y\rangle \\ &\geq \|z-y\|^2 + \|x-y\|^2 \\ &\geq \|x-y\|^2 \end{aligned}$$

ie. $\|z-x\| \geq \|x-y\|$. De plus, $y \in C$, donc $d(y,C) = d(x,C)$. D'où $y = P_C(x)$.

Montrons maintenant que $P_C(x)$ vérifie bien $(*)$. $\forall z \in C$, on a

$$\|x-z\|^2 \geq \|x-P_C(x)\|^2$$

Or, en développant :

$$\begin{aligned}\|x-z\|^2 &= \|(x-P_C(x))-(z-P_C(x))\|^2\\ &= \|x-P_C(x)\|^2+\|z-P_C(x)\|^2-2\langle x-P_C(x),z-P_C(x)\rangle\\ &\geq \|x-P_C(x)\|^2\end{aligned}$$

D'où, par la dernière inégalité,

$$\|z-P_C(x)\|^2-2\langle x-P_C(x),z-P_C(x)\rangle\geq 0 \qquad (***)$$

Soit maintenant $z_0\in C$. On va appliquer $(***)$ à $z=\lambda z_0+(1-\lambda)z_0\in C$ pour $\lambda\in]0,1]$:

$$\begin{aligned}&\lambda^2\|z_0+P_C(x)\|^2-2\lambda\langle x-P_C(x),z_0-P_C(x)\rangle\geq 0\\ \Longrightarrow\ &\lambda\|z_0+P_C(x)\|^2-2\langle x-P_C(x),z_0-P_C(x)\rangle\geq 0\\ \overset{\lambda\longrightarrow 0}{\Longrightarrow}\ &-2\langle x-P_C(x),z_0-P_C(x)\rangle\geq 0\end{aligned}$$

ce que l'on voulait. □

Remarque 4. $(*)$ traduit le fait géométrique que l'angle du vecteur $\overrightarrow{P_C(x)x}$ avec $\overrightarrow{P_C(x)z}$ est obtus pour tout $z\in C$. En effet, en notant cet angle θ, on a pour $z\in C$:

$$\langle x-P_C(x),z-P_C(x)\rangle=\|x-P_C(x)\|\,\|z-P_C(x)\|\cos(\theta)$$

et si θ est obtus, on a bien $\cos(\theta)\leq 0$.

Corollaire 5. Soit F un sous-espace vectoriel fermé de H. Alors $F\oplus F^\perp=H$.

Démonstration. Si $x\in F\cap F^\perp$, alors $\|x\|=\langle x,x\rangle=0$, et donc $x=0$. Montrons maintenant que $F+F^\perp=H$. Soit $x\in H$. Comme F est un convexe fermé de H (en tant que sous-espace vectoriel fermé), on peut appliquer le Théorème 3. Ainsi, il existe un unique $P_F(x)\in F$ tel que $d(x,F)=d(x,P_F(x))$ et

$$\forall z\in F,\ \langle x-P_F(x),z-P_F(x)\rangle\leq 0 \qquad (*)$$

Soit $z_0\in F$. on peut appliquer $(*)$ à $z=z_0$:

$$\langle x-P_F(x),z_0-P_F(x)\rangle\leq 0$$

On va également appliquer $(*)$ à $z=-z_0+2P_F(x)\in F$:

$$\langle x-P_F(x),-z_0+P_F(x)\rangle\leq 0\iff\langle x-P_F(x),z_0-P_F(x)\rangle\geq 0$$

Ce qui montre que l'inégalité de $(*)$ est en fait une égalité. On en tire :

$$\forall z\in F,\ \langle x-P_F(x),z\rangle=\langle x-P_F(x),z-P_F(x)\rangle-\langle x-P_F(x),0-P_F(x)\rangle=0$$

donc $x - P_F(x) \in F^\perp$. En conclusion, on a :

$$x = \underbrace{P_F(x)}_{\in F} + \underbrace{x - P_F(x)}_{\in F^\perp} \in F + F^\perp$$

et on a donc bien la somme directe $H = F \oplus F^\perp$. □

22 Simplicité de A_n pour $n \geq 5$

On montre que A_n est simple pour $n \geq 5$ en montrant dans un premier temps le cas $n = 5$, puis en s'y ramenant.

Lemme 1. Les 3-cycles sont conjugués dans A_n pour $n \geq 5$.

[PER] p. 15

Démonstration. Soient $\alpha = \begin{pmatrix} a_1 & a_2 & a_3 \end{pmatrix}$ et $\beta = \begin{pmatrix} b_1 & b_2 & b_3 \end{pmatrix}$ deux 3-cycles. Soit $\sigma \in S_n$ telle que

$$\forall i \in [\![1,3]\!], \sigma(a_i) = b_i$$

On a deux possibilités pour σ :

— σ est paire. Alors $\sigma \in A_n$, et le résultat est démontré pour α et β.

— σ est impaire. Comme $n \geq 5$, il existe c_1, c_2 tels que $c_1, c_2 \notin \{b_1, b_2, b_3\}$. On pose alors $\tau = \begin{pmatrix} c_1 & c_2 \end{pmatrix}$, et on a

$$(\tau\sigma)\begin{pmatrix} a_1 & a_2 & a_3 \end{pmatrix}(\tau\sigma)^{-1} = \begin{pmatrix} b_1 & b_2 & b_3 \end{pmatrix}$$

avec $\tau\sigma$ paire. Le résultat est encore démontré pour α et β.

□

Lemme 2. A_n est engendré par les 3-cycles pour $n \geq 3$.

[ROM21] p. 49

Démonstration. Montrons tout d'abord qu'un produit de deux transpositions est un produit de 3-cycles. Soient $\alpha = \begin{pmatrix} a_1 & a_2 \end{pmatrix}$ et $\beta = \begin{pmatrix} b_1 & b_2 \end{pmatrix}$ deux transpositions. Si $\alpha = \beta$, alors $\alpha\beta = \mathrm{id} = \sigma^3$ où σ désigne n'importe quel 3-cycle.

Si $\alpha \neq \beta$, on a deux possibilités :

— Leur support comporte un élément commun : $a_1 = b_1 = c$. Donc $\alpha = \begin{pmatrix} c & a_2 \end{pmatrix}$ et $\beta = \begin{pmatrix} c & b_2 \end{pmatrix}$ avec c, a_2, b_2 distincts. Donc $\alpha\beta = \begin{pmatrix} a_2, c, b_2 \end{pmatrix}$.

— Leur support n'a pas d'élément commun. Dans ce cas a_1, a_2, a_1, b_2 sont distincts et $\alpha\beta = \begin{pmatrix} a_1 & a_2 & b_1 \end{pmatrix}\begin{pmatrix} a_2 & b_1 & b_2 \end{pmatrix}$.

Soit maintenant $\sigma \in A_n$. Comme σ est paire, on peut la décomposer en un produit d'un nombre pair n de transpositions :

$$\sigma = \prod_{i=1}^{n-1} \tau_i \tau_{i+1}$$

qui est bien un produit de 3-cycles. □

Lemme 3. Les doubles transpositions sont conjuguées dans A_n pour $n \geq 5$.

p. 66

Démonstration. Soient $\alpha = \begin{pmatrix} a_1 & b_1 \end{pmatrix}\begin{pmatrix} c_1 & d_1 \end{pmatrix}\begin{pmatrix} e_1 \end{pmatrix}$ et $\beta = \begin{pmatrix} a_2 & b_2 \end{pmatrix}\begin{pmatrix} c_2 & d_2 \end{pmatrix}\begin{pmatrix} e_2 \end{pmatrix}$ deux doubles transpositions. Il suffit de prendre $\sigma \in A_5$ telle que $\sigma(a_1) = a_2$, $\sigma(b_1) = b_2$ et $\sigma(e_1) = e_2$ pour avoir $\sigma\alpha\sigma^{-1} = \beta$. □

Lemme 4. A_5 est simple.

Démonstration. Commençons par décrire les types possibles des permutations de A_5 (le "type" d'une permutation désigne les cardinaux des supports des cycles apparaissant dans sa décomposition en cycles disjoints).

Type de permutation	**Nombre de permutations**
[1]	1
[3]	$\frac{5\times4\times3}{3} = 20$
[5]	$\frac{5\times4\times3\times2\times1}{5} = 24$
[2,2]	$\frac{1}{2}\frac{5\times4\times3\times2}{4} = 15$

Soit $H \lhd A_5$ tel que $H \neq \{\mathrm{id}\}$. Montrons que $H = A_5$.

— Si H contient une permutation de type [2,2], alors par le Théorème 3, il contient toutes les permutations de type [3].

— Si H contient une permutation de type [3], alors par le Théorème 1, il les contient toutes.

— Si H contient une permutation de type [5], $\sigma = \begin{pmatrix} a & b & c & d & e \end{pmatrix}$, il contient alors le commutateur

$$\begin{aligned}\begin{pmatrix} a & b & c \end{pmatrix}\sigma\begin{pmatrix} a & b & c \end{pmatrix}^{-1}\sigma^{-1} &= \begin{pmatrix} a & b & c \end{pmatrix}\sigma\begin{pmatrix} c & b & a \end{pmatrix}\sigma^{-1} \\ &= \begin{pmatrix} a & b & c \end{pmatrix}\begin{pmatrix} \sigma(c) & \sigma(b) & \sigma(a) \end{pmatrix} \\ &= \begin{pmatrix} a & b & c \end{pmatrix}\begin{pmatrix} d & c & b \end{pmatrix} \\ &= \begin{pmatrix} b & d & a \end{pmatrix}\end{aligned}$$

qui est un 3-cycle. Par le Théorème 1, il les contient tous.

Or, H ne peut pas vérifier qu'un seul des points précédents en vertu du théorème de Lagrange, car ni $16 = 15+1$, ni $21 = 20+1$ ne divisent $|A_5| = 60$. Donc H vérifie au moins deux des points précédents, et ainsi $|H| \geq 1+15+20 = 36$. Donc $|H| = 60$ et $H = A_5$. □

Si les théorèmes de Sylow sont mentionnés dans le plan, il est préférable de mentionner l'argument suivant. **[PER]** p. 28

Remarque 5. Dans le raisonnement précédent, si H contient une permutation de type [5] (qui est donc d'ordre 5), alors H contient le 5-Sylow engendré par cet élément. Or, on sait par les théorèmes de Sylow que les sous-groupes de Sylow sont conjugués entre eux. Donc H contient tous les 5-Sylow et donc contient tous les éléments d'ordre 5.

Théorème 6. A_n est simple pour $n \geq 5$.

Démonstration. Soit $N \triangleleft A_n$ tel que $N \neq \{\mathrm{id}\}$. L'idée générale de la démonstration et de se ramener au cas $n = 5$ à l'aide d'une permutation bien spécifique.

Soit $\sigma \in N \setminus \{\mathrm{id}\}$, il existe donc $a \in [\![1, n]\!]$ tel que $\sigma(a) = b \neq a$. Soit $c \in [\![1, n]\!]$ différent de a, b et $\sigma(b)$. On pose $\tau = \begin{pmatrix} a & c & b \end{pmatrix} \in A_n$ (on a $\tau^{-1} = \begin{pmatrix} a & b & c \end{pmatrix}$). Soit $\rho = \tau\sigma\tau^{-1}\sigma^{-1}$. Par calcul :

$$\rho = \begin{pmatrix} a & c & b \end{pmatrix}\sigma\begin{pmatrix} a & b & c \end{pmatrix}\sigma^{-1} = \begin{pmatrix} a & c & b \end{pmatrix}\begin{pmatrix} \sigma(a) & \sigma(b) & \sigma(c) \end{pmatrix}$$

Notons bien que $\rho \neq \mathrm{id}$ (en tant que produit de 3-cycles, car $\sigma(b) \neq c$, donc $\rho(b) \neq b$ par calcul). Or, $\tau\sigma\tau^{-1} \in N$ car N est distingué et σ^{-1} aussi car N est un groupe, donc $\rho \in N$.

Notons $\mathscr{F} = \{a, b, c, \sigma(a), \sigma(b), \sigma(c)\}$. Comme $\sigma(a) = b$, $|\mathscr{F}| \leq 5$. Quitte à rajouter, au besoin, des éléments à $\mathscr{F}$, on peut supposer que $|\mathscr{F}| = 5$. On pose

$$A(\mathscr{F}) = \{\alpha \in A_n \mid \forall i \in [\![1, n]\!] \setminus \mathscr{F},\ \alpha(i) = i\}$$

le sous-groupe de A_n contenant les éléments qui laissent fixes $[\![1, n]\!] \setminus \mathscr{F}$. Si on pose $\mathscr{F} = \{a_1, a_2, a_3, a_4, a_5\}$, on a une bijection entre $\mathscr{F}$ et $[\![1, 5]\!]$:

$$\begin{aligned} \mathscr{F} &\to [\![1, 5]\!] \\ a_i &\mapsto i \end{aligned}$$

Donc $A(\mathscr{F})$ et A_5 sont deux groupes isomorphes (en effet, une permutation n'agissant que sur $\mathscr{F}$ peut s'identifier à une permutation n'agissant que sur $[\![1, 5]\!]$). De plus, par le Théorème 4, comme A_5 est simple, $A(\mathscr{F})$ l'est aussi.

Soit $N_0 = N \cap A(\mathscr{F})$. $N_0 \triangleleft A(\mathscr{F})$, en effet, soient $\alpha \in N_0$ et $\beta \in A(\mathscr{F})$:

- $\beta\alpha\beta^{-1} \in A(\mathscr{F})$ car $A(\mathscr{F})$ est un groupe.
- $\beta\alpha\beta^{-1} \in N$ car $N \triangleleft A_5$.

En particulier, N_0 est distingué dans $A(\mathscr{F})$ qui est simple. De plus, $\rho \in N_0$ (car $\mathrm{Supp}(\rho) \subseteq \mathscr{F}$ et $\epsilon(\rho) = (-1)^6 = 1$ donc $\rho \in A(\mathscr{F})$, et on avait déjà $\rho \in N$). Donc $N_0 \neq \{\mathrm{id}\}$, et ainsi $N_0 = A(\mathscr{F})$. On en déduit :

$$A(\mathscr{F}) = N \cap A(\mathscr{F}) \qquad (*)$$

Finalement, τ est un 3-cycle qui n'agit que sur $\mathscr{F}$, donc $\tau \in A(\mathscr{F})$ et par $(*)$, $\tau \in N$. Or, τ est un 3-cycle et les 3-cycles sont conjugués dans A_n (par le Théorème 1) donc N contient tous les 3-cycles. Et comme ceux-ci engendrent A_n (par le Théorème 2), on a $N = A_n$. □

23 Suite de polygones

Il s'agit ici d'étudier une suite de polygones à l'aide de déterminants classiques, et de montrer qu'elle converge vers l'isobarycentre du polygone de départ.

Lemme 1 (Déterminant circulant)**.** Soient $n \in \mathbb{N}^*$ et $a_1, \dots, a_n \in \mathbb{C}$. On pose $\omega = e^{\frac{2i\pi}{n}}$. Alors

$$\begin{vmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \dots & a_0 \end{vmatrix} = \prod_{j=0}^{n-1} P(\omega^j)$$

où $P = \sum_{k=0}^{n-1} a_k X^k$.

[GOU21] p. 153

Démonstration. On définit

$$A = \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \dots & a_0 \end{pmatrix} \in \mathcal{M}_n(\mathbb{C}) \text{ et } \Omega = (\omega^{(i-1)(j-1)})_{i,j\in[\![1,n]\!]} \in \mathcal{M}_n(\mathbb{C})$$

Pour $i \geq 2$, la i-ième ligne de A est

$$\begin{pmatrix} a_{n-i+1} & \dots & a_{n-1} & a_0 & \dots & a_{n-i-2} \end{pmatrix}$$

Si on multiplie cette ligne par la j-ième colonne de Ω, on obtient le coefficient

$$\begin{aligned} &a_{n-i+1} + a_{n-i+2}\omega^{j-1} + \dots + a_0\omega^{(j-1)(i-1)} + a_1\omega^{(j-1)i} + \dots + a_{n-i-2}\omega^{(j-1)(n-1)} \\ &= \omega^{(j-1)(i-1)}(a_0 + a_1\omega^{j-1} + \dots + a_{n-1}\omega^{(j-1)(n-1)}) \\ &= \omega^{(j-1)(i-1)}P(\omega^{j-1}) \end{aligned}$$

et c'est encore vrai pour $i = 1$ puisque $\omega^0 = 1$. Donc la j-ième colonne de $A\Omega$ est égale à la j-ième colonne de Ω multipliée par $P(\omega^{j-1})$. Ceci entraîne que

$$\det(A)\det(\Omega) = \det(A\Omega) = P(1)P(\omega)\dots P(\omega^{n-1})\det(\Omega)$$

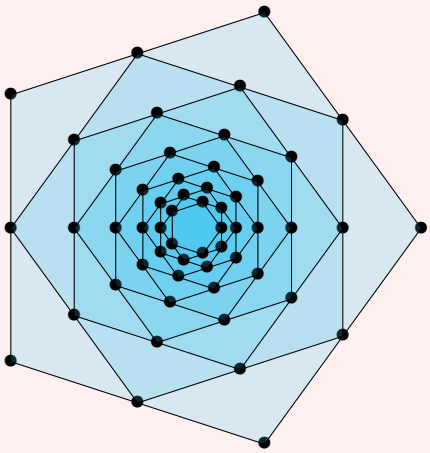
et le déterminant $\det(\Omega)$ est non nul (en tant que déterminant de Vandermonde à paramètres deux-à-deux distincts). D'où :

$$\det(A) = P(1)P(\omega)\dots P(\omega^{n-1})$$

□

[I-P] p. 389

Théorème 2 (Suite de polygones)**.** Soit P_0 un polygone dont les sommets sont $\{z_{0,1},\dots,z_{0,n}\}$. On définit la suite de polygones (P_k) par récurrence en disant que, pour tout $k\in\mathbb{N}^*$, les sommets de P_{k+1} sont les milieux des arêtes de P_k.



Alors la suite (P_k) converge vers l'isobarycentre de P_0.

Démonstration. On identifie P_k au vecteur colonne $Z_k=\begin{pmatrix}z_{k,1}\\ \vdots\\ z_{k,n}\end{pmatrix}\in\mathbb{C}^n$. Il s'agit de montrer que la suite (Z_k) converge vers $\begin{pmatrix}g\\ \vdots\\ g\end{pmatrix}$ où g désigne l'isobarycentre de P_0.

En utilisant la notation matricielle, la relation de récurrence s'écrit

$$\forall k\in\mathbb{N},\ Z_{k+1}=\begin{pmatrix}\frac{z_{k,1}+z_{k,2}}{2}\\ \vdots\\ \frac{z_{k,n}+z_{k,1}}{2}\end{pmatrix}=AZ_k \text{ où } A=\begin{pmatrix}\frac12&\frac12&0&\dots&0\\ 0&\frac12&\frac12&\ddots&\vdots\\ \vdots&\ddots&\ddots&\ddots&\vdots\\ 0&\dots&0&\frac12&\frac12\\ \frac12&0&\dots&0&\frac12\end{pmatrix}$$

Par une récurrence immédiate (c'est une suite géométrique), on a donc $\forall k\in\mathbb{N}, Z_k=A^kZ_0$. Il suffit donc de montrer que (A^k) converge dans $\mathcal{M}_n(\mathbb{C})$ (muni d'une norme quelconque par équivalence des normes en dimension finie).

Pour cela, étudions les valeurs propres de A :

$$\chi_A=\det(A-XI_n)=\begin{vmatrix}a_0&a_1&\dots&a_{n-1}\\ a_{n-1}&a_0&\dots&a_{n-2}\\ \vdots&\vdots&\ddots&\vdots\\ a_1&a_2&\dots&a_0\end{vmatrix}$$

avec $a_0=\frac12-X$, $a_1=\frac12$ et $\forall i>2$, $a_i=0$. On reconnaît le déterminant circulant du Théorème 1 et

en posant $P(Y)=\sum_{k=0}^{n-1}a_kY^k$ et $\omega=e^{\frac{2i\pi}{n}}$, la formule du déterminant circulant nous donne :

$$\chi_A=\prod_{j=1}^{n}P(\omega^j)=\prod_{j=1}^{n}\left(\sum_{k=0}^{n-1}a_k\omega^{kj}\right)=\prod_{j=1}^{n}\left(\frac{1}{2}-X+\frac{1}{2}\omega^j\right)=\prod_{j=1}^{n}(\lambda_j-X)$$

où $\lambda_j=\frac{1+\omega^j}{2}$. Et comme $\lambda_i=\lambda_j\iff i=j$, le polynôme χ_A est scindé à racines simples. Donc $\exists Q\in \mathrm{GL}_n(\mathbb{C})$ telle que $A=QDQ^{-1}$ et $D=\mathrm{Diag}(\lambda_1,\dots,\lambda_n)$. Or pour $j\neq n$,

$$|\lambda_j|=\left|\frac{1+\omega^j}{2}\right|=\left|e^{\frac{ij\pi}{n}}\,\frac{e^{\frac{ij\pi}{n}}+e^{-\frac{ij\pi}{n}}}{2}\right|=\left|\cos\left(\frac{\pi j}{n}\right)\right|<1$$

Ainsi, $\lambda_j^k\longrightarrow 0$ si $j<n$, donc la suite (A^k) converge dans $\mathscr{M}_n(\mathbb{C})$ vers la matrice $B=Q\,\mathrm{Diag}(0,\dots,0,1)Q^{-1}$ par continuité de l'application $M\mapsto QMQ^{-1}$.

On pose donc $X=BZ_0$, de sorte que la suite (Z_k) converge vers X. Par continuité de $M\mapsto AM$, la limite X vérifie forcément $X=AX$ ie. X est vecteur propre de A associé à la valeur propre 1. Or l'espace propre de A associé à la valeur propre 1 contient le vecteur $\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}$ et est de dimension 1 (car χ_A possède n racines distinctes), donc il est engendré par ce vecteur. Ainsi, il existe $a\in\mathbb{C}$ tel que $X=\begin{pmatrix}a\\ \vdots\\ a\end{pmatrix}$ ie. (Z_k) converge vers le point d'affixe a.

Enfin, on remarque que si g est l'isobarycentre de P_0, il est aussi égal à celui de P_k pour tout k (que l'on note g_k) car pour tout $k\geq 1$:

$$g_k=\frac{1}{n}\sum_{i=1}^{n}z_{k,i}=\frac{1}{n}\sum_{i=1}^{n}\frac{z_{k-1,i}+z_{k-1,i+1}}{2}=\frac{1}{n}\sum_{i=1}^{n}z_{k-1,i}=g_{k-1}$$

(en considérant les indices i modulo n). Or, la suite (Z_k) converge vers $\begin{pmatrix}a\\ \vdots\\ a\end{pmatrix}$, et la fonction φ qui à n points du plan associe son isobarycentre est continue. Donc,

$$g_k=\varphi(Z_k)\longrightarrow\varphi(a,\dots,a)=a$$

et comme pour tout k, $g_k=g$, on a bien $g=a$. □

24 $\exp : \mathcal{M}_n(\mathbb{R}) \to \mathrm{GL}_n(\mathbb{R})$ est surjective

Dans ce développement, on démontre que l'exponentielle de matrices est surjective en utilisant des théorèmes d'analyse.

Lemme 1. Soit $M \in \mathrm{GL}_n(\mathbb{C})$. Alors $M^{-1} \in \mathbb{C}[X]$ (ie. M^{-1} est un polynôme en M). **[I-P]** p. 396

Démonstration. D'après le théorème de Cayley-Hamilton, $\chi_M(M) = 0$. Or, en notant $\chi_M = \sum_{k=0}^{n} a_k X^k$, on a $a_0 = (-1)^n \det(M)$, d'où

$$0 = M^n + \cdots + a_1 M + (-1)^n \det(M) I_n$$

En notant $Q = X^{n-1} + a_{n-1}X^{n-2} + \cdots + a_2 X + a_1$, on en déduit que $(-1)^{n+1}\det(M)I_n = Q(M)M$. D'où

$$M^{-1} = \frac{(-1)^{n+1}}{\det(M)} Q(M) \in \mathbb{C}[M]$$

ce qu'il fallait démontrer. □

Lemme 2. Soit $M \in \mathcal{M}_n(\mathbb{C})$. Alors, $\exp(M) \in \mathrm{GL}_n(\mathbb{C})$.

Démonstration. M et $-M$ commutent, donc

$$\exp(M)\exp(-M) = \exp(M - M) = I_n = \exp(-M)\exp(M)$$

Ainsi $\exp(M)$ est inversible, d'inverse $\exp(-M)$. □

Notation 3. Soit $C \in \mathcal{M}_n(\mathbb{C})$. On note $\mathbb{C}[C]^* = \mathbb{C}[C] \cap \mathrm{GL}_n(\mathbb{C})$.

Lemme 4. Soit $C \in \mathcal{M}_n(\mathbb{C})$. $\mathbb{C}[C]^*$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{C})$.

Démonstration.

— $I_n \in \mathbb{C}[C]$ et $I_n \in \mathrm{GL}_n(\mathbb{C})$, donc $I_n \in \mathbb{C}[C]^*$.

— Soit $M \in \mathbb{C}[C]^*$. Comme $M \in \mathrm{GL}_n(\mathbb{C})$, M^{-1} existe, est inversible, et, par le Théorème 1, $M^{-1} \in \mathbb{C}[C]$.

— Enfin, $\mathbb{C}[C]^*$ est clairement stable par multiplication.

□

Lemme 5. exp est différentiable en 0 et,

$$\mathrm{d}\exp_0 = I_n$$

Démonstration. Soit $H \in \mathcal{M}_n(\mathbb{C})$.

$$\begin{aligned}\exp(0+H) - \exp(H) &= \sum_{k=0}^{+\infty} \frac{H^k}{k!} \\ &= I_n + H + \sum_{k=2}^{+\infty} \frac{H^k}{k!}\end{aligned}$$

Soit $\|.\|$ une norme d'algèbre sur $\mathcal{M}_n(\mathbb{C})$. On a :

$$\begin{aligned}\left\| \sum_{k=2}^{+\infty} \frac{H^k}{k!} \right\| &\leq \sum_{k=2}^{+\infty} \left\| \frac{H^k}{k!} \right\| \\ &\leq \sum_{k=2}^{+\infty} \frac{\|H\|^k}{k!} \\ &= e^{\|H\|} - \|H\| - 1\end{aligned}$$

En effectuant un développement limité de l'exponentielle réelle à l'origine, on obtient bien $\left\| \sum_{k=2}^{+\infty} \frac{H^k}{k!} \right\| = o(\|H\|)$. □

Théorème 6. exp : $\mathcal{M}_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$ est surjective.

Démonstration. Fixons $C \in \mathcal{M}_n(\mathbb{C})$ pour le reste de la démonstration. Comme $\mathbb{C}[C]$ est un sous-espace vectoriel de l'espace $\mathcal{M}_n(\mathbb{C})$, il est de dimension finie et est donc fermé. En particulier, $\exp(C) \in \mathbb{C}[C]$. Le Théorème 2 combiné au Théorème 4, nous dit que $\exp : \mathbb{C}[C] \to \mathbb{C}[C]^*$ est bien définie. Il s'agit de plus d'un morphisme de groupes. En effet, $\forall A, B \in \mathbb{C}[C]$, on a $AB = BA$, d'où $\exp(A)\exp(B) = \exp(A+B) = \exp(B)\exp(A)$.

Montrons que $\mathbb{C}[C]^*$ est un ouvert connexe de $\mathbb{C}[C]$. Notons qu'il s'agit bien d'un ouvert de $\mathbb{C}[C]$, car c'est l'intersection de $\mathbb{C}[C]$ avec $\mathrm{GL}_n(\mathbb{C})$ qui est ouvert dans $\mathcal{M}_n(\mathbb{C})$. Ensuite, soient $A, B \in \mathbb{C}[C]^*$. On pose

$$P = \det((1-X)A + XB)$$

P ne s'annule ni en 0, ni en 1 par inversibilité de A et B. P a un nombre fini de racines car n'est pas nul : on peut trouver une fonction continue $\gamma : [0,1] \to \mathbb{C}$ qui évite ces racines. Ainsi,

$$\forall t \in [0,1],\ (1-\gamma(t))A + \gamma(t)B \in \mathbb{C}[C]^*$$

donc $\mathbb{C}[C]^*$ est connexe par arcs, donc est en particulier connexe.

Il s'agit maintenant de montrer que $\exp(\mathbb{C}[C])$ est un ouvert-fermé de $\mathbb{C}[C]^*$. Commençons par montrer qu'il est ouvert en montrant qu'il contient un voisinage de chacun de ses points. Par le théorème d'inversion locale appliqué à $\exp : \mathbb{C}[C] \to \mathbb{C}[C]$ (qui est bien $\mathscr{C}^1$ sur l'espace de Banach $\mathbb{C}[C]$ et, par le Théorème 5, $\det(\mathrm{d}\exp_0) \neq 0$) : il existe U un voisinage de 0 dans $\mathbb{C}(C)$ et un ouvert V de $\mathbb{C}(C)$ contenant $\exp(0) = I_n$ tels que $\exp : U \to V$ soit un difféomorphisme de classe $\mathscr{C}^1$. Soit

$A \in \mathbb{C}[C]$. Posons

$$f_A : \begin{array}{ccc} \mathbb{C}[C] & \to & \mathbb{C}[C] \\ M & \mapsto & \exp(A)^{-1}M \end{array}$$

et montrons que $\exp(A)V = f^{-1}(V)$.Pour tout $B \in V$, $f_A(\exp(A)B) = \exp(A)^{-1}(\exp(A)B) = B \in V$, donc $\exp(A)V \subseteq f^{-1}(V)$.

Soit $B \in f^{-1}(V)$, alors $f_A(B) \in V$. Or, $f_A(B) = \exp(A)^{-1}B$, donc $B = \exp(A)f_A(B) \in \exp(A)V$. On en déduit que $\exp(A)V = f^{-1}(V)$ et que $\exp(A)V$ est un ouvert par continuité de f.

Comme V contient I_n, $\exp(A)V$ est un voisinage de $\exp(A)$. Or, $\exp(A)V$ est inclus dans $\mathbb{C}[C]$ car pour tout $B \in V$, il existe $M \in \mathbb{C}[C]$ tel que $\exp(M) = B$. Ainsi,

$$\exp(A)B = \exp(A)\exp(M) = \exp(A+M) \in \exp(\mathbb{C}[C])$$

On en déduit que $\exp(\mathbb{C}[C])$ est un ouvert.

Posons maintenant $O = \mathbb{C}[C]^* \setminus \exp(\mathbb{C}[C])$ et montrons que

$$O = \bigcup_{A \in O} A\exp(\mathbb{C}[C]) \qquad (*)$$

Soient $A \in O$ et $B \in \exp(\mathbb{C}[C])$. Alors $AB \in \mathbb{C}[C]^*$. Supposons par l'absurde que $AB \in \exp(\mathbb{C}[C])$. Il existe donc $M \in \exp(\mathbb{C}[C])$ tel que $AB = M$ et $A = MB^{-1}$. Comme $\exp(\mathbb{C}[C])$ est un groupe multiplicatif, alors $A \in \exp(\mathbb{C}[C])$: absurde. On conclut que

$$\bigcup_{A \in O} A\exp(\mathbb{C}[C]) \subseteq O$$

Réciproquement, supposons que $M \in O$. Comme $I_n \in \exp(\mathbb{C}[C])$, alors $M \in M\exp(\mathbb{C}[C])$. On en déduit $(*)$, ainsi que la fermeture de $\exp(\mathbb{C}[M])$ par passage au complémentaire.

$\exp(\mathbb{C}[M])$ est un ouvert fermé non vide (car contient I_n) de $\mathbb{C}[M]^*$, alors $\exp(\mathbb{C}[M]) = \mathbb{C}[M]^*$. Pour conclure, si $M \in \mathrm{GL}_n(\mathbb{C})$, alors $M \in \mathbb{C}[M]$ et donc $M \in \mathbb{C}[M]^*$. Ainsi, $M \in \exp(\mathbb{C}[M])$, et exp est bien surjective. □

Application 7. $\exp(\mathcal{M}_n(\mathbb{R})) = \mathrm{GL}_n(\mathbb{R})^2$, où $\mathrm{GL}_n(\mathbb{R})^2$ désigne les carrés de $\mathrm{GL}_n(\mathbb{R})$.

Démonstration. Soit $M \in \mathcal{M}_n(\mathbb{R})$. Alors,

$$\exp(M) = \exp\left(\frac{M}{2}\right)^2$$

d'où $\exp(\mathcal{M}_n(\mathbb{R})) \subseteq \mathrm{GL}_n(\mathbb{R})^2$. Réciproquement, soit $A \in \mathrm{GL}_n(\mathbb{R})^2$. Posons $B = A^2$. D'après le Théorème 6,

$$\exists P \in \mathbb{C}[X] \text{ telle que } A = \exp(P(A))$$

Comme A est une matrice réelle, alors en passant au conjugué, on obtient $A = \exp(\overline{P}(A))$. Ainsi,

$$B = A^2 = \exp((P+\overline{P})(A)) \in \exp(\mathcal{M}_n(\mathbb{R}))$$

d'où $\mathrm{GL}_n(\mathbb{R})^2 \subseteq \exp(\mathcal{M}_n(\mathbb{R}))$. □

25 Théorème central limite

En établissant d'abord le théorème de Lévy, on démontre le théorème central limite, qui dit que si (X_n) est une suite de variables aléatoires identiquement distribuées admettant un moment d'ordre 2, alors $\frac{X_1+\cdots+X_n-n\mathbb{E}(X_1)}{\sqrt{n}}$ converge en loi vers $\mathcal{N}(0,\mathrm{Var}(X_1))$.

Notation 1. Si X est une variable aléatoire réelle, on note ϕ_X sa fonction caractéristique.

Théorème 2 (Lévy)**.** Soient (X_n) une suite de variables aléatoires réelles définies sur un espace probabilité $(\Omega,\mathcal{A},\mathbb{P})$ et X une variable aléatoire réelle définie sur le même espace. Alors :

$$X_n \xrightarrow{(d)} X \iff \phi_{X_n} \text{ converge simplement vers } \phi_X$$

[Z-Q] p. 544

Démonstration. Sens direct : On suppose que (X_n) converge en loi vers X. Pour tout $t\in\mathbb{R}$, la fonction $g_t : x \mapsto e^{itx}$ est continue et bornée sur $\mathbb{R}$. Donc par définition de la convergence en loi :

$$\lim_{n\to+\infty} \mathbb{E}(g_t(X_n)) = \mathbb{E}(g_t(X))$$

ce que l'on voulait.

Réciproque : Soit $\varphi\in L_1(\mathbb{R})$. On suppose que sa transformée de Fourier, $f=\widehat{\varphi}$ appartient également à $L_1(\mathbb{R})$. Alors

$$\mathbb{E}(f(X_n)) = \mathbb{E}\left(\int_{\mathbb{R}} e^{itX_n}\varphi(t)\,\mathrm{d}t\right)$$

Comme la fonction $(\omega,t)\mapsto e^{itX_n(\omega)}\varphi(t)$ est intégrable pour la mesure $\mathbb{P}\otimes\lambda$, on peut appliquer le théorème de Fubini-Lebesgue pour intervertir espérance et intégrale :

$$\mathbb{E}(f(X_n)) = \int_{\mathbb{R}} \mathbb{E}(e^{itX_n})\varphi(t)\,\mathrm{d}t$$

On définit maintenant la suite de fonction $g_n : t\mapsto \mathbb{E}(e^{itX_n})\varphi(t)$. Alors :

- $\forall n\in\mathbb{N}$, g_n est mesurable.
- La suite de fonction (g_n) converge presque partout vers $g : t\mapsto \mathbb{E}(e^{itX})\varphi(t)$ par hypothèse.
- $\forall n\in\mathbb{N}$ et pp. en $t\in\mathbb{R}$, $|g_n(t)|\leq \mathbb{E}(|e^{itX_n}|)|\varphi(t)| \leq \mathbb{P}(\Omega)|\varphi(t)| = |\varphi(t)|$ avec $|\varphi|\in L_1(\mathbb{R})$.

On peut donc appliquer le théorème de convergence dominée pour obtenir

$$\mathbb{E}(f(X_n)) \longrightarrow \int_{\mathbb{R}} \mathbb{E}(e^{itX})\varphi(t)\,\mathrm{d}t = \mathbb{E}(f(X))$$

Ainsi, le résultat est vrai pour toute fonction $L_1(\mathbb{R})$ dans l'image de $L_1(\mathbb{R})$ par la transformée de Fourier. En particulier, il est vrai pour tout $f\in\mathcal{S}(\mathbb{R})$, dense dans $(\mathcal{C}(\mathbb{R}),\|.\|_\infty)$. Soient maintenant

$f \in \mathscr{C}(\mathbb{R})$ et (f_k) une suite de fonctions de $\mathscr{S}(\mathbb{R})$ qui converge uniformément vers f. Alors,

$$\begin{aligned}|\mathbb{E}(f(X_n)) - \mathbb{E}(f(X))| &= |\mathbb{E}(f(X_n)) - \mathbb{E}(f_k(X_n)) + \mathbb{E}(f_k(X_n)) \\ &\quad - \mathbb{E}(f_k(X)) + \mathbb{E}(f_k(X)) - \mathbb{E}(f(X))| \\ &\leq 2\|f - f_k\|_\infty + |\mathbb{E}(f_k(X_n)) - \mathbb{E}(f_k(X))| \\ &\longrightarrow 0\end{aligned}$$

□

Lemme 3. Soient $u, v \in \mathbb{C}$ de module inférieur ou égal à 1 et $n \in \mathbb{N}^*$. Alors

$$|z^n - u^n| \leq n|z-u|$$

[G-K] p. 307

Démonstration. $|z^n - u^n| = |(z-u)\sum_{k=0}^{n-1} z^k u^{n-1-k}| \leq n|z-u|$. □

Théorème 4 (Central limite)**.** Soit (X_n) une suite de variables aléatoires réelles indépendantes de même loi admettant un moment d'ordre 2. On note m l'espérance et σ^2 la variance commune à ces variables. On pose $S_n = X_1 + \cdots + X_n - nm$. Alors,

$$\left(\frac{S_n}{\sqrt{n}}\right) \xrightarrow{(d)} \mathscr{N}(0, \sigma^2)$$

Démonstration. On a $S_n = \sum_{k=1}^n (X_k - m)$. Notons ϕ la fonction caractéristique de $X_1 - m$. Comme les variables aléatoires $X_1 - m, \ldots, X_n - m$ sont indépendantes de même loi, la fonction caractéristique de $\frac{S_n}{\sqrt{n}}$ vaut $\forall t \in \mathbb{R}$,

$$\begin{aligned}\phi_{\frac{S_n}{\sqrt{n}}}(t) &= \mathbb{E}\left(e^{iS_n\left(\frac{t}{\sqrt{n}}\right)}\right) \\ &= \mathbb{E}\left(\prod_{k=1}^n e^{i(X_k-m)\left(\frac{t}{\sqrt{n}}\right)}\right) \\ &= \prod_{k=1}^n \phi_{X_k-m}\left(\frac{t}{\sqrt{n}}\right) \\ &= \phi\left(\frac{t}{\sqrt{n}}\right)^n\end{aligned}$$

D'après le Théorème 2, pour montrer que $\frac{S_n}{\sqrt{n}}$ converge en loi vers $\mathscr{N}(0,\sigma^2)$, il suffit de montrer que

$$\forall t \in \mathbb{R},\ \lim_{n\to+\infty} \phi\left(\frac{t}{\sqrt{n}}\right)^n = e^{-\frac{\sigma^2}{2}t^2}$$

car $t \mapsto e^{-\frac{\sigma^2}{2}t^2}$ est la fonction caractéristique de la loi $\mathscr{N}(0,\sigma^2)$.

Comme X_1 admet un moment d'ordre 2, ϕ est de classe $\mathscr{C}^2$ et

— $\phi(0) = 1$.

— $\phi'(0) = i^1\mathbb{E}(X_1^1) = 0$.

— $\phi''(0) = i^2\mathbb{E}(X_1^2) = -E(X^2) = -\sigma^2$ (car $m = 0$).

Ce qui donne le développement limité en 0 de ϕ à l'ordre 2 (par la formule de Taylor-Young) :

$$\phi(t) = \phi(0) + \frac{\phi'(0)}{1!}(t-0) + \frac{\phi''(0)}{2!}(t-0)^2 + o(t^2) = 1 - \frac{\sigma^2 t^2}{2} + o(t^2) \qquad (*)$$

Et, en appliquant le Théorème 3 :

$$\begin{aligned}\left|\phi\left(\frac{t}{\sqrt{n}}\right)^n - e^{-\frac{\sigma^2}{2}t^2}\right| &= \left|\phi\left(\frac{t}{\sqrt{n}}\right)^n - \left(e^{-\frac{\sigma^2}{2n}t^2}\right)^n\right| \\ &\leq n\left|\phi\left(\frac{t}{\sqrt{n}}\right) - e^{-\frac{\sigma^2}{2n}t^2}\right|\end{aligned}$$

On a d'une part, par développement limité :

$$e^{-\frac{\sigma^2}{2n}t^2} = 1 - \frac{\sigma^2}{2n}t^2 + o\left(\frac{1}{n}\right)$$

Et d'autre part, par $(*)$:

$$\phi\left(\frac{t}{\sqrt{n}}\right) = 1 - \frac{\sigma^2}{2n}t^2 + o\left(\frac{1}{n}\right)$$

On obtient ainsi le résultat cherché, à savoir :

$$n\left|\phi\left(\frac{t}{\sqrt{n}}\right) - e^{-\frac{\sigma^2}{2n}t^2}\right| = o(1)$$

□

26 Théorème chinois

On montre le théorème chinois et on propose une application à la résolution d'un système de congruences.

Soit A un anneau principal. Soient $r \geq 2$ un entier et $a_1, \dots, a_r \in A$ des éléments premiers entre eux deux à deux. **[ROM21]** p. 250

Notation 1. Pour tout $i \in [\![1, r]\!]$, on note

$$\pi_i = \pi_{(a_i)} : A \to A/(a_i)$$

la surjection canonique de A sur $A/(a_i)$. On note également $\pi = \pi_{(a_1 \dots a_r)} : A \to A/(a_1 \dots A_r)$.

Théorème 2 (Chinois)**.** Alors :

(i) L'application :

$$\varphi : \begin{array}{ccc} A & \to & A/(a_1) \times \cdots \times A/(a_r) \\ x & \mapsto & (\pi_1(x), \dots, \pi_r(x)) \end{array}$$

est un morphisme d'anneaux de noyau $\mathrm{Ker}(\varphi) = (a_1 \dots a_r)$.

(ii) Il existe $u_1, \dots, u_r \in A$ tels que

$$\sum_{i=1}^{r} u_i b_i = 1$$

où $\forall i \in [\![1, r]\!]$, $b_i = \frac{a}{a_i}$ et $a = a_1 \dots a_r$.

(iii) φ est surjectif et induit un isomorphisme $\overline{\varphi} : A/(a_1 \dots a_r) \to A/(a_1) \times \cdots \times A/(a_r)$. On a,

$$\overline{\varphi}^{-1} : \begin{array}{ccc} A/(a_1) \times \cdots \times A/(a_r) & \to & A/(a_1 \dots a_r) \\ (\pi_1(x_1), \dots, \pi_r(x_r)) & \mapsto & \pi\left(\sum_{i=1}^{r} x_i u_i b_i\right) \end{array}$$

où π est la surjection canonique de A sur le quotient $A/(a_1 \dots a_r)$.

Démonstration. (i) On vérifie sans difficulté que φ est un morphisme d'anneaux (du fait que les projections canoniques sur les quotients en sont). De là,

$$\begin{aligned} \mathrm{Ker}(\varphi) &= \{x \in A \mid \forall i \in [\![1, r]\!], \pi_i(x) = 0\} \\ &= \{x \in A \mid \forall i \in [\![1, r]\!], a_i \mid x\} \\ &= \{x \in A \mid \mathrm{ppcm}(a_1, \dots, a_r) \mid x\} \end{aligned}$$

Mais, $a_1, \dots, a_r$ sont premiers entre eux deux à deux. Donc,

$$\mathrm{ppcm}(a_1, \dots, a_r) = a_1 \dots a_r$$

et on conclut que $\mathrm{Ker}(\varphi) = (a_1 \dots a_r)$.

(ii) Supposons par l'absurde que $b_1, \dots, b_r$ ne sont pas premiers entre eux dans leur ensemble.

Comme A est principal, donc factoriel, il existe un premier $p \in A$ tel que

$$\forall i \in [\![1,r]\!],\ p \mid b_i$$

Comme p divise $b_1 = a_2 \dots a_r$, il existe $i \in [\![2,r]\!]$ tel que $p \mid a_i$. Mais, divisant b_i, il divise a_j où $j \in [\![1,r]\!] \setminus \{i\}$. Contradiction car a_1 et a_j sont premiers entre eux. La fin du raisonnement est une conséquence directe du théorème de Bézout valable dans les anneaux principaux.

(iii) Pour $i,j \in [\![1,r]\!]$ tels que $i \neq j$, on a

$$\pi_j(b_i) = \pi_j(0)$$

puisque b_i est multiple de a_j. Ceci permet d'écrire

$$\pi_j(1) = \pi_j\left(\sum_{i=1}^{r} u_i b_i\right) = \pi_j(u_j)\pi_j(b_j)$$

Donc, $\pi_j(b_j)$ est inversible dans $A/(a_j)$, d'inverse $\pi_j(u_j)$. Ainsi, soient $\pi_1(x_1), \dots, \pi_r(x_r) \in A/(a_1) \times \cdots \times A/(a_r)$. En posant

$$x = \sum_{i=1}^{r} x_i u_i b_i$$

on a

$$\pi_j(x) = \pi_j(x_j)\pi_j(u_j)\pi_j(b_j) = \pi_j(x_j)$$

donc $\varphi(x) = (\pi_1(x_1), \dots, \pi_r(x_r))$. Le morphisme φ est surjectif. Par le théorème de factorisation des morphismes, il induit un isomorphisme

$$\overline{\varphi} : \begin{array}{ccc} A/(a_1 \dots a_r) & \to & A/(a_1) \times \cdots \times A/(a_r) \\ \pi(x) & \mapsto & (\pi_1(x), \dots, \pi_r(x)) \end{array}$$

et on a même prouvé que l'inverse $\overline{\varphi}^{-1}$ est défini par

$$\overline{\varphi}^{-1} : \begin{array}{ccc} A/(a_1) \times \cdots \times A/(a_r) & \to & A/(a_1 \dots a_r) \\ (\pi_1(x_1), \dots, \pi_r(x_r)) & \mapsto & \pi\left(\sum_{i=1}^{r} x_i u_i b_i\right) \end{array}$$

□

Exemple 3. Le système

$$\begin{cases} u \equiv 1 \mod 3 \\ u \equiv 3 \mod 5 \\ u \equiv 0 \mod 7 \end{cases}$$

admet une unique solution dans $\mathbb{Z}/105\mathbb{Z} : \overline{28}$. Les solutions dans $\mathbb{Z}$ sont donc de la forme $28 + 105k$ avec $k \in \mathbb{Z}$.

[ULM18] p. 58

Démonstration. On se place dans l'anneau principal $A = \mathbb{Z}$. Les entiers 3, 5 et 7 sont premiers entre eux : le triplet $(1+(3), 3+(5), 0+(7)) = (x_1+(3), x_2+(5), x_3+(3))$ admet un unique antécédent

par $\overline{\varphi}^{-1}$ du Théorème 2. On a ainsi existence et unicité d'une solution modulo $3 \times 5 \times 7 = 105$. On explicite une relation de Bézout pour $15, 21, 35$:

$$\underbrace{-1}_{=u_1} \times \underbrace{35}_{=b_1} + \underbrace{6}_{=u_2} \times \underbrace{21}_{=b_2} + \underbrace{(-6)}_{=u_3} \times \underbrace{15}_{=b_3} = 1$$

Reste à calculer

$$\begin{aligned}\overline{\varphi}^{-1}(1+(3), 3+(5), 0+(7)) &= \sum_{i=1}^{3} x_i u_i b_i + (105) \\ &= 1 \times (-1) \times 35 + 3 \times 6 \times 21 + 0 \times (-6) \times 15 + (105) \\ &= 343 + (105) \\ &= 28 + (105)\end{aligned}$$

Les solutions sont bien de la forme escomptée. □

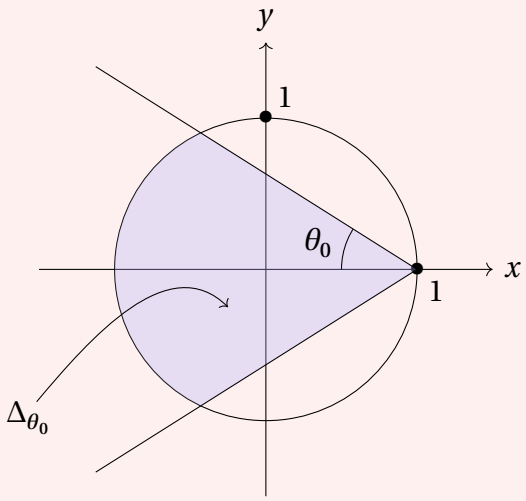
[ULM18] utilise un autre algorithme pour trouver la solution. Le fait de chercher un antécédent permet de faire un lien "direct" avec le Théorème 2. Attention, il faut réussir à trouver les coefficients de Bézout…

27 Théorème d'Abel angulaire

On montre le théorème d'Abel "angulaire", qui permet d'intervertir certaines sommes et limites, et on l'applique justement au calcul de deux sommes.

Théorème 1 (Abel angulaire)**.** Soit $\sum a_n z^n$ une série entière de rayon de convergence supérieur ou égal à 1 telle que $\sum a_n$ converge. On note f la somme de cette série sur le disque unité D de $\mathbb{C}$. On fixe $\theta_0 \in \left[0, \frac{\pi}{2}\right[$ et on pose $\Delta_{\theta_0} = \{z \in D \mid \exists \rho > 0 \text{ et } \exists \theta \in [-\theta_0, \theta_0] \text{ tels que } z = 1 - \rho e^{i\theta}\}$.

[GOU20] p. 263



Alors $\lim\limits_{\substack{z\to 1\\ z\in\Delta_{\theta_0}}} f(z) = \sum_{n=0}^{+\infty} a_n$.

Démonstration. On note $\forall n \in \mathbb{N}$, $S = \sum_{n=0}^{+\infty} a_n$, $S_n = \sum_{k=0}^{n} a_k$ et $R_n = S - S_n$. On chercher à majorer $|f(z) - S|$; on va effectuer une transformation d'Abel en écrivant $\forall n \geq 1$, $a_n = R_{n-1} - R_n$. Soit $z \in D \setminus \{0\}$. $\forall N \in \mathbb{N}^*$, on a

$$\begin{aligned}
\sum_{n=0}^{N} a_n z^n - S_N &= \sum_{n=0}^{N} a_n (z^n - 1) \\
&= \sum_{n=1}^{N} (R_{n-1} - R_n)(z^n - 1) \\
&= \sum_{n=0}^{N-1} R_n (z^{n+1} - 1) - \sum_{n=1}^{N} R_n (z^n - 1) \\
&= \sum_{n=0}^{N-1} R_n (z^{n+1} - z^n) - R_N (z^N - 1) \\
&= (z-1) \sum_{n=0}^{N-1} R_n z^n - R_N (z^N - 1)
\end{aligned}$$

Donc en faisant $N \to +\infty$:

$$f(z) - S = (z-1) \sum_{n=0}^{+\infty} R_n z^n \qquad (*)$$

Soit $\epsilon > 0$. $\exists N \in \mathbb{N}$ tel que $\forall n \geq N$, $|R_n| < \epsilon$. D'après $(*)$, $\forall z \in D$,

$$\begin{aligned} |f(z) - S| &\leq |z-1| \left| \sum_{n=0}^{N} R_n z^n \right| + \epsilon |z-1| \left(\sum_{n=N+1}^{+\infty} |z|^n \right) \\ &\leq |z-1| \left(\sum_{n=0}^{N} |R_n| \right) + \epsilon \frac{|z-1|}{1-|z|} \end{aligned} \tag{$**$}$$

Soit $z \in \Delta_{\theta_0}$ de sorte que $z = 1 - \rho e^{i\theta}$ avec $\rho > 0$ et $|\theta| \leq \theta_0$. Notons avant toute chose que $|z-1| = \rho$. Cherchons maintenant des conditions sur z pour majorer les deux termes :

— On a :

$$\begin{aligned} |z|^2 &= (1 - \rho\cos(\theta))^2 + (\rho\sin(\theta))^2 \\ &= 1 - 2\rho\cos(\theta) + \rho^2(\cos(\theta)^2 + \sin(\theta)^2) \\ &= 1 - 2\rho\cos(\theta) + \rho^2 \end{aligned}$$

En supposant $\rho \leq \cos(\theta_0)$, cela permet de majorer le deuxième terme de $(**)$:

$$\begin{aligned} \frac{|z-1|}{1-|z|} &= \frac{|z-1|}{1-|z|^2}(1+|z|) \\ &= \frac{\rho}{2\rho\cos(\theta) - \rho^2}(1+|z|) \\ &\leq \frac{2}{2\cos(\theta) - \rho} \\ &\leq \frac{2}{2\cos(\theta_0) - \cos(\theta_0)} \\ &= \frac{2}{\cos(\theta_0)} \end{aligned}$$

— Soit $\alpha > 0$ suffisamment petit pour que $\alpha \sum_{n=0}^{N} |R_n| < \epsilon$. Si $z \in \Delta_{\theta_0}$ tel que $|z-1| \leq \alpha$, alors on peut majorer le premier terme de $(**)$:

$$|z-1| \left(\sum_{n=0}^{N} |R_n| \right) \leq \alpha \left(\sum_{n=0}^{N} |R_n| \right) < \epsilon$$

Donc, en faisant $z \longrightarrow 1$ tel que $z \in \Delta_{\theta_0}$ (on aura bien $\rho = |z-1| \leq \inf\{\alpha, \cos(\theta_0)\}$), et en injectant les deux majorations trouvées dans $(**)$:

$$|f(z) - S| \leq \epsilon + \epsilon \frac{2}{\cos(\theta_0)} = \epsilon \left(1 + \frac{2}{\cos(\theta_0)} \right)$$

d'où le résultat. □

Application 2.

$$\sum_{n=0}^{+\infty} \frac{(-1)^n}{(2n+1)} = \frac{\pi}{4}$$

Démonstration. En appliquant le Théorème 1 :

$$\begin{aligned}\sum_{n=0}^{+\infty}\frac{(-1)^n}{(2n+1)} &= \lim_{\substack{x\to 1\\ x<1}}\sum_{n=0}^{+\infty}\frac{(-1)^n}{(2n+1)}x^n\\ &\overset{x>0}{=} \lim_{\substack{x\to 1\\ x<1}}\frac{1}{\sqrt{x}}\sum_{n=0}^{+\infty}\frac{(-1)^n}{(2n+1)}\sqrt{x}^{2n+1}\\ &= \lim_{\substack{x\to 1\\ x<1}}\frac{1}{\sqrt{x}}\arctan(\sqrt{x})\\ &= \arctan(1)\\ &= \frac{\pi}{4}\end{aligned}$$

□

La preuve de l'application précédente écrite dans **[GOU20]** est un peu lacunaire. Merci aux personnes qui l'ont signalée et corrigée.

Application 3.

$$\sum_{n=0}^{+\infty}\frac{(-1)^{n-1}}{n} = \ln(2)$$

Démonstration. Toujours en appliquant le Théorème 1 :

$$\begin{aligned}\sum_{n=0}^{+\infty}\frac{(-1)^{n-1}}{n} &= \lim_{\substack{x\to 1\\ x<1}}\sum_{n=0}^{+\infty}\frac{(-1)^{n-1}}{n}x^n\\ &= \lim_{\substack{x\to 1\\ x<1}}\ln(1+x)\\ &= \ln(2)\end{aligned}$$

□

28 Théorème de Cauchy-Lipschitz linéaire

En construisant un raisonnement autour du théorème du point fixe de Banach, on montre le théorème de Cauchy-Lipschitz, qui garantit l'existence d'une solution répondant à une condition initiale et l'unicité d'une solution maximale.

Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Lemme 1. Soit I un intervalle compact. L'espace $(\mathscr{C}(I, \mathbb{K}^d), \|.\|_\infty)$ est complet.

Démonstration. Soit (f_n) une suite de Cauchy de $(\mathscr{C}(I, \mathbb{K}^d), \|.\|_\infty)$. Soit $x \in I$, on a

$$\forall p, q \in \mathbb{N}, |f_p(x) - f_q(x)| \leq \|f_p - f_q\|_\infty$$

donc $(f_n(x))$ est de Cauchy dans $\mathbb{K}$. Comme $\mathbb{K}$ est complet, la suite $(f_n(x))$ converge vers une limite notée $f(x)$. Ainsi, la suite de fonctions (f_n) converge simplement vers la fonction $f : I \to \mathbb{K}$ nouvellement définie. Il reste à montrer que la fonction f est continue.

Notons déjà que (f_n) est de Cauchy, et est en particulier bornée :

$$\exists M \geq 0 \text{ tel que } \|f_n\|_\infty \leq M$$

donc en particulier, si $x \in I$, $|f_n(x)| \leq M$. Par passage à la limite, on obtient $|f(x)| \leq M$. Donc f est bornée et écrire $\|f\|_\infty$ a bien du sens.

Soit $\epsilon > 0$. Par définition,

$$\exists N \in \mathbb{N} \text{ tel que } \forall p, q \geq N, \|f_p - f_q\|_\infty < \epsilon$$

Donc,

$$\forall x \in I, \forall p, q \geq N, |f_p(x) - f_q(x)| \leq \|f_p - f_q\|_\infty < \epsilon$$

En faisant tendre p vers l'infini, on obtient :

$$\forall x \in I, \forall q \geq N, |f(x) - f_q(x)| < \epsilon$$

Nous venons d'écrire exactement la définition de la convergence uniforme ! Ainsi, (f_n) est une suite de fonctions continues qui converge uniformément vers f, donc f est continue. □

Théorème 2 (Cauchy-Lipschitz linéaire)**.** Soient $A : I \to \mathcal{M}_d(\mathbb{K})$ et $B : I \to \mathbb{K}^d$ deux fonctions continues. Alors $\forall t_0 \in I$, le problème de Cauchy

$$\begin{cases} Y' = A(t)Y + B(t) \\ Y(t_0) = y_0 \end{cases} \qquad (C)$$

admet une unique solution définie sur I tout entier.

[DAN] p. 520

Démonstration. Commençons par supposer l'intervalle I compact. On va montrer l'existence d'une solution globale. On écrit l'équation sous forme intégrale :

$$Y \in \mathscr{C}^1 \text{ vérifie } (C) \iff Y(t) = y_0 + \int_{t_0}^{t} A(u)Y(u) + B(u)\,\mathrm{d}u \qquad (*)$$

et on introduit la suite de fonctions (Y_n) définie par récurrence sur I par $Y_0 = y_0$ et :

$$\forall n \in \mathbb{N}^*,\ Y_{n+1}(t) = y_0 + \int_{t_0}^{t} A(u)Y_n(u) + B(u)\,\mathrm{d}u \qquad (**)$$

Notons $\alpha = \sup_{t\in I} \|A(t)\|$ et $\beta = \sup_{t\in I} \|B(t)\|$. Montrons par récurrence que pour tout $n \geq 1$ et tout $t \in I$:

$$\|Y_n(t) - Y_{n-1}(t)\| \leq (\alpha\|y_0\| + \beta)\frac{\alpha^{n-1}|t-t_0|^n}{n!}$$

Le résultat est clairement vrai pour $n = 1$, supposons donc le vrai à rang $n \geq 1$. Pour $t \geq t_0$:

$$\begin{aligned}
\|Y_{n+1}(t) - Y_n(t)\| &= \left\| \int_{t_0}^{t} A(u) \times (Y_n(u) - Y_{n-1}(u))\,\mathrm{d}u \right\| \\
&\leq \alpha \int_{t_0}^{t} (\alpha\|y_0\| + \beta)\frac{\alpha^{n-1}|u-t_0|^n}{n!}\mathrm{d}u \\
&\leq (\alpha\|y_0\| + \beta)\frac{\alpha^n|t-t_0|^{n+1}}{(n+1)!}
\end{aligned}$$

et on procède de même pour $t \leq t_0$, ce qui achève la récurrence.

Soit L la longueur de I. On obtient donc :

$$\forall n \in \mathbb{N}^*,\ \|Y_n - Y_{n-1}\|_\infty \leq (\alpha\|y_0\| + \beta)\frac{\alpha^{n-1}}{n!}L^n$$

Il en résulte que la série de fonction $\sum(Y_n - Y_{n-1})$ est normalement convergente. Comme $(\mathscr{C}(I,\mathbb{K}^d), \|.\|_\infty)$ est complet, la série est uniformément convergente. On a donc l'existence d'une fonction $Y \in \mathscr{C}(I,\mathbb{K}^d)$ telle que

$$\left\| \sum_{n=1}^{N} (Y_n - Y_{n-1}) - Y \right\|_\infty = \|Y_n - (Y + Y_0)\|_\infty \longrightarrow 0$$

ie. (Y_n) converge vers $Y + Y_0 = Y + y_0 = Z$. Par convergence uniforme sur un intervalle compact, il est possible de passer à la limite dans $(**)$. D'où :

$$\forall t \in I,\ Z(t) = y_0 + \int_{t_0}^{t} A(u)Z(u) + B(u)\,\mathrm{d}u$$

et comme Z est continue, elle est $\mathscr{C}^1$ et vérifie donc bien $(*)$.

On peut maintenant montrer l'unicité. Soient Y et Z deux solutions de (C) sur I. Par récurrence sur l'entier n, on montre comme ci-dessus que pour tout $t \in I$:

$$\|Y(t) - Z(t)\| \leq \frac{\alpha^n|t-t_0|^n}{n!}\|Y - Z\|_\infty \longrightarrow 0$$

donc Y et Z coïncident bien sur I.

Supposons maintenant I quelconque. Il existe donc (K_n) une suite croissante d'intervalles compacts telle que $I = \bigcup_{n=0}^{+\infty} K_n$. En particulier, on définit bien l'application

$$\theta : \begin{array}{ccc} I & \to & \mathbb{K}^d \\ t & \mapsto & Y_n(t) \end{array}$$

(où Y_n est la solution de (C) sur $K_n \ni t$). En particulier, θ est dérivable sur I tout entier, vérifie (C), et prolonge toute solution. □

La preuve, telle qu'elle est écrite ici, est en grande partie issue d'un livre d'Alain Pommellet. Elle est également disponible (sous une forme un peu différente) comme l'indique la référence, dans **[DAN]**. Selon la leçon, on pourra préférer le théorème suivant (dont la démonstration utilise des arguments semblables).

[GOU20] p. 374

Théorème 3 (Cauchy-Lipschitz local)**.** Soient I un intervalle de $\mathbb{R}$ et Ω un ouvert de E. Soit $F : I \times \Omega \to E$ une fonction continue et localement lipschitzienne en la seconde variable. Alors, pour tout $(t_0, y_0) \in I \times \Omega$, le problème de Cauchy

$$\begin{cases} y' = F(t,y) \\ y(t_0) = y_0 \end{cases} \qquad (C)$$

admet une unique solution maximale.

Démonstration. Nous commençons par montrer l'existence en 4 étapes.

— Localisation : Fixons un réel $r > 0$ tel que le produit $P = [t_0 - r, t_0 + r] \times \overline{B}(y_0, r)$ soit contenu dans $I \times \Omega$. F est continue sur P qui est compact, donc est bornée par M sur P.

— Mise sous forme intégrale : Comme une solution de $y' = F(t,y)$ est de ce fait $\mathscr{C}^1$, on a

$$y \in \mathscr{C}^1 \text{ vérifie } (C) \iff y(t) = y_0 + \int_{t_0}^{t} F(u, y(u))\,\mathrm{d}u \qquad (*)$$

— Choix d'un domaine stable : Soit $\alpha \in]0, r[$. Introduisons l'intervalle $I_\alpha = [t_0 - \alpha, t_0 + \alpha]$, l'espace $A_\alpha = \mathscr{C}(I_\alpha, \overline{B}(y_0, r))$, puis l'application

$$\Psi : \begin{array}{ccc} A_\alpha & \to & \mathscr{C}(I_\alpha, E) \\ \varphi & \mapsto & \left(t \mapsto y_0 + \int_{t_0}^{t} F(u, \varphi(u))\,\mathrm{d}u\right) \end{array}$$

Le problème est ici de rendre A_α stable par Ψ. Pour tout $t \in I_\alpha$,

$$\begin{aligned} &\|F(t, \varphi(t))\| \leq M \\ \implies &\|\Psi(\varphi)(t) - y_0\| \leq M|t - t_0| \leq \alpha M \end{aligned}$$

Par suite, en choisissant $\alpha M < r$, le domaine A_α est stable par Ψ.

— Détermination d'un domaine de contraction : Ici, A_α est normé par la norme $\|.\|_\infty$, et on veut faire de Ψ une contraction stricte. Soient $\varphi, \phi \in A_\alpha$, par définition, pour tout $t \in I_\alpha$,

$$\begin{aligned}\|(\Psi(\varphi)-\Psi(\phi))(t)\| &= \left\| \int_{t_0}^{t} (F(u,\varphi(u)) - F(u,\phi(u)))\,\mathrm{d}u \right\| \\ &\leq k|t-t_0|\,\|\varphi-\phi\|_\infty \\ &\leq k\alpha\,\|\varphi-\phi\|_\infty\end{aligned}$$

où k désigne le rapport de lipschitziannité de F. On choisit désormais α tel que $k\alpha < 1$ et $\alpha M < r$.

— Conclusion : L'application Ψ est, par choix de α, une contraction stricte de $(A_\alpha, \|.\|_\infty)$ dans lui-même. Le fermé $\overline{B}(y_0, r)$ de l'espace de Banach de E est complet, par suite $(A_\alpha, \|.\|_\infty)$ l'est aussi.

Par le théorème du point fixe de Banach, Ψ possède donc un point fixe φ dans A_α. φ est alors de classe $\mathscr{C}^1$ et vérifie (C) par $(*)$.

Il reste maintenant à montrer l'unicité. On note $\mathscr{S}$ l'ensemble des solutions de (C). $\mathscr{S} \neq \emptyset$, donc peut définir J comme la réunion des intervalles de définition des solutions de (C).

Soient $\varphi, \phi \in \mathscr{S}$ (on note K et L leur intervalle de définition). Une récurrence sur n donne

$$\begin{aligned}\forall t \in K \cap L,\ \forall n \in \mathbb{N},\ \|\varphi(t)-\phi(t)\| &\leq \left| \int_{t_0}^{t} \|F(u,\varphi(u)) - F(u,\phi(u))\|\,\mathrm{d}u \right| \\ &\leq \frac{|t-t_0|^n}{n!} k^n \sup_{t\in K\cap L} |\varphi(t)-\phi(t)| \\ &\longrightarrow 0\end{aligned}$$

Donc φ et ϕ coïncident sur $K \cap L$.

Ainsi, on définit correctement l'application

$$\theta : \begin{array}{ccc} J & \to & E \\ t & \mapsto & \phi(t) \end{array}$$

(où $\phi \in S$ tel que t est dans son intervalle de définition). Si $t \in J$, il existe $\phi \in \mathscr{S}$ tel que t soit dans son intervalle de définition K. Comme ϕ et θ coïncident sur K, θ est dérivable sur K et

$$\forall t \in K,\ \theta'(t) = \phi'(t) = F(t,\phi(t)) = F(t,\theta(t))$$

Et comme $\theta(t_0) = y_0$, $\theta \in \mathscr{S}$ et prolonge toute solution. Donc θ est maximale et est bien unique. □

29 Théorème de Dirichlet faible

En raisonnant par l'absurde et en utilisant certaines propriétés des polynômes cyclotomiques, on démontre que l'ensemble des premiers congrus à 1 modulo un certain entier n est infini.

Lemme 1. Soient $a \in \mathbb{N}$ et p premier tels que $p \mid \Phi_n(a)$ mais $p \nmid \Phi_d(a)$ pour tout diviseur strict d de n. Alors $p \equiv 1 \mod n$ ou $p \mid n$.

[GOU21] p. 99

Démonstration. On a,

$$X^n - 1 = \prod_{d|n} \Phi_d = \Phi_n \underbrace{\prod_{d||n} \Phi_d}_{=F}$$

Comme $F \in \mathbb{Z}[X]$, en évaluant en a :

$$a^n - 1 = \Phi_n(a)F(a) \implies p \mid a^n - 1 \text{ car } F(a) \in \mathbb{Z}$$

Autrement dit, $a^n \equiv 1 \mod p$. En notant m l'ordre de $\overline{a}$ dans $(\mathbb{Z}/p\mathbb{Z})^*$, on a $a^m \equiv 1 \mod p$. D'où $m \mid n$. Ainsi :

— Si $m = n$, alors $\overline{a}$ est d'ordre n. Donc par le théorème de Lagrange, $n \mid |(\mathbb{Z}/p\mathbb{Z})^*| = p - 1$ ie. $p \equiv 1 \mod n$.

— Sinon, $m < n$. Comme $m \mid n$,

$$X^n - 1 = \prod_{d|n} \Phi_d = \Phi_n \left(\prod_{d|m} \Phi_d \right) \left(\prod_{\substack{d||n \\ d \nmid m}} \Phi_d \right) = \Phi_n (X^m - 1) \left(\prod_{\substack{d||n \\ d \nmid m}} \Phi_d \right)$$

Mais, $\overline{a}$ est racine de $\overline{\Phi_n}$ et $X^m - \overline{1} \in \mathbb{Z}/p\mathbb{Z}[X]$. En particulier, $\overline{a}$ est (au moins) racine double de $X^n - \overline{1}$. On peut donc écrire,

$$X^n - 1 \equiv (X - a)^2 G(X) \mod p$$

Avec $X = Y + a$, cela donne :

$$(Y + a)^n - 1 \equiv Y^2 G(Y + a) \mod p$$

Le polynôme de droite est de degré ≥ 2, donc p divise les coefficients des termes de degré 0 et 1 de $(Y + a)^n - 1$, ie.

$$p \mid a^n - 1 \text{ et } p \mid \binom{n}{1} a^{n-1} = n a^{n-1}$$

De la première égalité, on en tire $p \nmid a$. Ainsi, a est premier avec p (c'est donc également vrai pour a^{n-1}). Finalement, on tire de la deuxième égalité que $p \mid n$.

□

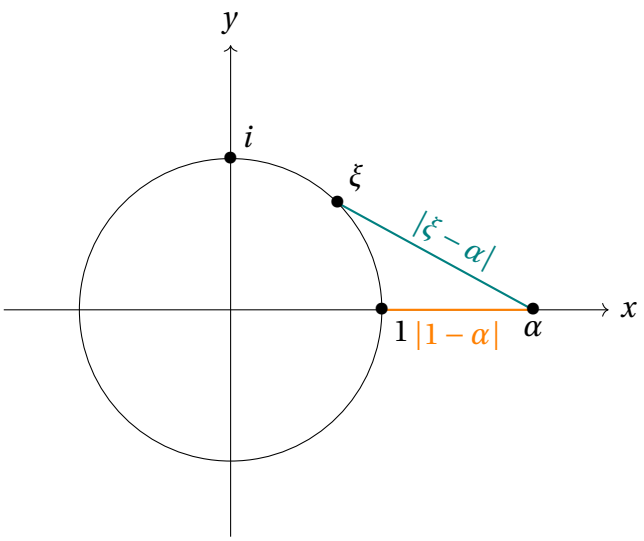
Théorème 2 (Dirichlet faible)**.** Pour tout entier n, il existe une infinité de nombres premiers congrus à 1 modulo n.

Démonstration. On suppose par l'absurde qu'il n'existe qu'un nombre fini de premiers de la forme $1+kn$, que l'on note $p_1, \dots, p_m$. On considère $N = \Phi_n(\alpha)$ où $\alpha = np_1 \dots p_m$. On remarque en particulier que $N \equiv a_0 \mod \alpha$, où a_0 est le coefficient constant de Φ_n (cela se voit en écrivant $\Phi_n = \sum_{k=0}^{\varphi(n)} a_k X^k$, ce qui donne $N = a_0 + \alpha \sum_{k=1}^{\varphi(n)} a_k \alpha^{k-1}$ une fois évalué en α).

Or, $X^n - 1 = \prod_{d|n} \Phi_d$. En évaluant en 0, on en tire :

$$-1 = \prod_{d|n} \Phi_d(0) \implies \pm 1 = a_0, \text{ car } \forall d \mid n, \Phi_d \in \mathbb{Z}[X]$$

Ainsi, $N \equiv \pm 1 \mod \alpha$. Or $|N| = |\Phi_n(\alpha)| = \prod_{\xi \in \pi_n^*} |\alpha - \xi| > 1$. On peut en effet interpréter $|\alpha - \xi|$ comme la distance du complexe α au complexe ξ ; le premier est sur l'axe réel et est supérieur ou égal à 2, le second est sur le cercle unité :



En particulier, il existe p premier tel que $p \mid N$. Par le Théorème 1 :

— Ou bien $p \mid n$, dans ce cas $p \mid \alpha = np_1 \dots p_m$.

— Ou bien $p \equiv 1 \mod n$, dans ce cas $p = p_k$ pour un certain $k \in [\![1, m]\!]$. Et on a encore $p \mid \alpha$.

Pour conclure, on écrit $N = \alpha q \pm 1$ (par division euclidienne), et on a $p \mid N - \alpha q = \pm 1$: absurde. □

Si vous choisissez de présenter ce développement, il faut au moins connaître l'énoncé de la version forte du théorème.

Théorème 3 (Progression arithmétique de Dirichlet)**.** Pour tout entier n et pour tout m premier avec n, il existe une infinité de nombres premiers congrus à m modulo n.

30 Théorème de Fejér

Dans ce développement, on montre le théorème de Fejér, qui assure la convergence de la série de Fourier d'une fonction au sens de Cesàro.

Lemme 1. Soit $f : \mathbb{R} \to \mathbb{C}$ une fonction continue et T-périodique. Alors f est uniformément continue sur $\mathbb{R}$.

Démonstration. Le théorème de Heine implique la continuité uniforme de f sur $[-T, 2T]$, ce qui s'écrit :

$$\forall \epsilon > 0, \exists \eta > 0 \text{ tel que } \forall x, y \in [-T, 2T], |x - y| < \eta \implies |f(x) - f(y)| < \epsilon \qquad (*)$$

Soit $\epsilon > 0$ et soit le $\eta > 0$ correspondant donné par $(*)$, que l'on peut supposer strictement inférieur à T. Soient $x, y \in \mathbb{R}$ tels que $|x - y| < \eta$. Il existe $k \in \mathbb{Z}$ tel que $x' = x + kT \in [0, T]$. Alors,

$$y' = y + kT \in [x' - \eta, x' + \eta] \subseteq [-T, 2T]$$

Comme $|x' - y'| < \eta$, on en déduit

$$|f(x) - f(y)| = |f(x') - f(y')| < \epsilon$$

ce qu'il fallait démontrer. □

Notation 2. On note $\forall n \in \mathbb{Z}$, $e_n : x \mapsto e^{inx}$ et, pour toute fonction f continue et 2π-périodique, $c_n(f)$ son n-ième coefficient de Fourier.

[GOU21] p. 306

Théorème 3 (Fejér)**.** Soit $f : \mathbb{R} \to \mathbb{C}$ une fonction continue et 2π-périodique. On note pour tout $n \in \mathbb{N}$, S_n le n-ième terme de sa série de Fourier et

$$C_n = \frac{1}{n+1} \sum_{k=0}^{n} S_k$$

la suite des moyennes de Cesàro correspondante. Alors (C_n) converge uniformément vers f sur $\mathbb{R}$.

Démonstration. On commence par noter, pour tout $n \in \mathbb{N}$, $D_n = \sum_{k=-n}^{n} e_k$ et $F_n = \frac{1}{n+1} \sum_{k=0}^{n} D_k$ les noyaux de Dirichlet et de Fejér. Comme, pour tout $k \in \mathbb{Z}^*$, $\int_{-\pi}^{\pi} e_n(t)\,\mathrm{d}t = 0$, on a pour tout $n \in \mathbb{N}$,

$$\frac{1}{2\pi} \int_{-\pi}^{\pi} D_n(t)\,\mathrm{d}t = \frac{1}{2\pi} \int_{-\pi}^{\pi} e_0(t)\,\mathrm{d}t = 1$$

et donc,

$$\frac{1}{2\pi} \int_{-\pi}^{\pi} F_n(t)\,\mathrm{d}t = \frac{1}{n+1} \left(\sum_{k=0}^{n} \frac{1}{2\pi} \int_{-\pi}^{\pi} D_n(t)\,\mathrm{d}t \right) = 1 \qquad (*)$$

Calculons le noyau de Dirichlet. Soit $x \in \mathbb{R} \setminus 2\pi\mathbb{Z}$. On a pour tout $N \in \mathbb{N}$,

$$\begin{aligned} D_N(x) &= e^{-iNx} \sum_{n=0}^{2N} e^{inx} \\ &= e^{-iNx} \frac{e^{(2N+1)ix} - 1}{e^{ix} - 1} \\ &= e^{-iNx} \frac{e^{(2N+1)i\frac{x}{2}} \left(e^{(2N+1)i\frac{x}{2}} - e^{-(2N+1)i\frac{x}{2}} \right)}{e^{i\frac{x}{2}} \left(e^{i\frac{x}{2}} - e^{-i\frac{x}{2}} \right)} \\ &= \frac{2i \sin\left(\left(N + \frac{1}{2} \right) x \right)}{2i \sin\left(\frac{x}{2} \right)} \\ &= \frac{\sin\left(\left(N + \frac{1}{2} \right) x \right)}{\sin\left(\frac{x}{2} \right)} \end{aligned}$$

D'où, pour tout $N \in \mathbb{N}^*$:

$$\begin{aligned} NF_{N-1} &= \sum_{n=0}^{N-1} D_n \\ &= \sum_{n=0}^{N} \frac{\sin\left(\left(n + \frac{1}{2} \right) x \right)}{\sin\left(\frac{x}{2} \right)} \\ &= \frac{1}{\sin\left(\frac{x}{2} \right)} \operatorname{Im} \left(\sum_{n=0}^{N-1} e^{i(n+\frac{1}{2})x} \right) \\ &= \frac{1}{\sin\left(\frac{x}{2} \right)} \operatorname{Im} \left(e^{\frac{ix}{2}} \frac{e^{iNx} - 1}{e^{ix} - 1} \right) \\ &= \frac{1}{\sin\left(\frac{x}{2} \right)} \operatorname{Im} \left(e^{\frac{ix}{2}} \frac{e^{\frac{iNx}{2}} 2i \sin\left(\frac{Nx}{2} \right)}{e^{\frac{ix}{2}} 2i \sin\left(\frac{x}{2} \right)} \right) \\ &= \frac{\sin\left(\frac{Nx}{2} \right)}{\sin\left(\frac{x}{2} \right)^2} \operatorname{Im} \left(e^{\frac{iNx}{2}} \right) \\ &= \frac{\sin\left(\frac{Nx}{2} \right)^2}{\sin\left(\frac{x}{2} \right)^2} \end{aligned} \qquad (**)$$

Maintenant, on remarque que pour tout $n \in \mathbb{N}$ et pour tout $x \in \mathbb{R}$,

$$S_n(x) = \frac{1}{2\pi} \sum_{k=0}^{n} \left(\int_{-\pi}^{\pi} f(t) e^{-ikt} \, \mathrm{d}t \right) e^{ikx} = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(t) D_n(x-t) \, \mathrm{d}t = f * D_n$$

donc $C_n = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(t) F_n(x-t) \, \mathrm{d}t = f * F_n = F_n * f$ par commutativité du produit de convolution. Soit $\epsilon > 0$. Le Théorème 1 assure l'existence de $\eta \in]0, \pi[$ tel que

$$\forall x, y \in \mathbb{R}, \, |x - y| < \eta \implies |f(x) - f(y)| < \epsilon$$

De plus, $|f|$ est continue sur tous les compacts de la forme $[2k\pi, 2(k+1)\pi]$, on peut donc la

majorer par un réel $M > 0$. Alors, pour tout $x \in \mathbb{R}$,

$$\begin{aligned}
|f(x) - C_n(x)| &= \left| \frac{1}{2\pi} \int_{-\pi}^{\pi} f(x-t) F_n(t)\,\mathrm{d}t - f(x) \times \underbrace{\frac{1}{2\pi} \int_{-\pi}^{\pi} F_n(t)\,\mathrm{d}t}_{=1 \text{ par } (*)} \right| \\
&= \left| \frac{1}{2\pi} \int_{-\pi}^{\pi} (f(x-t) - f(x)) F_n(t)\,\mathrm{d}t \right| \\
&\leq \frac{1}{2\pi} \int_{\eta \leq |t| \leq \pi} 2M F_n(t)\,\mathrm{d}t + \frac{1}{2\pi} \int_{-\eta}^{\eta} \epsilon F_n(t)\,\mathrm{d}t \\
&\leq \frac{2M}{2\pi} \int_{\eta \leq |t| \leq \pi} F_n(t)\,\mathrm{d}t + \epsilon
\end{aligned}$$

Or, $(**)$ montre que

$$\forall n \in \mathbb{N},\ \forall x \in [-\pi, \pi] \text{ tel que } |x| > \eta, \text{ on a } |F_n(x)| \leq \frac{1}{(n+1)\sin\left(\frac{\eta}{2}\right)^2}$$

donc (F_n) converge uniformément vers 0 sur $[-\pi, \pi] \setminus [-\eta, \eta]$. Il existe ainsi $N \in \mathbb{N}$ tel que

$$\forall n \geq N,\ \int_{\eta \leq |t| \leq \pi} F_n(t)\,\mathrm{d}t < \epsilon$$

de sorte que

$$\forall n \geq N,\ \forall x \in \mathbb{R},\ |f(x) - C_n(x)| \leq \left(\frac{M}{\pi} + 1\right)\epsilon$$

D'où le résultat. □

Je préfère la preuve de **[GOU21]**, qui est plus "clés en main". Il est possible de passer les calculs des noyaux de Dirichlet et de Fejér dans un premier temps, puis de les montrer à la fin selon le temps restant.

31 Théorème de Frobenius-Zolotarev

Nous démontrons le théorème de Frobenius-Zolotarev qui permet de calculer la signature d'un endomorphisme d'un espace vectoriel sur un corps fini possédant au moins 3 *éléments.*

Soient $p \geq 3$ un nombre premier et V un espace vectoriel sur $\mathbb{F}_p$ de dimension finie.

Définition 1. Soit H un hyperplan de V et soit G une droite supplémentaire de H dans V.La dilatation u de base H, de direction G, et de rapport $\lambda \in \mathbb{K}^*$ est l'unique endomorphisme de V défini par

$$\forall g \in G,\ \forall h \in H,\ u(g+h) = h + \lambda g$$

[I-P] p. 203

Remarque 2. On suppose connu le fait que les transvections et les dilatations engendrent $\mathrm{GL}(V)$.

[PER] p. 99

Lemme 3. Soient $u \in \mathrm{GL}(V)$ et H un hyperplan de V tel que $u_{|H} = \mathrm{id}_H$. Si $\det(u) \neq 1$, alors u est une dilatation.

p. 96

Démonstration. On note $n = \dim(V)$. Comme $u_{|H} = \mathrm{id}_H$ et $\dim(H) = n-1$, on en déduit que 1 est valeur propre de multiplicité $n-1$ de u et que H est le sous-espace propre associé :

$$H = E_1(u) = \mathrm{Ker}(u - \mathrm{id}_V)$$

On pose $\lambda = \det(u) \notin \{0,1\}$. λ est valeur propre de u (on peut le voir par exemple en calculant le polynôme caractéristique de u) de multiplicité 1. Donc u est diagonalisable, et dans une base $\mathscr{B}$ adaptée à la diagonalisation, on a :

$$\mathrm{Mat}(u,\mathscr{B}) = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & 1 & 0 \\ 0 & \dots & 0 & \lambda \end{pmatrix}$$

d'où le résultat. □

Lemme 4. Les dilatations engendrent $\mathrm{GL}(V)$.

[I-P] p. 203

Démonstration. Pour obtenir le résultat, il suffit de montrer que toute transvection est la composée de deux dilatations (cf. Théorème 2). Soit u une transvection d'hyperplan H. Comme $\mathbb{F}_p$ contient au moins 3 éléments, il existe alors v une dilatation d'hyperplan H et de rapport $\lambda \neq 1$.

Ainsi, l'application $w = u \circ v$ est dans $\mathrm{GL}(V)$ et fixe H. Comme $\det(w) = \det(v) = \lambda \neq 1$, le Théorème 3 permet de conclure que w est une dilatation. Ainsi, $u = w \circ v^{-1}$ est le produit de deux dilatations v^{-1} est une dilatation (toujours d'après le Théorème 3). □

Notation 5. Soit $a \in \mathbb{F}_p$. On note $\left(\frac{a}{p}\right)$ le symbole de Legendre de a modulo p.

Théorème 6 (Frobenius-Zolotarev)**.**

$$\forall u \in \mathrm{GL}(V), \epsilon(u) = \left(\frac{\det(u)}{p}\right)$$

où u est vu comme une permutation des éléments de V.

Démonstration. Le groupe multiplicatif d'un corps fini est cyclique, donc il existe $a \in \mathbb{F}_p^*$ tel que

$$\mathbb{F}_p^* = \langle a \rangle$$

En conséquence, si u est la dilatation de V de base H, de direction G, et de rapport $\lambda \in \mathbb{F}_p^*$, alors il existe $k \in \mathbb{N}^*$ tel que $\lambda = a^k$. On en déduit que si v est la dilatation de V de base H, de direction G, et de rapport a, alors $\forall x \in V$ écrit $x = g + h$ avec $g \in G$ et $h \in H$:

$$v^k(x) = v^k(g+h) = h + a^k g = h + \lambda g = u(g+h) = u(x)$$

d'où $v^k = u$. Ainsi, toute dilatation est une puissance d'une dilatation de rapport a.

Comme det, $\left(\frac{\cdot}{p}\right)$ et ϵ sont tous trois des morphismes de groupes, et comme les dilatations engendrent $\mathrm{GL}(V)$ (cf. Théorème 4), il suffit de montrer le résultat pour les dilatations de rapport a.

Soit u une dilatation de base H, de direction G, et de rapport a. Supposons par l'absurde que $\left(\frac{\det(u)}{p}\right) = 1$. Comme $\det(u) = a$, on a $\left(\frac{a}{p}\right) = 1$. Mais, $\mathbb{F}_p^* = \langle a \rangle$, donc $\forall x \in \mathbb{F}_p^*$, $\left(\frac{x}{p}\right) = 1$ ie. tout élément de $\mathbb{F}_p^*$ est un carré. Or, il y a $\frac{p-1}{2}$ carrés dans $\mathbb{F}_p^*$ (et $|\mathbb{F}_p^*| = p-1$, bien-sûr) : contradiction.

Il ne reste qu'à montrer que $\epsilon(u) = -1$. Pour cela, on va étudier les orbites des éléments V sous l'action de u.

Soit $h \in H$. On a $u(h) = h$, donc son orbite est réduite à $\{h\}$ qui est de cardinal 1. Elle compte donc comme un + dans le signe de $\epsilon(u)$.

Soit maintenant $x \in V$ écrit $x = g + h$ avec $g \in G \setminus \{0\}$ et $h \in H$ de sorte que $u^k(x) = h + a^k g$ pour tout $k \in \mathbb{N}$.

— $\mathbb{F}_p^*$ est cyclique d'ordre $p-1$, donc $a^{p-1} = 1$. Ainsi, $u^{p-1}(x) = x$.

— Supposons par l'absurde que $\exists 1 \leq i < j \leq p-1$ tel que $u^i(x) = u^j(x)$. On a,

$$\begin{aligned} h + a^j g = h + a^i g &\iff a^{j-i}(a^i - 1)\underbrace{g}_{\neq 0} = 0 \\ &\implies a^{j-i} = 0 \text{ ou } a^i = 1 \end{aligned}$$

ce qui est absurde dans les deux cas.

L'orbite de x sous l'action de u est donc $\{x, \dots, u^{p-2}(x)\}$ qui est de cardinal $p-1$ (pair) et compte donc comme un − dans le signe de $\epsilon(u)$.

Il ne reste qu'à compter le nombre d'orbites de cardinal $p-1$. Les éléments contenus dans ces orbites forment exactement l'ensemble

$$\bigcup_{h\in H}\{g+h \mid g\in G, g\neq 0\}$$

et il y en a donc

$$|H|\times(|G|-1)=p^{n-1}(p-1)$$

(car H est un hyperplan et G est une droite). Comme ces orbites sont de cardinal $p-1$, il y a donc exactement p^{n-1} orbites. Or, p^{n-1} est impair, donc $\epsilon(u)$ est de signe négatif. Ainsi, $\epsilon(u)=-1$. □

32 Théorème de Kronecker

En utilisant les polynômes symétriques, nous montrons ici que toutes les racines d'un polynôme unitaire à coefficients entiers dont les racines sont dans $D(0,1) \setminus \{0\}$, sont en fait des racines de l'unité.

Lemme 1 (Relations de Viète)**.** Soient A un anneau commutatif unitaire intègre et $P = \sum_{i=1}^{n} a_i X^i \in A[X]$ que l'on suppose scindé dans $A[X]$ et tel que $a_n \in A^*$. Si on note $\Sigma_k(X_1, \dots, X_n)$ le k-ième polynôme symétrique élémentaire en n variables et α_1, ..., α_n les racines de P (comptées avec multiplicité), alors $\Sigma_k(\alpha_1, \dots, \alpha_n) = (-1)^k a_{n-k} a_n^{-1}$.

Démonstration. On a $P = a_n \prod_{i=1}^{n}(X - \alpha_i)$. En développant partiellement P, on a de même :

$$P = a_n X^n - a_n(\alpha_1 + \cdots + \alpha_n)X^{n-1} + \cdots + (-1)^n a_n \alpha_1 \dots \alpha_n$$

Par identification avec la forme développée, les coefficients de X^{n-1} doivent être égaux. En particulier :

$$a_{n-1} = -a_n(\alpha_1 + \cdots + \alpha_n) \iff \underbrace{\alpha_1 + \cdots + \alpha_n}_{=\Sigma_1(\alpha_1, \dots \alpha_n)} = -a_{n-1} a_n^{-1}$$

Et on procède de même pour trouver les autres coefficients. Par exemple, $a_0 = (-1)^n a_n \alpha_1 \dots \alpha_n \iff \Sigma_n(\alpha_1, \dots \alpha_n) = (-1)^n a_0 a_n^{-1}$. □

Remarque 2. Tout au long de ce développement, nous utiliserons implicitement le fait que tout polynôme à coefficients dans $\mathbb{C}$ (donc à fortiori aussi dans $\mathbb{Z}$) admet n racines complexes comptées avec multiplicité. Il s'agit du théorème de d'Alembert-Gauss.

Théorème 3 (Kronecker)**.** Soit $P \in \mathbb{Z}[X]$ unitaire tel que toutes ses racines complexes appartiennent au disque unité épointé en l'origine (que l'on note D). Alors toutes ses racines sont des racines de l'unité.

[I-P] p. 279

Démonstration. Notons par Ω_n l'ensemble des polynômes unitaires à coefficients dans $\mathbb{Z}$ tels que toutes leurs racines complexes appartiennent à D. Soit $P \in \Omega_n$ dont on note $a_0, \dots, a_n$ les coefficients et $z_1, \dots, z_n$ les racines complexes. On note $\forall k \in [\![0, n]\!]$, $\sigma_k = \Sigma_k(z_1, \dots, z_n)$. D'après le Théorème 1, on a :

$$\forall k \in [\![0, n]\!],\ \sigma_k = (-1)^k a_{n-k} \qquad (*)$$

D'où $\forall k \in [\![0,n]\!]$:

$$\begin{aligned}|\sigma_k| &= \left|\sum_{I\in\mathscr{P}_k([\![1,n]\!])}\prod_{i\in I} z_i\right| \\ &\leq \sum_{I\in\mathscr{P}_k([\![1,n]\!])}\prod_{i\in I}|z_i| \\ &\leq |\mathscr{P}_k([\![1,n]\!])|\times 1 \\ &= \binom{n}{k}\end{aligned}$$

Et par $(*)$,

$$\forall k \in [\![0,n]\!],\ |a_k| \leq \binom{n}{n-k} = \binom{n}{k}$$

Ω_n est donc un ensemble fini (car on n'a qu'un nombre limité de choix possibles pour les coefficients a_k).

On pose maintenant

$$\forall k \in \mathbb{N},\ P_k = \prod_{j=0}^{n}(X - z_j^k)$$

qui sont des polynômes unitaires de degré n dont les racines $z_1^k, \dots, z_n^k$ appartiennent toutes à D. Soient $k \in \mathbb{N}$ et $r \in [\![0,n]\!]$. D'après le Théorème 1, le coefficient de X^{n-r} de P_k est $(-1)^r\Sigma_r(z_1^k,\dots,z_n^k)$. Mais, $\Sigma_r(X_1^k,\dots,X_n^k) \in \mathbb{Z}[X]$, donc on peut y appliquer le théorème fondamental des polynômes symétriques :

$$\exists Q_{r,k} \in \mathbb{Z}[X] \text{ tel que } \Sigma_r(X_1^k,\dots,X_n^k) = Q_{r,k}(\Sigma_1(X_1,\dots,X_n),\dots,\Sigma_n(X_1,\dots,X_n))$$

Or, comme $P \in \mathbb{Z}[X]$, on a $\forall j \in [\![0,n]\!]$, $\Sigma_j(z_1,\dots,z_n) \in \mathbb{Z}$ d'après le Théorème 1. En particulier, on a $\Sigma_r(X_1^k,\dots,X_n^k) \in \mathbb{Z}[X]$ car $Q_{r,k} \in \mathbb{Z}[X]$. On en déduit que $\forall k \in \mathbb{N}$, $P_k \in \Omega_n$.

Comme Ω_n est fini, l'ensemble des racines de tous les P_k ; qui est $\{z \in \mathbb{C} \mid \exists k \in \mathbb{N}, P_k(z) = 0\}$ est fini. Soit $j \in [\![1,n]\!]$. L'ensemble $\{z_j^k \mid k \in \mathbb{N}\}$ est inclus dans l'ensemble de ces racines, qui est fini ; il est donc lui-même fini :

$$\exists k \neq k' \text{ tel que } z_j^k = z_j^{k'}$$

Quitte à échanger les deux, on peut supposer $k \geq k'$. Comme $z_j \neq 0$, on a $z_j^{k-k'} = 1$. Donc z_j est une racine de l'unité ; ce que l'on voulait. □

Corollaire 4. Soit $P \in \mathbb{Z}[X]$ unitaire et irréductible sur $\mathbb{Q}$ tel que toutes ses racines complexes soient de module inférieur ou égal à 1. Alors $P = X$ ou P est un polynôme cyclotomique.

Démonstration. Si 0 est racine de P, alors $X \mid P$, donc $P = X$ par irréductibilité et unitarité. Sinon, 0 n'est pas racine de P. On peut donc appliquer le Théorème 3 à P ; et donc les racines de P sont des racines de l'unité. Ainsi, en notant N le maximum des ordres des racines de P, on a :

$$P \mid (X^N - 1)^n \text{ où } n = \deg(P)$$

Or, la décomposition en irréductibles de $X^N - 1$ est

$$X^N - 1 = \prod_{d|N} \Phi_d$$

Puisque $\mathbb{Q}[X]$ est un anneau factoriel, P est premier. Donc d'après le lemme de Gauss, comme $P \mid X^N - 1$:

$$\exists d \mid N \text{ tel que } P = \Phi_d$$

□

33 Premier théorème de Sylow

En procédant par récurrence sur le cardinal du groupe, on montre l'existence d'un sous-groupe de Sylow.

Théorème 1 (Cauchy "faible")**.** Soit G un groupe abélien fini et soit p un diviseur premier de l'ordre de G. Alors, il existe un sous-groupe de G d'ordre p.

[GOU21] p. 44

Démonstration. G est fini, on peut donc l'écrire

$$G = \langle x_1, \dots, x_n \rangle$$

où $(x_1, \dots, x_n)$ est un système de générateurs de G. On définit

$$\varphi : \begin{array}{ccc} \langle x_1 \rangle \times \cdots \times \langle x_n \rangle & \to & G \\ (y_1, \dots, y_n) & \mapsto & y_1 \dots y_n \end{array}$$

Comme G est abélien, φ est clairement un morphisme de groupes. Et comme $(x_1, \dots, x_n)$ est un système de générateurs de G, φ est surjectif.On peut appliquer le premier théorème d'isomorphisme pour obtenir

$$G \cong (\langle x_1 \rangle \times \cdots \times \langle x_n \rangle)/\mathrm{Ker}(\varphi)$$

En particulier, $|G| \times |\mathrm{Ker}(\varphi)| = |\langle x_1 \rangle| \times \cdots \times |\langle x_n \rangle|$. On note, pour tout $i \in [\![1, n]\!]$, $r_i = |\langle x_i \rangle|$. On a ainsi,

$$G \mid r_1 \dots r_n \implies p \mid r_1 \dots r_n$$

par transitivité de $|$. Par le lemme d'Euclide, il existe $i \in [\![1, n]\!]$ tel que $p \mid r_i$. On écrit $r_i = pq$ avec $q \in \mathbb{N}^*$, et on pose $x = x_i^q$. Alors, x est d'ordre p et $H = \langle x \rangle$ est un sous-groupe de G d'ordre p. □

Théorème 2 (Premier théorème de Sylow)**.** Soit G un groupe fini d'ordre np^α avec $n, \alpha \in \mathbb{N}$ et p premier tel que $p \nmid n$. Alors, il existe un sous-groupe de G d'ordre p^α.

Démonstration. Posons $h = |G|$. On va procéder par récurrence forte sur h.

— Si $h = 1$: Alors, $n = 1$ et $\alpha = 0$. La propriété est donc triviale.

— On suppose la propriété vraie pour les groupes d'ordre strictement inférieur à h. Si $\alpha = 0$, c'est encore une fois trivial, pour les mêmes raisons qu'à l'initialisation de la propriété. Supposons donc $\alpha \geq 1$. On fait agir G sur lui-même par conjugaison, via l'action :

$$(g, h) \mapsto g h g^{-1}$$

Soit Ω un système de représentants associé à la relation "être dans la même orbite". La formule des classes donne

$$|G| = \sum_{\omega \in \Omega} |G \cdot \omega| = \sum_{\omega \in \Omega} (G : \mathrm{Stab}_G(\omega)) = \sum_{\omega \in \Omega} \frac{|G|}{|\mathrm{Stab}_G(\omega)|} \qquad (*)$$

Mais,

$$\mathrm{Stab}_G(\omega) = G \iff \forall g \in G,\, g\omega g^{-1} = \omega \iff \omega \in Z(G)$$

donc, en regroupant, on peut réécrire $(*)$:

$$\begin{aligned} |G| &= \sum_{\omega\in\Omega} \frac{|G|}{|\mathrm{Stab}_G(\omega)|} \\ &= \sum_{\omega\in Z(G)} \frac{|G|}{|\mathrm{Stab}_G(\omega)|} + \sum_{\omega\notin Z(G)} \frac{|G|}{|\mathrm{Stab}_G(\omega)|} \\ &= |Z(G)| + \sum_{\omega\notin Z(G)} \frac{|G|}{|\mathrm{Stab}_G(\omega)|} \qquad (**) \end{aligned}$$

On a maintenant deux cas :

— Il existe ω tel que $p^\alpha \mid |\mathrm{Stab}_G(\omega)|$: Alors, comme $\mathrm{Stab}_G(\omega)$ est un sous-groupe de G d'ordre divisant strictement celui de G, on peut y appliquer l'hypothèse de récurrence pour obtenir un sous-groupe d'ordre p^α. Ce sous-groupe est donc également un sous-groupe de G.

— Pour tout ω, $p^\alpha \nmid |\mathrm{Stab}_G(\omega)|$: Alors, en factorisant par p dans les termes de la somme de $(**)$, on constate que $p \mid \frac{|G|}{|\mathrm{Stab}_G(\omega)|}$ pour tout $\omega \notin Z(G)$. Comme $p \mid h$, toujours d'après $(**)$, on a

$$p \mid |Z(G)|$$

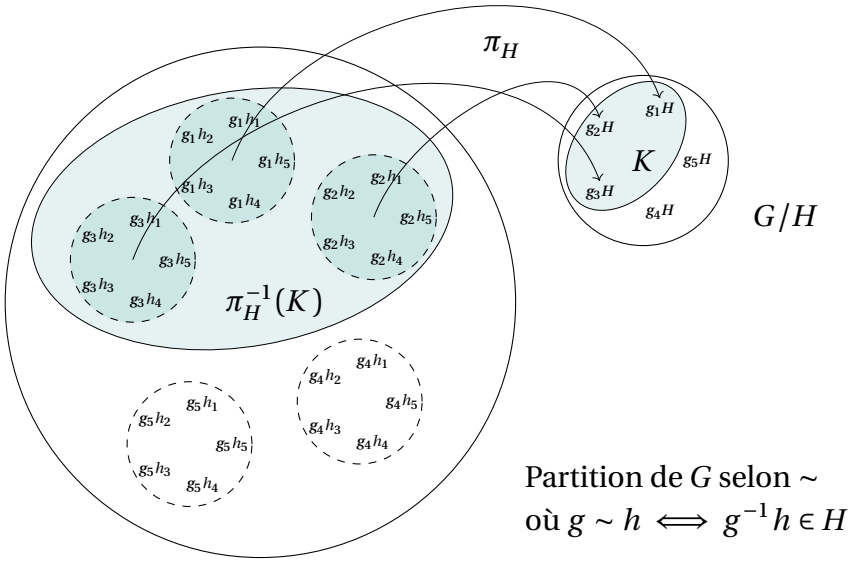
$Z(G)$ étant commutatif, on peut appliquer le Théorème 1. On obtient l'existence d'un sous-groupe H de $Z(G)$ d'ordre p, qui est de plus distingué dans G car inclus dans $Z(G)$. Alors,

$$|G/H| = \frac{|G|}{|H|} = np^{\alpha-1}$$

Il suffit maintenant d'appliquer l'hypothèse de récurrence à G/H, qui donne l'existence d'un sous-groupe K de G/H d'ordre $p^{\alpha-1}$. On considère la surjection canonique

$$\pi_H : G \to G/H$$

Alors, $\pi_H^{-1}(K) = \{g \in G \mid gH \in K\}$ est un sous-groupe de G d'ordre $|K| \times |H| = p^\alpha$:



ce qu'on voulait.

□

34 Théorème de Wantzel

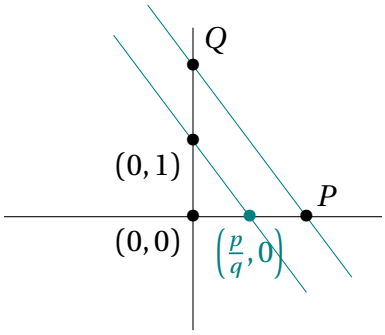
Une application sympathique de la théorie des corps en géométrie. Les arguments sont assez simples et donnent lieu à de jolies applications.

Notation 1. On note $\mathbb{E}$ l'ensemble des nombres constructibles. Tout au long du développement, on se permettra de confondre points et coordonnées.

Lemme 2. $\mathbb{E}$ contient le corps $\mathbb{Q}$.

[GOZ] p. 49

Démonstration. Tout élément $z \in \mathbb{Z}$ est constructible. Soit $(p,q) \in \mathbb{Z}^* \times \mathbb{N}^*$. Les points $P = (p,0)$ et $Q = (0,q)$ sont constructibles. On considère la droite (d), parallèle à (PQ) passant par $(0,1)$. Cette droite est constructible, et son point d'intersection avec la droite passant par les points $(0,0)$ et $(1,0)$ est $\left(\frac{p}{q},0\right)$ par le théorème de Thalès.

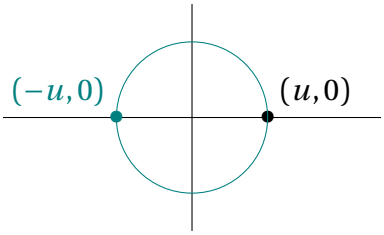


Donc $\frac{p}{q} \in \mathbb{E}$. Comme $0 \in \mathbb{E}$, on a bien $\mathbb{Q} \subseteq \mathbb{E}$. □

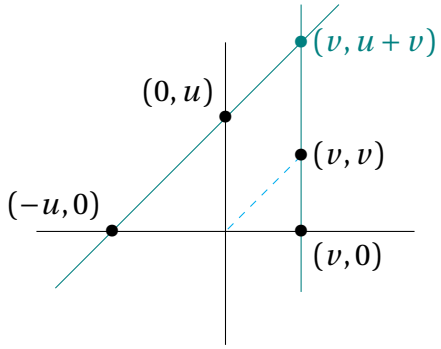
Lemme 3. $\mathbb{E}$ est un sous-corps de $\mathbb{R}$ stable par racine carrée.

Démonstration. Soient $u, v \in \mathbb{E}$. Commençons par montrer que $\mathbb{E}$ est un sous-corps de $\mathbb{R}$.

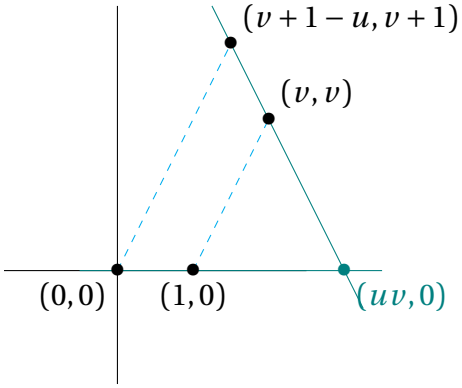
— Le point $(u,0)$ est constructible donc son symétrique $(-u,0)$ l'est aussi. Donc $-u \in \mathbb{E}$.



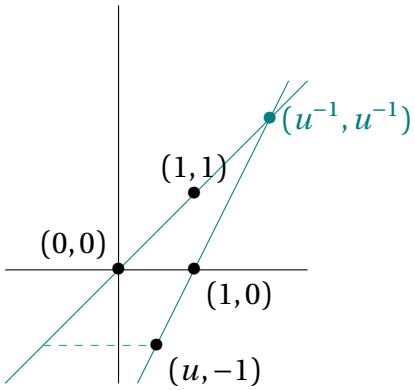
— La droite passant par les points $(0,u)$ et $(-u,0)$ et la droite passant par les points $(v,0)$ et (v,v) ont pour point d'intersection $(v,u+v)$ (par le théorème de Thalès). Donc $u+v \in \mathbb{E}$.



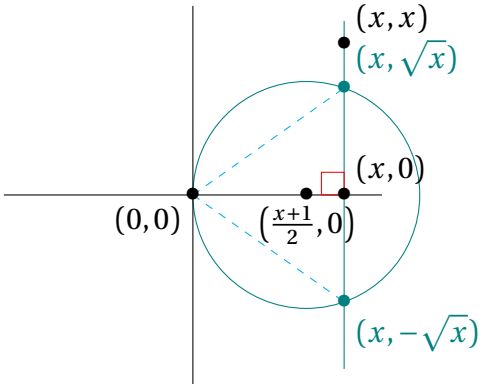
— D'après ce qui précède, $v+1$ et $v+1-u$ appartiennent à $\mathbb{E}$. La droite passant par les points $(v+1-u, v+1)$ et (u,v) et la droite passant par les points $(0,0)$ et $(1,0)$ ont pour point d'intersection $(uv,0)$ (par le théorème de Thalès). Donc $uv \in \mathbb{E}$.



— On suppose $u \neq 0$. La droite passant par les points $(1,0)$ et $(u,-1)$ et la droite passant par les points $(0,0)$ et $(1,1)$ ont pour point d'intersection (u^{-1}, u^{-1}) (par le théorème de Thalès). Donc $u^{-1} \in \mathbb{E}$.



Ainsi, $\mathbb{E}$ est un sous-corps de $\mathbb{R}$, qui contient $\mathbb{Q}$ par le Théorème 2. Maintenant, soit $x \in \mathbb{E}$ avec $x > 0$. Comme $\mathbb{E}$ est un sous-corps de $\mathbb{R}$, on a $\frac{x+1}{2} \in \mathbb{E}$. Le cercle de centre $\left(\frac{x+1}{2}, 0\right)$ passant par $(0,0)$ et la droite passant par les points $(x,0)$ et (x,x) ont pour point d'intersection $(x, \sqrt{x})$ et $(x, -\sqrt{x})$ par le théorème de Pythagore. Donc $\sqrt{x} \in \mathbb{E}$.



□

Théorème 4 (Wantzel)**.** Soit $\alpha \in \mathbb{R}$. Alors, $\alpha \in \mathbb{E}$ si et seulement s'il existe une suite finie $(L_0, \dots, L_p)$ de sous-corps de $\mathbb{R}$ vérifiant :

(i) $L_0 = \mathbb{Q}$.

(ii) $\forall i \in [\![0, p-1]\!]$, L_{i+1} est une extension quadratique (de degré 2) de L_i.

(iii) $\alpha \in L_p$.

Démonstration. On suppose α constructible. Alors, il existe un point M tel que α est l'abscisse de M. M s'obtient à l'aide d'un nombre fini de constructions de points $M_1, \dots, M_m$. Pour tout $i \in [\![1, m]\!]$, on note (x_i, y_i) les coordonnées de M_i. De ce fait, on a une tour d'extension **[ULM18]** p. 103

$$\underbrace{K_0}_{=\mathbb{Q}} \subseteq K_1 \subseteq \cdots \subseteq K_m$$

avec $\alpha \in K_m$ et pour tout $0 \in [\![1, m-1]\!]$, $K_{i+1} = K_i(x_i, y_i)$. Soit $i \in [\![1, m-1]\!]$. Montrons que $[K_{i+1} : K_i] \leq 2$. On a différents cas possibles :

— M_i est l'intersection de deux droites passant par des nombres constructibles de K_i. Alors, les coordonnées (x_i, y_i) de M_i sont solution d'un système d'équations de la forme

$$\begin{cases} ax + by = c \\ a'x + b'y = c' \end{cases}$$

avec $a, b, c, a', b', c' \in K_i$ par construction. Donc, $x_i, y_i \in K_i$ et ainsi, $[K_{i+1} : K_i] = 1$.

— M_i est l'intersection d'une droite et d'un cercle passant par des points dont les coordonnées sont des nombres constructibles de K_i et de rayon un nombre constructible de K_i. Alors, les coordonnées (x_i, y_i) de M_i sont solution d'un système d'équations de la forme

$$\begin{cases} ax + by = c \\ (x-a')^2 + (y-b')^2 = c' \end{cases}$$

avec $a, b, c, a', b', c' \in K_i$ par construction. Raisonnons selon la nullité de a.

— Si $a \neq 0$, la première équation donne

$$x = -\frac{by + c}{a}$$

et en réinjectant dans la deuxième équation, on obtient que y_i est racine d'un polynôme de degré 2. Ainsi, $[K_i(y_i) : K_i] \leq 2$. Puisque $x_i = -\frac{by_i+c}{a} \in K_i(y_i)$, on a bien $[K_{i+1} : K_i] \leq 2$.

— Si $a = 0$, alors $y_i = \frac{c}{b} \in K_i$ (on ne peut pas avoir $b = 0$ dans ce cas). Or, cette fois-ci c'est x_i qui est racine d'un polynôme de degré 2. On peut conclure de la même manière que ci-dessus.

— M_i est l'intersection de deux cercles passant par des points dont les coordonnées sont des nombres constructibles de K_i et de rayon un nombre constructible de K_i. Alors, les coordonnées (x_i, y_i) de M_i sont solution d'un système d'équations de la forme

$$\begin{cases} (x-a)^2 + (y-b)^2 = c \\ (x-a')^2 + (y-b')^2 = c' \end{cases}$$

avec $a, b, c, a', b', c' \in K_i$ par construction. On soustrait la deuxième équation à la première, pour obtenir le système équivalent :

$$\begin{cases} -2(a-a')x - 2(b-b')y = c - c' - (a^2 - a'^2) - (b^2 - b'^2) \\ (x-a')^2 + (y-b')^2 = c' \end{cases}$$

ce qui nous ramène au cas précédent.

Il suffit alors d'extraire de la suite $(K_0, \dots, K_m)$ une sous-suite $(L_0, \dots, L_p)$ strictement croissante (au sens de l'inclusion) en ne conservant dans la suite initiale que les corps extension quadratique du précédent (avec $L_0 = K_0$ et $L_p = K_n$). On obtient une suite de sous-corps de $\mathbb{R}$ (par le Théorème 3) qui remplit les trois conditions annoncées.

Réciproquement, supposons l'existence d'une suite $(L_0, \dots, L_p)$ de sous-corps de $\mathbb{R}$ répondant aux trois conditions de l'énoncé. Montrons par récurrence que

$$\forall j \in [\![0, p]\!],\ L_j \subseteq \mathbb{E}$$

— Initialisation : $L_0 = \mathbb{Q}$: cela résulte du Théorème 2.

— Hérédité : Supposons $L_j \subseteq \mathbb{E}$ pour $j \in [\![0, p-1]\!]$. Soit $x \in L_{j+1}$. Comme, par hypothèse,

$$[L_{j+1} : L_j] = 2$$

la famille $(1, x, x^2)$ est L_j-liée :

$$\exists a, b, c \in L_j \text{ non tous nuls tels que } ax^2 + bx + c = 0$$

— Si $a = 0$, alors, $x = -\frac{c}{b} \in L_j$. Donc $x \in \mathbb{E}$.

— Si $a \neq 0$, alors, $x = \frac{1}{2a}(-b \pm \sqrt{b^2 - 4ac})$. Donc, comme $\mathbb{E}$ est un sous-corps de $\mathbb{R}$ stable par racine carrée (cf. Théorème 3), $x \in \mathbb{E}$.

Ainsi, $L_{j+1} \subseteq \mathbb{E}$. En conclusion, $L_p \subseteq \mathbb{E}$, donc α est constructible.

□

La réciproque et la conclusion du sens direct du théorème sont mieux rédigées dans **[GOZ]**, à mon avis.

Corollaire 5. Si $\alpha \in \mathbb{R}$ est constructible, il existe $e \in \mathbb{N}$ tel $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^e$.

[GOZ] p. 52

Démonstration. Soit $\alpha \in \mathbb{E}$. D'après le théorème précédent, il existe une suite finie $(L_0, \dots, L_p)$ de sous-corps de $\mathbb{R}$ vérifiant :

(i) $L_0 = \mathbb{Q}$.

(ii) $\forall i \in [\![0, p-1]\!]$, L_{i+1} est une extension quadratique (de degré 2) de L_i.

(iii) $\alpha \in L_p$.

Par le théorème de la base télescopique,

$$[L_p : \mathbb{Q}] = 2^p$$

et par ce même théorème,

$$[L_p : \mathbb{Q}] = [L_p : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$$

et en particulier, $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ est un diviseur de 2^p : ce qu'on voulait. □

Application 6 (Duplication du cube)**.** Soit un cube de volume $\mathcal{V}$ dont on suppose son arête a constructible. Il est impossible de dessiner, à la règle et au compas, l'arête d'un cube de volume $2\mathcal{V}$.

Démonstration. On a $\mathcal{V} = a^3$ et donc $2\mathcal{V} = 2a^3$. L'arête d'un cube est la racine cubique de son volume. Il faut donc construire le nombre

$$\sqrt[3]{2a^3} = a\sqrt[3]{2}$$

Comme a est constructible, ceci revient à construire le nombre

$$\alpha = \sqrt[3]{2}$$

Le polynôme $P = X^3 - 2$ est irréductible sur $\mathbb{Q}$ (par le critère d'Eisenstein) et annule α : c'est son polynôme minimal sur $\mathbb{Q}$. On a ainsi

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$$

donc α n'est pas constructible par le Théorème 5. □

35 Théorème de Wedderburn

En utilisant les polynômes cyclotomiques, nous montrons que tout corps fini est commutatif.

Lemme 1. Soient $\mathbb{K}$ et $\mathbb{L}$ deux corps finis tels que $\mathbb{K}$ est commutatif et $\mathbb{K} \subseteq \mathbb{L}$. Alors $\exists d \in \mathbb{N}^*$ tel que $|\mathbb{L}| = |\mathbb{K}|^d$.

[GOU21] p. 100

Démonstration. $\mathbb{L}$ est un espace vectoriel sur $\mathbb{K}$ de dimension finie d (car $\mathbb{L}$ est fini). Donc $\mathbb{L}$ est isomorphe en tant que $\mathbb{K}$-espace vectoriel à $\mathbb{K}^d$. En particulier, $|\mathbb{L}| = |\mathbb{K}|^d$. □

Théorème 2 (Wedderburn)**.** Tout corps fini est commutatif.

Démonstration. Soit $\mathbb{K}$ un corps. L'idée va être de procéder par récurrence sur le cardinal du corps.

— Si $|\mathbb{K}| = 2$: alors $\mathbb{K} = \{0, 1\}$ est commutatif.

— On suppose le résultat vrai pour tout corps fini de cardinal strictement inférieur à $\mathbb{K}$. On veut montrer que $\mathbb{K}$ est commutatif. Supposons par l'absurde que $\mathbb{K}$ ne l'est pas. On pose

$$Z = Z(\mathbb{K}) = \{x \in \mathbb{K} \mid \forall y \in \mathbb{K},\ xy = yx\}$$

le centre de $\mathbb{K}$ dont on note q le cardinal. C'est un sous-corps de $\mathbb{K}$ qui est (par hypothèse) inclus strictement dans $\mathbb{K}$. Donc Z est commutatif, et par le Théorème 1, on peut écrire $|\mathbb{K}| = q^n$ où $n \in \mathbb{N}^*$. Si $x \in \mathbb{K}$, on pose

$$\mathbb{K}_x = Z_{\mathbb{K}}(\{x\}) = \{y \in \mathbb{K} \mid xy = yx\}$$

Montrons que

$$\exists d \mid n \text{ tel que } |\mathbb{K}_x| = q^d \qquad (*)$$

Notons déjà encore une fois que $\mathbb{K}_x$ est un sous-corps de $\mathbb{K}$.

— Si $\mathbb{K}_x = \mathbb{K}$, on a $|\mathbb{K}_x| = |\mathbb{K}| = q^n$. Il suffit donc de prendre $d = n$.

— Sinon, $\mathbb{K}_x \subsetneq \mathbb{K}$, donc $\mathbb{K}_x$ est commutatif par hypothèse. Par le Théorème 1, il existe $k \in \mathbb{N}^*$ tel que $|\mathbb{K}| = |\mathbb{K}_x|^k$.

Mais, Z est un sous-corps (commutatif) de $\mathbb{K}_x$, donc d'après le Théorème 1, il existe $d \in \mathbb{N}^*$ tel que $|\mathbb{K}_x| = |Z|^d$. Donc on a

$$q^n = |\mathbb{K}| = |\mathbb{K}_x|^k = (q^d)^k = q^{dk}$$

d'où $d \mid n$.

On considère l'action par conjugaison de $\mathbb{K}^*$ sur lui-même $(x, y) \mapsto xyx^{-1}$. Si $y \in \mathbb{K}^*$, alors

$$\mathrm{Stab}_{\mathbb{K}^*}(y) = \{x \in \mathbb{K}^* \mid x.y = y\} = \mathbb{K}_y^*$$

Soit Ω un système de représentants associé à la relation d'équivalence "être dans la même orbite". L'équation aux classes donne alors

$$|\mathbb{K}^*| = \sum_{\omega\in\Omega} \frac{|\mathbb{K}^*|}{|\operatorname{Stab}_{\mathbb{K}^*}(\omega)|}$$

Or,

$$\operatorname{Stab}_{\mathbb{K}^*}(\omega) = \mathbb{K}^* \iff \forall x \in \mathbb{K}^*, \omega x = x\omega \iff \omega \in Z^*$$

donc en notant $\Omega' = \Omega \setminus Z^*$, on a :

$$|\mathbb{K}^*| = \sum_{\omega\in Z^*} \frac{|\mathbb{K}^*|}{|\operatorname{Stab}_{\mathbb{K}^*}(\omega)|} + \sum_{\omega\in\Omega'} \frac{|\mathbb{K}^*|}{|\operatorname{Stab}_{\mathbb{K}^*}(\omega)|} = |Z^*| + \sum_{\omega\in\Omega} \frac{|\mathbb{K}^*|}{|\mathbb{K}^*_\omega|} \qquad (**)$$

Soit $\omega \in \Omega'$. Par $(*)$,

$$\exists d \mid n \text{ tel que } |\operatorname{Stab}_{\mathbb{K}^*}(\omega)| = |\mathbb{K}^*_\omega| = q^d - 1$$

De plus, $d \neq n$ (car $\omega \notin Z^*$). Si maintenant on pose

$$\forall d \mid n,\ \lambda_d = |\{\omega \in \Omega' \mid |\operatorname{Stab}_{\mathbb{K}^*}(\omega)| = q^d - 1\}|$$

on peut alors écrire en remplaçant dans $(**)$:

$$q^n - 1 = |K^*| = (q-1) + \sum_{d||n} \lambda_d \left(\frac{q^n-1}{q^d-1}\right) \qquad (***)$$

Si $d \,||\, n$, on a

$$X^n - 1 = \prod_{k|n} \Phi_k = \Phi_n \left(\prod_{k|d} \Phi_k\right) \left(\prod_{\substack{k||n \\ k\nmid d}} \Phi_k\right) = \Phi_n(X^d - 1) \left(\prod_{\substack{k||n \\ k\nmid d}} \Phi_k\right)$$

Donc, $\Phi_n \mid \frac{X^n-1}{X^d-1}$ dans $\mathbb{Z}[X]$. Ceci étant vrai quelque soit d divisant strictement n, on en déduit

$$\Phi_n \mid \sum_{d||n} \lambda_d \frac{X^n-1}{X^d-1} \text{ dans } \mathbb{Z}[X]$$

Comme de plus, $\Phi_n \mid X^n - 1$ dans $\mathbb{Z}[X]$, on conclut que

$$\Phi_n \mid X^n - 1 - \sum_{d||n} \lambda_d \frac{X^n-1}{X^d-1} \text{ dans } \mathbb{Z}[X]$$

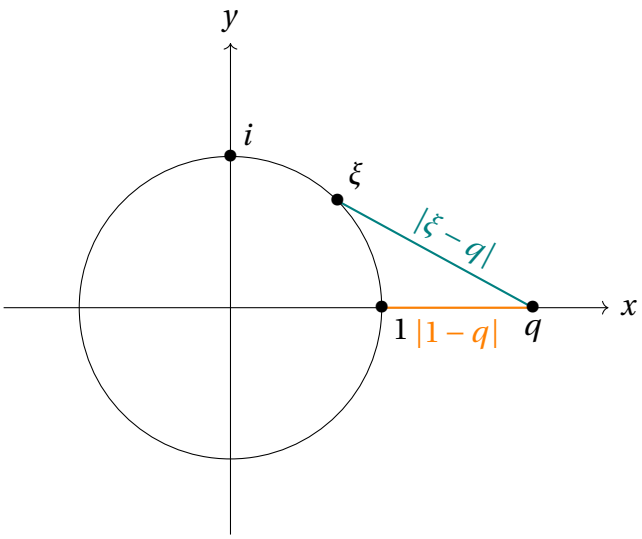
ce qui donne, une fois évalué en q :

$$\Phi_n(q) \mid q^n - 1 - \sum_{d||n} \lambda_d \frac{q^n-1}{q^d-1} \overset{(***)}{=} q - 1 \implies |\Phi_n(q)| \leq q - 1$$

Mais $n \geq 2$, donc

$$\begin{aligned} |\Phi_n(q)| &= \prod_{\xi \in \mu_n^*} |q - \xi| \\ &> \prod_{i=1}^{\varphi(n)} |q - 1| \\ &\geq |q - 1| \end{aligned}$$

On peut en effet interpréter $|q - \xi|$ comme la distance du complexe q au complexe ξ ; le premier est sur l'axe réel et est supérieur ou égal à 2, le second est sur le cercle unité mais n'est pas sur l'axe réel :



cela nous permet de justifier l'inégalité stricte. On a donc une contradiction.

□

36 Théorème de Weierstrass (par la convolution)

On montre le théorème de Weierstrass par la convolution (sans forcément développer toute la théorie derrière, ce qui peut être utile dans certaines leçons).

[GOU20] p. 304

Notation 1. $\forall n \in \mathbb{N}$, on note :

$$a_n = \int_{-1}^{1} (1-t^2)^n \,\mathrm{d}t \text{ et } p_n : t \mapsto \frac{(1-t^2)^n}{a_n} \mathbb{1}_{[-1,1]}(t)$$

Lemme 2. La suite (p_n) vérifie :

(i) $\forall n \in \mathbb{N}$, $p_n \geq 0$.

(ii) $\forall n \in \mathbb{N}$, $\int_{\mathbb{R}} p_n(t) = 1$.

(iii) $\forall \alpha > 0$, $\lim_{n\to+\infty} \int_{|t|>\alpha} p_n(t)\,\mathrm{d}t = 0$.

Autrement dit, (p_n) est une **approximation positive de l'identité**.

Démonstration. Notons tout d'abord que

$$\forall n \in \mathbb{N}^*,\ a_n = 2\int_0^1 (1-t^2)^n \,\mathrm{d}t \geq 2\int_0^1 t(1-t^2)^n \,\mathrm{d}t = \left[-\frac{(1-t^2)^{n+1}}{n+1}\right]_0^1 = \frac{1}{n+1}$$

(i) $\forall n \in \mathbb{N}$, $p_n \geq 0$ car $a_n \geq 0$ et $(1-t^2)^n \geq 0$ pour tout $t \in [-1,1]$.

(ii) $\forall n \in \mathbb{N}$, $\int_{\mathbb{R}} p_n(t)\,\mathrm{d}t = \frac{1}{a_n}\int_{-1}^{1}(1-t^2)^n \,\mathrm{d}t = 1$.

(iii) Soit $\alpha > 0$.

— Si $\alpha < 1$: $\forall n \in \mathbb{N}^*$,

$$\int_{|t|\geq\alpha} p_n(t)\,\mathrm{d}t = \frac{2}{a_n}\int_\alpha^1 (1-t^2)^n \,\mathrm{d}t \leq \frac{2}{a_n}(1-\alpha^2)^n \leq 2(n+1)(1-\alpha^2)^n$$

et comme $|1-\alpha^2| < 1$, on a $\int_{|t|\geq\alpha} p_n(t)\,\mathrm{d}t \longrightarrow 0$.

— Si $\alpha \geq 1$:

$$\int_{|t|\geq\alpha} p_n(t)\,\mathrm{d}t = 0$$

□

Théorème 3 (Weierstrass)**.** Toute fonction continue $f : [a,b] \to \mathbb{R}$ (avec $a, b \in \mathbb{R}$ tels que $a \leq b$) est limite uniforme de fonctions polynômiales sur $[a,b]$.

Démonstration. Soit $f \in \mathscr{C}_C(\mathbb{R})$ continue. Montrons que $(f * p_n)$ converge uniformément vers f. Soit $\epsilon > 0$. Par le théorème de Heine f est uniformément continue sur son support, donc l'est aussi sur $\mathbb{R}$ entier :

$$\exists \eta > 0 \text{ tel que } \forall x, y \in \mathbb{R},\ |x-y| < \eta \implies |f(x)-f(y)| < \epsilon$$

De plus, f est bornée et atteint ses bornes (donc écrire $\|f\|_\infty$ a du sens). On peut appliquer le Théorème 2 Point (iii) :

$$\exists N \in \mathbb{N} \text{ tel que } \forall n \geq N, \int_{|t|\geq\eta} p_n(t)\,\mathrm{d}t < \epsilon$$

Donc, toujours avec le Théorème 2, pour tout $n \geq N$ et pour tout $x \in \mathbb{R}$,

$$\begin{aligned}
|f * p_n(x) - f(x)| &\overset{(ii)}{=} \left| \int_{\mathbb{R}} f(x-t)p_n(t)\,\mathrm{d}t - f(x)\int_{\mathbb{R}} p_n(t)\,\mathrm{d}t \right| \\
&= \left| \int_{\mathbb{R}} (f(x-t)-f(x))p_n(t)\,\mathrm{d}t \right| \\
&\leq \int_{\mathbb{R}} |(f(x-t)-f(x))p_n(t)|\,\mathrm{d}t \\
&\overset{(i)}{=} \int_{\mathbb{R}} |f(x-t)-f(x)|\,p_n(t)\,\mathrm{d}t \\
&= \int_{|t|\geq\eta} |f(x-t)-f(x)|\,p_n(t)\,\mathrm{d}t + \int_{-\eta}^{\eta} |f(x-t)-f(x)|\,p_n(t)\,\mathrm{d}t \\
&= 2\|f\|_\infty \epsilon + \epsilon \int_{-\eta}^{\eta} p_n(t)\,\mathrm{d}t \\
&\overset{(i)}{\leq} 2\|f\|_\infty \epsilon + \epsilon \int_{\mathbb{R}} p_n(t)\,\mathrm{d}t \\
&= (2\|f\|_\infty + 1)\epsilon
\end{aligned}$$

d'où la convergence uniforme. Soit maintenant $n \in \mathbb{N}$. Supposons que f est à support dans $I = \left[-\frac{1}{2}, \frac{1}{2}\right]$ et montrons que pour tout $f * p_n$ est une fonction polynômiale.

$$\forall x \in I, (f * p_n)(x) = (p_n * f)(x) = \int_{-\frac{1}{2}}^{\frac{1}{2}} p_n(x-t)f(t)\,\mathrm{d}t \qquad (*)$$

Notons que $\forall x, t \in I, |x-t| \leq 1$, donc

$$p_n(x-t) = \frac{(1-(x-t)^2)^n}{a_n} \overset{\text{développement}}{=} \sum_{k=0}^{2n} q_k(t)x^k$$

où $\forall k \in [\![0, 2n]\!]$, q_k est une fonction polynômiale. En remplaçant dans $(*)$, on obtient :

$$\forall x \in I, (f * p_n)(x) = \sum_{k=0}^{2n} \left(\int_{-\frac{1}{2}}^{\frac{1}{2}} q_k(t)f(t)\,\mathrm{d}t \right) x^k$$

qui est bien une fonction polynômiale sur I.

Soient maintenant $[a, b]$ un intervalle fermé de $\mathbb{R}$ et $f : [a, b] \to \mathbb{R}$. On considère $[c, d]$ un intervalle plus grand avec $c < a$ et $b < d$ et on prolonge f par :

— Une fonction affine sur $[c, a]$ qui vaut 0 en c et $f(a)$ en a.

— Une fonction affine sur $[b, d]$ qui vaut 0 en d et $f(b)$ en b.

Et on peut encore prolonger cette fonction sur $\mathbb{R}$ tout entier en une fonction $\widetilde{f}$ telle que $\widetilde{f} = 0$ pour tout $x \notin [c, d]$. On a donc $\widetilde{f} \in \mathscr{C}_C(\mathbb{R})$. Nous allons maintenant avoir besoin du changement de

variable suivant :

$$\varphi : \begin{array}{ccc} I & \to & [c,d] \\ x & \mapsto & (d-c)x + \frac{c+d}{2} \end{array}$$

Comme $\widetilde{f} \circ \varphi$ est continue, à support dans I, on peut maintenant affirmer que $\widetilde{f} \circ \varphi$ est limite uniforme d'une suite de polynômes (ρ_n). Donc $\widetilde{f}$ est limite uniforme de la suite $(\rho_n \circ \varphi^{-1})$ où $\forall n \in \mathbb{N}$, $\rho_n \circ \varphi^{-1}$ est bien une fonction polynômiale car φ (donc φ^{-1} aussi) est affine. A fortiori, $f = \widetilde{f}_{|[a,b]}$ est aussi limite de fonctions polynômiales sur $[a,b]$. □

La fin de la preuve me semble mieux écrite dans **[I-P]**.

37 Théorème de Weierstrass (par les probabilités)

On montre le théorème de Weierstrass en faisant un raisonnement sur des variables aléatoires suivant une loi de Bernoulli.

[G-K] p. 195

Théorème 1 (Bernstein)**.** Soit $f : [0,1] \to \mathbb{R}$ continue. On note

$$\forall n \in \mathbb{N}^*, B_n(f) : x \mapsto \sum_{k=0}^{n} \binom{n}{k} f\left(\frac{k}{n}\right) x^k (1-x)^{n-k}$$

le n-ième polynôme de Bernstein associé à f. Alors le suite de fonctions $(B_n(f))$ converge uniformément vers f.

Démonstration. Soit $x \in]0,1[$. On se place sur un espace probabilité $(\Omega, \mathscr{A}, \mathbb{P})$ et considère (X_k) une suite de variables aléatoires indépendantes de même loi $\mathscr{B}(x)$. On note $\forall n \in \mathbb{N}^*, S_n = \sum_{k=1}^{n} X_k$. Ainsi, $S_n \sim \mathscr{B}(n,x)$ et donc par la formule de transfert,

$$\mathbb{E}\left(f\left(\frac{S_n}{n}\right)\right) = \sum_{k=0}^{n} \binom{n}{k} f\left(\frac{k}{n}\right) x^k (1-x)^{n-k} = B_n(f)(x)$$

La fonction f est continue sur $[0,1]$ qui est un compact de $\mathbb{R}$, donc par le théorème de Heine ; elle y est uniformément continue. Soit donc $\epsilon > 0$,

$$\exists \eta > 0 \text{ tel que } \forall x, y \in [0,1], |x-y| < \eta \implies |f(x) - f(y)| < \epsilon$$

On a,

$$\begin{aligned}
|B_n(f)(x) - f(x)| &= \left|\mathbb{E}\left(f\left(\frac{S_n}{n}\right)\right) - f(x)\right| \\
&= \left|\mathbb{E}\left(f\left(\frac{S_n}{n}\right) - f(x)\right)\right| \\
&\leq \mathbb{E}\left|f\left(\frac{S_n}{n}\right) - f(x)\right| \\
&\leq \mathbb{E}\left(\mathbb{1}_{\left\{\left|\frac{S_n}{n} - x\right| < \eta\right\}} \left|f\left(\frac{S_n}{n}\right) - f(x)\right|\right) + \mathbb{E}\left(\mathbb{1}_{\left\{\left|\frac{S_n}{n} - x\right| \geq \eta\right\}} \left|f\left(\frac{S_n}{n}\right) - f(x)\right|\right) \\
&\leq \mathbb{E}(\epsilon) + 2\|f\|_\infty \mathbb{E}\left(\mathbb{1}_{\left\{\left|\frac{S_n}{n} - x\right| \geq \eta\right\}}\right) \\
&= \epsilon + 2\|f\|_\infty \mathbb{P}\left(\left|\frac{S_n}{n} - x\right| \geq \eta\right) \qquad (*)
\end{aligned}$$

Comme $\mathbb{E}\left(\frac{S_n}{n}\right) = x$, on peut appliquer l'inégalité de Bienaymé-Tchebychev :

$$\mathbb{P}\left(\left|\frac{S_n}{n} - x\right| \geq \eta\right) = \mathbb{P}\left(\left|\frac{S_n}{n} - \mathbb{E}\left(\frac{S_n}{n}\right)\right| \geq \eta\right) \leq \frac{1}{\eta^2} \operatorname{Var}\left(\frac{S_n}{n}\right)$$

Comme les X_k sont indépendantes et de même loi :

$$\mathrm{Var}\left(\frac{S_n}{n}\right) = \frac{1}{n^2}\mathrm{Var}(S_n) = \frac{1}{n}\mathrm{Var}(X_1) = \frac{x(1-x)}{n} \leq \frac{1}{n}$$

En réinjectant cela dans $(*)$, cela donne

$$|B_n(f)(x) - f(x)| \leq \epsilon + \frac{2\|f\|_\infty}{n\eta^2}$$

qui est une majoration indépendante de x. Comme la fonction $B_n(f) - f$ est continue sur $[0,1]$, on peut passer à la borne supérieure :

$$\|B_n(f) - f\|_\infty = \sup_{x\in[0,1]} |B_n(f)(x) - f(x)| \leq \epsilon + \frac{2\|f\|_\infty}{n\eta^2}$$

ce qui donne après un passage à la limite supérieure :

$$\begin{aligned} &\limsup_{n\to+\infty} \|B_n(f) - f\|_\infty \leq \epsilon \\ \overset{\epsilon\longrightarrow 0}{\Longrightarrow} &\limsup_{n\to+\infty} \|B_n(f) - f\|_\infty = 0 \\ \Longrightarrow &\lim_{n\to+\infty} \|B_n(f) - f\|_\infty = 0 \end{aligned}$$

□

Théorème 2 (Weierstrass)**.** Toute fonction continue $f : [a,b] \to \mathbb{R}$ (avec $a, b \in \mathbb{R}$ tels que $a \leq b$) est limite uniforme de fonctions polynômiales sur $[a,b]$.

Démonstration. On va avoir besoin du changement de variable suivant :

$$\varphi : \begin{array}{ccc} [0,1] & \to & [a,b] \\ x & \mapsto & a + (b-a)x \end{array}$$

Par le Théorème 1, la fonction $f \circ \varphi^{-1}$ est limite uniforme d'une suite de fonctions polynômiales (p_n). Donc f est limite uniforme de la suite $(p_n \circ \varphi)$ où $\forall n \in \mathbb{N}$, $p_n \circ \varphi$ est bien une fonction polynômiale car φ est affine. □

38 Théorème des deux carrés de Fermat

Nous démontrons le théorème des deux carrés de Fermat (qui donne des conditions sur la décomposition en facteurs premiers d'un entier pour que celui-ci soit somme de deux carrés) à l'aide de l'anneau des entiers de Gauss $\mathbb{Z}[i]$.

Lemme 1. Soit $p \geq 3$ un nombre premier. Alors $x \in \mathbb{F}_p^*$ est un carré si et seulement si $x^{\frac{p-1}{2}} = 1$.

[I-P] p. 137

Démonstration. On pose $X = \{x \in \mathbb{F}_p \mid x^{\frac{p-1}{2}} = 1\}$, et on note S l'ensemble des carrés de $\mathbb{F}_p^*$. Comme un polynôme de degré d sur $\mathbb{F}_p$ possède au plus d racines, on a $|X| \leq \deg\left(X^{\frac{p-1}{2}} - 1\right) = \frac{p-1}{2}$.

D'autre part, si $x \in S$, on peut écrire $x = y^2$ et on a donc $x^{\frac{p-1}{2}} = y^{p-1} = 1$ car $|\mathbb{F}_p^*| = p-1$. Donc, $S \subseteq X$.

Pour conclure, calculons le cardinal de S. Pour cela, considérons le morphisme

$$\begin{array}{ccc} \mathbb{F}_p^* & \to & S \\ x & \mapsto & x^2 \end{array}$$

dont le noyau est $\{x \in \mathbb{F}_p^* \mid x^2 = 1\} = \{\pm 1\}$ qui est de cardinal 2. En appliquant le premier théorème d'isomorphisme, et en considérant les cardinaux; on obtient $|S| = \frac{p-1}{2}$. Donc $S = X$. □

Introduisons maintenant des notations qui seront utiles pour la suite.

Notation 2. On note

$$N : \begin{array}{ccc} \mathbb{Z}[i] & \to & \mathbb{N} \\ a+ib & \mapsto & a^2+b^2 \end{array}$$

et Σ l'ensemble des entiers qui sont somme de deux carrés.

Remarque 3. $n \in \Sigma \iff \exists z \in \mathbb{Z}[i]$ tel que $N(z) = n$.

Lemme 4. Voici quelques propriétés sur N et $\mathbb{Z}[i]$ dont nous aurons besoin :

(i) N est multiplicative.

(ii) $\mathbb{Z}[i]^* = \{z \in \mathbb{Z}[i] \mid N(z) = 1\} = \{\pm 1, \pm i\}$.

(iii) $\mathbb{Z}[i]$ est euclidien de stathme N.

Démonstration. (i) On a $\forall z, z' \in \mathbb{C}$, $|zz'|^2 = |z|^2|z'|^2$ (par multiplicativité de $(.)^2$ et de $|.|$). Et N n'est que la restriction de $|.|^2$ à $\mathbb{Z}[i]$. Il est également tout-à-fait possible de montrer cette propriété par un calcul direct.

(ii) Soit $z \in \mathbb{Z}[i]^*$. On a $N(z)N(z^{-1}) = N(zz^{-1}) = N(1) = 1$. Comme N est à valeurs dans $\mathbb{N}$, on a $N(z) = N(z^{-1}) = 1$. En écrivant $z = a+ib$, on a $N(z) = a^2+b^2 = 1$, d'où $a = \pm 1$ ou $b = \pm 1$. Réciproquement, ± 1 et $\pm i$ sont bien inversibles dans $\mathbb{Z}[i]$ et de module 1.

(iii) Soient $z, t \in \mathbb{Z}[i]$. On pose $\frac{z}{t} = x + iy \in \mathbb{C}$ avec $x, y \in \mathbb{R}$. Soient $a, b \in \mathbb{Z}$ tels que :

— $|x - a| \leq \frac{1}{2}$.

— $|y - b| \leq \frac{1}{2}$.

(Ces nombres existent bien, ne pas hésiter à faire un dessin pour s'en convaincre.) On pose $q = a + ib \in \mathbb{Z}[i]$, et on a

$$\left|\frac{z}{t} - q\right| = (x-a)^2 + (y-b)^2 \leq \frac{1}{4} + \frac{1}{4} < 1$$

On pose alors $r = z - qt$, et on a bien

$$z = tq + r \text{ et } N(r) = r^2 = |t^2| \left|\frac{z}{t} - q^2\right| < |t|^2 = N(t)$$

□

Lemme 5. Soit p un nombre premier. Si p n'est pas irréductible dans $\mathbb{Z}[i]$, alors $p \in \Sigma$.

Démonstration. On suppose que p n'est pas irréductible dans $\mathbb{Z}[i]$. On peut donc écrire $p = uv$ avec $u, v \in \mathbb{Z}[i]$ non inversibles. Ainsi,

$$p^2 = N(p) = N(uv) = \underbrace{N(u)}_{\neq 1}\underbrace{N(v)}_{\neq 1} \overset{p \text{ premier}}{\Longrightarrow} N(u) = N(v) = p$$

Par la Théorème 3, $p \in \Sigma$. □

Théorème 6 (Deux carrés de Fermat)**.** Soit $n \in \mathbb{N}^*$. Alors $n \in \Sigma$ si et seulement si $v_p(n)$ est pair pour tout p premier tel que $p \equiv 3 \mod 4$ (où $v_p(n)$ désigne la valuation p-adique de n).

Démonstration. Sens direct : On écrit $n = a^2 + b^2$ avec $a, b \in \mathbb{Z}$. Soit $p \mid n$ tel que $p \equiv 3 \mod 4$. Montrons que $p \notin \Sigma$. On suppose par l'absurde que l'on peut écrire $p = c^2 + d^2$ avec $c, d \in \mathbb{Z}$. On va discerner les cas :

— Si $c \equiv \pm 1 \mod 4$, alors $c^2 \equiv 1 \mod 4$ (et de même pour d^2).

— Si $c \equiv \pm 2 \mod 4$, alors $c^2 \equiv 0 \mod 4$ (et de même pour d^2).

Donc $p = c^2 + d^2 \equiv 0, 1 \text{ ou } 2 \mod 4$: absurde. En particulier, par le Théorème 5 (en prenant la contraposée), p est irréductible dans $\mathbb{Z}[i]$. Comme $\mathbb{Z}[i]$ est euclidien (cf. Théorème 4), p est un élément premier de $\mathbb{Z}[i]$. Mais, $p \mid n = (a + ib)(a - ib)$. Donc $p \mid a + ib$ ou $p \mid a - ib$. Dans les deux cas, on a $p \mid a$ et $p \mid b$. Ainsi,

$$\left(\frac{a}{p}\right)^2 + \left(\frac{b}{p}\right)^2 = \frac{n}{p^2}$$

donc de deux choses l'une ; on a :

$$p^2 \mid n \text{ et } \frac{n}{p^2} \in \Sigma$$

Il suffit alors d'itérer le processus (en remplaçant n par $\frac{n}{p^2}$) k fois jusqu'à ce que p ne divise plus $\frac{n}{p^{2k}}$. On a alors $n = p^{2k}u$ avec $p \nmid u$. D'où $v_p(n) = 2k$.

Réciproque : Soit p premier diviseur de n tel que $p \equiv 3 \mod 4$. Alors $p^{v_p(n)} = \left(p^{\frac{v_p(n)}{2}}\right)^2$ est un carré, donc $p^{v_p(n)} \in \Sigma$.

Soit maintenant p premier tel que $p = 2$ ou $p \equiv 1 \mod 4$. Alors en conséquence du Théorème 1 (le cas $p = 2$ étant trivial), -1 est un carré de $\mathbb{F}_p$ ie. $\exists a \in \mathbb{Z}$ tel que $-1 \equiv a^2 \mod p$. Donc $p \mid a^2 + 1 = (a - i)(a + i)$. Oui mais, p ne divise ni $a - i$, ni $a + i$. Donc p n'est pas un élément premier de $\mathbb{Z}[i]$ et n'est donc pas irréductible dans $\mathbb{Z}[i]$ (toujours parce que $\mathbb{Z}[i]$ est euclidien, cf. Théorème 4). En vertu du Théorème 5, $p \in \Sigma$.

Comme N est multiplicative, par la Théorème 3, on en déduit que Σ est stable par multiplication. Donc $n \in \Sigma$ (en décomposant n en produit de facteurs premiers). □

Remarque 7. Le fait qu'un élément irréductible d'un anneau euclidien est premier est une conséquence directe du lemme d'Euclide, vrai dans les anneaux factoriels (donc à fortiori aussi dans les anneaux euclidiens).

[PER] p. 48

39 Théorème des événements rares de Poisson

On établit la convergence en loi vers une loi de Poisson d'une suite de variables aléatoires.

Lemme 1. Soient $z_1, \dots, z_n, u_1, \dots u_n \in \mathbb{C}$ de module inférieur ou égal à 1. Alors

$$|z_1 \dots z_n - u_1 \dots u_n| \leq |z_1 - u_1| + \dots |z_n - u_n|$$

[G-K] p. 372

Démonstration. $|z_1 z_2 - u_1 u_2| = |z_1(z_2 - u_2) + u_2(z_1 - u_1)| \leq |z_1 - u_1| + |z_2 - u_2|$. On procède ensuite par récurrence pour montrer le résultat. □

Théorème 2 (des événements rares de Poisson)**.** Soit $(N_n)_{n\geq 1}$ une suite d'entiers tendant vers l'infini. On suppose que pour tout n, $A_{n,N_1}, \dots, A_{n,N_n}$ sont des événements indépendants avec $\mathbb{P}(A_{n,N_k}) = p_{n,k}$. On suppose également que :

(i) $\lim_{n\to+\infty} s_n = \lambda > 0$ où $\forall n \in \mathbb{N}, s_n = \sum_{k=1}^{N_n} p_{n,k}$.

(ii) $\lim_{n\to+\infty} \sup_{k\in[\![1,N_n]\!]} p_{n,k} = 0$.

Alors, la suite de variables aléatoires (S_n) définie par

$$\forall n \in \mathbb{N}^*, S_n = \sum_{k=1}^{N_n} \mathbb{1}_{A_{n,k}}$$

converge en loi vers la loi de Poisson de paramètre λ.

p. 390

Démonstration. Pour la suite, on note $\forall n \in \mathbb{N}$, $m_n = \max_{k\in[\![1,N_n]\!]} p_{n,k}$. On calcule

$$\begin{aligned}
\phi_{S_n}(t) &= \mathbb{E}\left(e^{itS_n}\right) \\
&= \mathbb{E}\left(e^{it\sum_{k=1}^{N_n} \mathbb{1}_{A_{n,k}}}\right) \\
&= \mathbb{E}\left(\prod_{k=1}^{N_n} e^{it\mathbb{1}_{A_{n,k}}}\right) \\
&= \prod_{k=1}^{N_n} \mathbb{E}\left(e^{it\mathbb{1}_{A_{n,k}}}\right) \text{ par indépendance} \\
&= \prod_{k=1}^{N_n} \left((1-p_{n,k}) + e^{it}p_{n,k}\right) \\
&= \prod_{k=1}^{N_n} \left(p_{n,k}(e^{it}-1) + 1\right)
\end{aligned}$$

l'avant-dernière égalité étant justifiée par le fait que

$$\mathbb{P}(e^{it\mathbb{1}_{A_{n,k}}} = e^{it}) = \mathbb{P}(A_{n,k} = 1) = p_{n,k} \text{ et } \mathbb{P}(e^{it\mathbb{1}_{A_{n,k}}} = 1) = \mathbb{P}(A_{n,k} = 0) = 1 - p_{n,k}$$

Soient $P_{n,k}$ des variables aléatoires indépendantes suivant les lois de Poisson de paramètres

respectifs $p_{n,k}$. On pose

$$S'_n = \sum_{k=1}^{N_n} P_{n,k}$$

et on calcule la fonction caractéristique de cette nouvelle variable aléatoire :

$$\begin{aligned}\phi_{S'_n}(t) &= \prod_{k=1}^{N_n} \phi_{P_{n,k}}(t) \text{ par indépendance} \\ &= \prod_{k=1}^{N_n} \exp(p_{n,k}(e^{it}-1))) \\ &= \exp(s_n(e^{it}-1))\end{aligned}$$

Par différence, on obtient

$$|\phi_{S_n}(t) - \phi_{S'_n}(t)| = \left| \prod_{k=1}^{N_n} \left(p_{n,k}(e^{it}-1)+1\right) - \prod_{k=1}^{N_n} \exp(p_{n,k}(e^{it}-1))) \right|$$

ce qui, après application du Théorème 1, donne l'inégalité

$$|\phi_{S_n}(t) - \phi_{S'_n}(t)| \leq \sum_{k=1}^{N_n} g(p_{n,k}(e^{it}-1))$$

avec $g : z \mapsto |e^z - 1 - z|$. Mais, par développement en série entière :

$$\begin{aligned}g(z) &= \left| \sum_{k=2}^{+\infty} \frac{z^k}{k!} \right| \\ &= \left| \sum_{k=0}^{+\infty} \frac{z^{k+2}}{(k+2)!} \right| \\ &= \left| z^2 \sum_{k=0}^{+\infty} \frac{z^k}{k!} \frac{1}{(k+1)(k+2)} \right| \\ &\leq |z|^2 \sum_{k=0}^{+\infty} \frac{|z|^k}{k!} \left| \frac{1}{(k+1)(k+2)} \right| \\ &\leq |z|^2 \frac{e^{|z|}}{2}\end{aligned}$$

Mais, comme $|p_{n,k}(e^{it}-1)| \leq 2p_{n,k} \leq 2$, on a :

$$\begin{aligned}|\phi_{S_n}(t) - \phi_{S'_n}(t)| &\leq \sum_{k=1}^{N_n} (2p_{n,k})^2 \frac{e^2}{2} \\ &= 2e^2 \sum_{k=1}^{N_n} 2p_{n,k}^2 \\ &\leq 2e^2 \underbrace{s_n}_{\longrightarrow \lambda} \underbrace{m_n}_{\longrightarrow 0} \\ &\longrightarrow 0\end{aligned}$$

Enfin,

$$\begin{aligned}|\phi_{S_n}(t)-\exp(\lambda(e^{it}-1))| &\leq |\phi_{S_n}(t)-\phi_{S'_n}(t)|+|\phi_{S'_n}(t)-\exp(\lambda(e^{it}-1))| \\ &\leq \underbrace{|\phi_{S_n}(t)-\phi_{S'_n}(t)|}_{\longrightarrow 0}+|\underbrace{\exp(s_n(e^{it}-1))-\exp(\lambda(e^{it}-1))|}_{\longrightarrow 0 \text{ car } s_n\longrightarrow\lambda} \quad \longrightarrow 0\end{aligned}$$

et le théorème de Lévy permet de conclure. □

40 Transformée de Fourier d'une gaussienne

On calcule la transformée de Fourier d'une fonction de type gaussienne $x \mapsto e^{-ax^2}$ à l'aide du théorème intégral de Cauchy.

Proposition 1. On définit $\forall a \in \mathbb{R}_*^+$,

$$\gamma_a : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & e^{-ax^2} \end{array}$$

Alors,

$$\forall \xi \in \mathbb{R}, \widehat{\gamma_a}(\xi) = \sqrt{\frac{\pi}{a}} e^{\frac{-\xi^2}{4a}}$$

[AMR08] p. 156

Démonstration. Soit $a \in \mathbb{R}_*^+$. On a

$$\forall \xi \in \mathbb{R}, \widehat{\gamma_a}(\xi) = \int_{-\infty}^{+\infty} e^{-ax^2} e^{-ix\xi} \, \mathrm{d}x$$

et en écrivant

$$ax^2 + ix\xi = a\left(x^2 + i\frac{x\xi}{a}\right) = a\left(\left(x + i\frac{\xi}{2a}\right)^2 + \frac{\xi^2}{4a^2}\right)$$

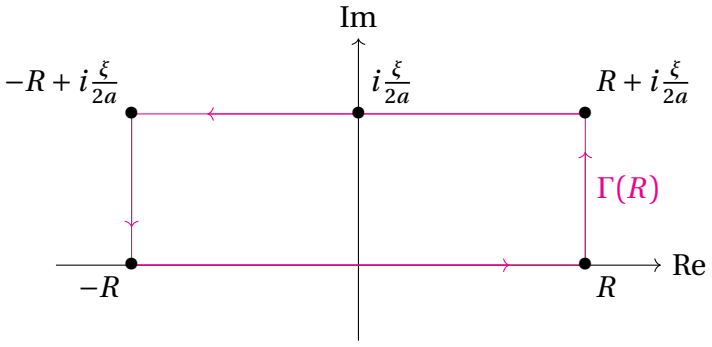
on en déduit que

$$\forall \xi \in \mathbb{R}, \widehat{\gamma_a}(\xi) = e^{-\frac{\xi^2}{4a}} \int_{-\infty}^{+\infty} e^{-a\left(x+i\frac{\xi}{2a}\right)^2} \, \mathrm{d}x \qquad (*)$$

On va considérer la fonction

$$\begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ z & \mapsto & e^{-az^2} \end{array}$$

Pour $R > 0$ et $\xi \in \mathbb{R}$, on note $\Gamma(R)$ le rectangle de sommets $-R, R, R + i\frac{\xi}{2a}, -R + i\frac{\xi}{2a}$ parcouru dans le sens direct :



On a,

$$\underbrace{\int_{\Gamma(R)} e^{-az^2} \, \mathrm{d}z}_{=I(R)} = \underbrace{\int_{-R}^{R} e^{-az^2} \, \mathrm{d}z}_{=I_1(R)} + \underbrace{\int_{R}^{R+i\frac{\xi}{2a}} e^{-az^2} \, \mathrm{d}z}_{=I_2(R)} + \underbrace{\int_{R+i\frac{\xi}{2a}}^{-R+i\frac{\xi}{2a}} e^{-az^2} \, \mathrm{d}z}_{=I_3(R)} + \underbrace{\int_{-R+i\frac{\xi}{2a}}^{-R} e^{-az^2} \, \mathrm{d}z}_{=I_4(R)}$$

Nous allons traiter les intégrales séparément.

— Pour $I_1(R)$: On a affaire à une intégrale sur l'axe réel. Or, on connait la valeur de l'intégrale de Gauss :

$$\int_{-\infty}^{+\infty} e^{-y^2}\,\mathrm{d}y = \sqrt{\pi}$$

Donc en faisant le changement de variable $y = \sqrt{a}x$, on obtient :

$$\sqrt{a}\int_{-\infty}^{+\infty} e^{-ax^2}\,\mathrm{d}x = \sqrt{\pi} \iff \int_{-\infty}^{+\infty} e^{-ax^2}\,\mathrm{d}x = \sqrt{\frac{\pi}{a}}$$

D'où :

$$I_1(R) \longrightarrow \sqrt{\frac{\pi}{a}}$$

quand $R \longrightarrow +\infty$.

— Pour $I_2(R)$: On a :

$$\begin{aligned} &\forall z \in \left[R, R + i\frac{\xi}{2a}\right],\ z = R + it \text{ avec } t \in \left[0, \frac{\xi}{2a}\right] \\ \Longrightarrow\ &\mathrm{d}z = i\mathrm{d}t \end{aligned}$$

D'où :

$$I_2(R) = i\int_0^{\frac{\xi}{2a}} e^{-a(R+it)^2}\,\mathrm{d}t$$

On en déduit,

$$\begin{aligned} |I_2(R)| &\leq \int_0^{\frac{\xi}{2a}} \left|e^{-a(R+it)^2}\right| \mathrm{d}t \\ &= \int_0^{\frac{\xi}{2a}} \left|e^{-a(R^2-t^2)}\right| \underbrace{|e^{i2aRt}|}_{=1}\,\mathrm{d}t \\ &= \int_0^{\frac{\xi}{2a}} e^{-a(R^2-t^2)}\,\mathrm{d}t \\ &= e^{-aR^2}\int_0^{\frac{\xi}{2a}} e^{at^2}\,\mathrm{d}t \\ &\longrightarrow 0 \end{aligned}$$

quand $R \longrightarrow +\infty$.

— Pour $I_3(R)$: On a :

$$\begin{aligned} &\forall z \in \left[R + i\frac{\xi}{2a}, -R + i\frac{\xi}{2a}\right],\ z = t + i\frac{\xi}{2a} \text{ avec } t \in [R, -R] \\ \Longrightarrow\ &\mathrm{d}z = \mathrm{d}t \end{aligned}$$

D'où :

$$I_3(R) = \int_R^{-R} e^{-a\left(t+i\frac{\xi}{2a}\right)^2}\,\mathrm{d}t = -\int_{-R}^{R} e^{-a\left(t+i\frac{\xi}{2a}\right)^2}\,\mathrm{d}t = -e^{\frac{\xi^2}{4a}}\int_{-R}^{R} e^{-a\left(t+i\frac{\xi}{2a}\right)^2}\,\mathrm{d}t$$

qui est une intégrale généralisée absolument convergente. Ainsi par $(*)$,

$$I_3(R) \longrightarrow -e^{\frac{\xi^2}{4a}}\widehat{\gamma_a}(\xi)$$

quand $R \longrightarrow +\infty$.

— Pour $I_4(R)$: Ce cas-ci se traite exactement comme $I_2(R)$. On a :

$$\begin{aligned} &\forall z \in \left[-R + i\frac{\xi}{2a}, -R\right], z = -R + it \text{ avec } t \in \left[\frac{\xi}{2a}, 0\right] \\ \Longrightarrow\ &\mathrm{d}z = i\mathrm{d}t \end{aligned}$$

D'où :

$$I_4(R) = i\int_{\frac{\xi}{2a}}^{0} e^{-a(-R+it)^2}\,\mathrm{d}t = -i\int_{0}^{\frac{\xi}{2a}} e^{-a(-R+it)^2}\,\mathrm{d}t$$

On en déduit,

$$|I_4(R)| \leq \int_0^{\frac{\xi}{2a}} \left|e^{-a(-R+it)^2}\right| \mathrm{d}t = e^{-aR^2}\int_0^{\frac{\xi}{2a}} e^{at^2}\,\mathrm{d}t \longrightarrow 0$$

quand $R \longrightarrow +\infty$.

— Pour $I(R)$: La fonction $z \mapsto e^{-az^2}$ est holomorphe et le contour $\Gamma(R)$ est fermé. Donc $I(R) = 0$ en vertu du théorème intégral de Cauchy.

En passant à la limite, on obtient ainsi :

$$0 = \sqrt{\frac{\pi}{a}} + 0 - e^{\frac{\xi^2}{4a}}\widehat{\gamma_a}(\xi) + 0 \iff \widehat{\gamma_a}(\xi) = \sqrt{\frac{\pi}{a}}e^{\frac{-\xi^2}{4a}}$$

□

41 Trigonalisation simultanée

Nous montrons le théorème de trigonalisation simultanée grâce à l'utilisation des applications transposées (et donc, de la dualité).

Soit E un espace vectoriel de dimension n sur un corps $\mathbb{K}$.

[GOU21] p. 176

Lemme 1. Soit $g \in \mathscr{L}(E)$ un endomorphisme. Soit F un sous-espace vectoriel de E stable par g. Alors,

$$\chi_{g_{|F}} \mid \chi_g$$

Démonstration. On note m la dimension de F. Considérons G, un supplémentaire de F dans E. Soient $\mathscr{B}_F$ et $\mathscr{B}_G$ des bases respectives de F et de G. Alors, la matrice de g dans la base de E constituée de l'union disjointe de $\mathscr{B}_F$ et $\mathscr{B}_G$ est de la forme

$$M = \begin{pmatrix} A & * \\ 0 & * \end{pmatrix}$$

avec $A \in \mathscr{M}_m(\mathbb{K})$, qui est la matrice de l'endomorphisme induit $g_{|F}$. On constate clairement que $\chi_{g_{|F}} = \chi_A \mid \chi_M = \chi_g$. □

Lemme 2. Soit $g \in \mathscr{L}(E)$ un endomorphisme trigonalisable. Soit F un sous-espace vectoriel de E stable par g. Alors, $g_{|F}$ est trigonalisable.

Démonstration. g est trigonalisable si et seulement si son polynôme caractéristique est scindé sur $\mathbb{K}$. Dans ce cas, le polynôme caractéristique de sa restriction à F l'est aussi au vu du Théorème 1. □

Lemme 3. Soient $f, g \in \mathscr{L}(E)$. On suppose que f et g sont trigonalisables et commutent. Alors, f et g ont un vecteur propre commun.

Démonstration. f est trigonalisable, donc f admet une valeur propre $\lambda \in \mathbb{K}$ (cf. première colonne de la matrice de f dans une base de trigonalisation). Le sous-espace propre $E_\lambda = \operatorname{Ker}(f - \lambda \operatorname{id}_E)$ est alors stable par g :

$$\forall x \in E_\lambda, (f - \lambda \operatorname{id}_E)(g(x)) = g((f - \lambda \operatorname{id}_E)(x))$$

car f, g et $\lambda \operatorname{id}_E$ commutent. Ainsi,

$$\forall x \in E_\lambda, (f - \lambda \operatorname{id}_E)(g(x)) = 0$$

Par le Théorème 2, la restriction de g à E_λ est trigonalisable. Donc, $g_{|E_\lambda}$ admet un vecteur propre $x \in E_\lambda$ qui est, par construction, un vecteur propre commun à f et g. □

Théorème 4 (Trigonalisation simultanée)**.** Soient $f, g \in \mathscr{L}(E)$. On suppose que f et g sont trigonalisables et commutent. Alors, il existe une base de trigonalisation commune de f et g.

Démonstration. On va procéder par récurrence sur n.

— Si $n = 1$: c'est évident.

— Supposons le résultat vrai au rang $n-1$. Pour tout $\varphi \in E^*$,

$$\begin{aligned}({}^t f \circ {}^t g)(\varphi) &= {}^t f(\varphi \circ g)\\ &= \varphi \circ g \circ f\\ &= \varphi \circ f \circ g\\ &= ({}^t g \circ {}^t f)(\varphi)\end{aligned}$$

ie. ${}^t f {}^t g = {}^t f {}^t g$. De plus, ${}^t f$ et ${}^t g$ sont trigonalisables (car possèdent les mêmes polynômes caractéristiques que f et g). Par le Théorème 3 appliqué à ${}^t f$ et ${}^t g$, il existe un vecteur propre $\psi \in E^*$ commun à ces deux endomorphismes. Le sous-espace vectoriel $\mathrm{Vect}(\psi)$ est ainsi stable par ${}^t f$ et ${}^t g$. Notons

$$H = \mathrm{Vect}(\psi)^\circ = \{x \in E \mid \psi(x) = 0\} = \mathrm{Ker}(\psi)$$

c'est un hyperplan de E (donc de dimension $n-1$), qui est de plus stable par f et g. En effet, en notant $\lambda \in \mathbb{K}$ la valeur propre de f associée à ψ, on a :

$$\forall x \in H,\ \psi(f(x)) = {}^t f(\psi)(x) = \lambda \psi(x) = 0$$

et un même calcul montre la stabilité par g. D'après l'hypothèse de récurrence appliquée aux endomorphismes induits $f_{|H}$ et $g_{|H}$, on obtient une base $\mathscr{B}_H$ de H de cotrigonalisation pour $f_{|H}$ et $g_{|H}$. On la complète en une base quelconque $\mathscr{B}$ de E, dans laquelle on obtient

$$\mathrm{Mat}(f, \mathscr{B}) = \begin{pmatrix} & \mathrm{Mat}(f_{|H}, \mathscr{B}_H) & & * \\ & & & \vdots \\ & & & * \\ 0 & \cdots & 0 & * \end{pmatrix} \text{ et } \mathrm{Mat}(g, \mathscr{B}) = \begin{pmatrix} & \mathrm{Mat}(g_{|H}, \mathscr{B}_H) & & * \\ & & & \vdots \\ & & & * \\ 0 & \cdots & 0 & * \end{pmatrix}$$

où $\mathrm{Mat}(f_{|H}, \mathscr{B}_H)$ et $\mathrm{Mat}(g_{|H}, \mathscr{B}_H)$ sont triangulaires supérieures d'ordre $n-1$.

□

Bibliographie

Analyse de Fourier dans les espaces fonctionnels **[AMR08]**

Mohammed El-Amrani. *Analyse de Fourier dans les espaces fonctionnels. Niveau M1*. Ellipses, 28 août 2008.
https://www.editions-ellipses.fr/accueil/3908-14232-analyse-de-fourier-dans-les-espaces-fonctionnels-niveau-m1-9782729839031.html.

Suites et séries numériques, suites et séries de fonctions **[AMR11]**

Mohammed El-Amrani. *Suites et séries numériques, suites et séries de fonctions*. Ellipses, 15 nov. 2011.
https://www.editions-ellipses.fr/accueil/3910-14234-suites-et-series-numeriques-suites-et-series-de-fonctions-9782729870393.html.

Objectif agrégation **[BMP]**

Vincent Beck, Jérome Malick et Gabriel Peyré. *Objectif agrégation*. 2e éd. H&K, 22 août 2005.
https://objectifagregation.github.io.

Analyse **[B-P]**

Marc Briane et Gilles Pages. *Analyse. Théorie de l'intégration*. 8e éd. De Boeck Supérieur, 29 août 2023.
https://www.deboecksuperieur.com/ouvrage/9782807359550-analyse-theorie-de-l-integration.

Nouvelles histoires hédonistes de groupes et de géométries **[C-G]**

Philippe Caldero et Jérôme Germoni. *Nouvelles histoires hédonistes de groupes et de géométries. Tome 1*. Calvage & Mounet, 13 mai 2017.
http://www.calvage-et-mounet.fr/2022/05/09/nouvelles-histoires-hedoniste-de-groupes-et-de-geometrie/.

Mathématiques pour l'agrégation **[DAN]**

Jean-François Dantzer. *Mathématiques pour l'agrégation. Analyse et probabilités*. De Boeck Supérieur, 20 avr. 2021.
https://www.deboecksuperieur.com/ouvrage/9782807332904-mathematiques-pour-l-agregation-analyse-et-probabilites.

Analyse numérique et équations différentielles **[DEM]**

Jean-Pierre Demailly. *Analyse numérique et équations différentielles*. 4e éd. EDP Sciences, 11 mai 2016.
https://www.uga-editions.com/menu-principal/collections-et-revues/collections/grenoble-sciences/analyse-numerique-et-equations-differentielles-239866.kjsp.

Leçons pour l'agrégation de mathématiques **[D-L]**

Maximilien Dreveton et Joachim Lhabouz. *Leçons pour l'agrégation de mathématiques. Préparation à l'oral*. Ellipses, 28 mai 2019.
https://www.editions-ellipses.fr/accueil/3543-13866-lecons-pour-lagregation-de-mathematiques-preparation-a-loral-9782340030183.html.

Oraux X-ENS Mathématiques **[FGN3]**

Serge Francinou, Hervé Gianella et Serge Nicolas. *Oraux X-ENS Mathématiques. Volume 3*. 3e éd. Cassini, 27 mai 2020.
https://store.cassini.fr/fr/enseignement-des-mathematiques/103-oraux-x-ens-mathematiques-nouvelle-serie-vol-3.html.

Oraux X-ENS Mathématiques **[FGN2]**

Serge Francinou, Hervé Gianella et Serge Nicolas. *Oraux X-ENS Mathématiques. Volume 2*. 2e éd. Cassini, 16 mars 2021.
https://store.cassini.fr/fr/enseignement-des-mathematiques/111-oraux-x-ens-mathematiques-nouvelle-serie-vol-2.html.

De l'intégration aux probabilités **[G-K]**

Olivier Garet et Aline Kurtzmann. *De l'intégration aux probabilités*. 2e éd. Ellipses, 28 mai 2019.
https://www.editions-ellipses.fr/accueil/4593-14919-de-l-integration-aux-probabilites-2e-edition-augmentee-9782340030206.html.

Les maths en tête **[GOU20]**

Xavier Gourdon. *Les maths en tête. Analyse*. 3e éd. Ellipses, 21 avr. 2020.
https://www.editions-ellipses.fr/accueil/10446-les-maths-en-tete-analyse-3e-edition-9782340038561.html.

Les maths en tête **[GOU21]**

Xavier Gourdon. *Les maths en tête. Algèbre et probabilités*. 3e éd. Ellipses, 13 juill. 2021.
https://www.editions-ellipses.fr/accueil/13722-25266-les-maths-en-tete-algebre-et-probabilites-3e-edition-9782340056763.html.

Théorie de Galois **[GOZ]**

Ivan Gozard. *Théorie de Galois. Niveau L3-M1*. 2e éd. Ellipses, 1er avr. 2009.
https://www.editions-ellipses.fr/accueil/4897-15223-theorie-de-galois-niveau-l3-m1-2e-edition-9782729842772.html.

Algèbre Linéaire **[GRI]**

Joseph GRIFONE. *Algèbre Linéaire*. 6e éd. Cépaduès, 9 jan. 2019.
https://www.cepadues.com/livres/algebre-lineaire-edition-9782364936737.html.

Les Contre-Exemples en Mathématiques **[HAU]**

Bertrand HAUCHECORNE. *Les Contre-Exemples en Mathématiques*. 2e éd. Ellipses, 13 juin 2007.
https://www.editions-ellipses.fr/accueil/5328-les-contre-exemples-en-mathematiques-9782729834180.html.

L'oral à l'agrégation de mathématiques **[I-P]**

Lucas ISENMANN et Timothée PECATTE. *L'oral à l'agrégation de mathématiques. Une sélection de développements*. 2e éd. Ellipses, 26 mars 2024.
https://www.editions-ellipses.fr/accueil/15218-28346-loral-a-lagregation-de-mathematiques-une-selection-de-developpements-2e-edition-9782340086487.html.

Cours d'analyse fonctionnelle **[LI]**

Daniel LI. *Cours d'analyse fonctionnelle. avec 200 exercices corrigés*. Ellipses, 3 déc. 2013.
https://www.editions-ellipses.fr/accueil/6558-cours-danalyse-fonctionnelle-avec-200-exercices-corriges-9782729883058.html.

Algèbre et calcul formel **[FFN]**

Loïc Foissy ODILE FLEURY et Alain NINET. *Algèbre et calcul formel. Agrégation de Mathématiques Option C*. 2e éd. Ellipses, 9 mai 2023.
https://www.editions-ellipses.fr/accueil/14799-algebre-et-calcul-formel-agregation-de-mathematiques-option-c-2e-edition-9782340078567.html.

Cours d'algèbre **[PER]**

Daniel PERRIN. *Cours d'algèbre. pour l'agrégation*. Ellipses, 15 fév. 1996.
https://www.editions-ellipses.fr/accueil/7778-18110-cours-d-algebre-agregation-9782729855529.html.

L'algèbre discrète de la transformée de Fourier **[PEY]**

Gabriel PEYRÉ. *L'algèbre discrète de la transformée de Fourier. Niveau M1*. Ellipses, 15 jan. 2004.
https://adtf-livre.github.io.

Analyse complexe et applications **[QUE]**

Martine QUEFFÉLLEC et Hervé QUEFFÉLEC. *Analyse complexe et applications. Nouveau tirage*. Calvage & Mounet, 13 mai 2017.
http://www.calvage-et-mounet.fr/2022/05/09/analyse-complexe-et-applications/.

Formulaire de maths **[R-R]**

Olivier Rodot et Jean-Étienne Rombaldi. *Formulaire de maths. Avec résumés de cours*. De Boeck Supérieur, 30 août 2022.
https://www.deboecksuperieur.com/ouvrage/9782807339880-formulaire-de-maths.

Analyse matricielle **[ROM19-2]**

Jean-Étienne Rombaldi. *Analyse matricielle. Cours et exercices résolus*. 2e éd. EDP Sciences, 7 nov. 2019.
https://laboutique.edpsciences.fr/produit/1101/9782759824199/analyse-matricielle-cours-et-exercices-resolus.

Éléments d'analyse réelle **[ROM19-1]**

Jean-Étienne Rombaldi. *Éléments d'analyse réelle*. 2e éd. EDP Sciences, 6 juin 2019.
https://laboutique.edpsciences.fr/produit/1082/9782759823789/elements-d-analyse-reelle.

Mathématiques pour l'agrégation **[ROM21]**

Jean-Étienne Rombaldi. *Mathématiques pour l'agrégation. Algèbre et géométrie*. 2e éd. De Boeck Supérieur, 20 avr. 2021.
https://www.deboecksuperieur.com/ouvrage/9782807332201-mathematiques-pour-l-agregation-algebre-et-geometrie.

Petit guide de calcul différentiel **[ROU]**

François Rouvière. *Petit guide de calcul différentiel. à l'usage de la licence et de l'agrégation*. 4e éd. Cassini, 27 fév. 2015.
https://store.cassini.fr/fr/enseignement-des-mathematiques/94-petit-guide-de-calcul-differentiel-4e-ed.html.

Anneaux, corps, résultants **[ULM18]**

Felix Ulmer. *Anneaux, corps, résultants. Algèbre pour L3/M1/agrégation*. Ellipses, 28 août 2018.
https://www.editions-ellipses.fr/accueil/9852-20186-anneaux-corps-resultants-algebre-pour-l3-m1-agregation-9782340025752.html.

Théorie des groupes **[ULM21]**

Felix Ulmer. *Théorie des groupes. Cours et exercices*. 2e éd. Ellipses, 3 août 2021.
https://www.editions-ellipses.fr/accueil/13760-25304-theorie-des-groupes-2e-edition-9782340057241.html.

Analyse pour l'agrégation **[Z-Q]**

Claude ZUILY et Hervé QUEFFÉLEC. *Analyse pour l'agrégation. Agrégation/Master Mathématiques.* 5e éd. Dunod, 26 août 2020.

https://www.dunod.com/prepas-concours/analyse-pour-agregation-agregationmaster-mathematiques.