
Développements pour les oraux d'agrégation

Pierrick Le Vourc'h

Table des matières

1	Classement des développements	3
1.1	Leçons d'algèbre et géométrie	3
1.2	Leçons d'analyse et probabilités	5
2	Enveloppe convexe de $\exp(M_n(\mathbf{R}))$	7
3	Développement alternatif : image de l'exponentielle matricielle	10
4	Corps des nombres algébriques	12
5	Loi de réciprocité quadratique	14
6	Déterminant de Gram et inégalité d'Hadamard	16
7	$SO_3(\mathbf{R})$ et les quaternions	18
8	Compacité dans un espace de Banach	20
9	Convergence des méthodes itératives et caractérisation du rayon spectral	22
10	Inégalité de Hardy	25
11	Hadamard-Lévy	27
12	Processus de branchement de Galton-Watson	29
13	Formule des compléments	31
14	Générateurs de $O(E)$, $SO(E)$	33
15	Générateurs des groupes linéaire et spécial linéaire, application à la connexité	34
16	Théorème du point fixe de Brouwer	36
17	Calcul de l'intégrale de Fresnel	39
18	Moyenne arithmético-géométrique, application à la méthode des isopérimètres	41
19	Inégalité de Le Cam	42
20	Sous-espace engendré par les translatées d'une fonction	44
21	Morphismes continus de S^1 dans $GL_n(\mathbf{R})$.	46
22	Codiagonalisation d'une famille d'endomorphismes	48
23	Séries de Hardy	50

24	Permutations, convergence et somme	52
25	Théorème de Lévy et application au théorème central limite (non rédigé)	54
26	Borel-Cantelli et application aux nombres premiers	56
27	Équation de la chaleur	58
28	Fonctions dont la série des coefficients de Fourier converge absolument	61
29	Théorème ergodique de Von Neumann	63
30	Résolution d'une équation aux dérivées partielles elliptiques	65
31	Lemme de Schwarz et automorphismes bianalytiques du disque	67
32	Simplicité de $SO_3(\mathbb{R})$	69
33	Polynômes cyclotomiques et théorème de Wedderburn	71
34	Indécomposabilité de la loi de Poisson	73
35	Théorème de Fourier-Plancherel	75
36	Théorème de Sharkowski	76
37	Isométries du cube	78
38	Ellipsoïde de John-Loewner	80
39	Équation de Pell-Fermat	83
40	Décomposition polaire	85
41	Enveloppe convexe de $O_n(\mathbb{R})$	86
42	Dénombrement des polynômes irréductibles unitaires sur un corps fini	87
43	Algorithme de descente de gradient à pas optimal	89
44	Nombres de Bell	91
45	Système de congruences	93
46	Conditions de cyclicité de $(\mathbb{Z}/n\mathbb{Z})^\times$	95
47	Théorèmes de point fixe compact	96
48	Théorème de Weierstrass par les probabilités	99
49	Système de Lotka-Volterra	101
50	Théorème de structure des polynômes symétriques	103
51	Action de Steinitz	104
52	Théorème de Cauchy-Lipschitz linéaire	105
53	Prolongement méromorphe de la fonction Gamma d'Euler	107
54	Autres résultats rédigés toujours utiles	108

1 Classement des développements

1.1 Leçons d'algèbre et géométrie

Leçon	Développements
101	$SO_3(\mathbf{R})$ et les quaternions Polynômes cyclotomiques et théorème de Wedderburn Isométries du cube
102	Morphismes continus de $\mathbf{S}^1$ dans $GL_n(\mathbf{R})$ Polynômes cyclotomiques et théorème de Wedderburn
103	Polynômes cyclotomiques et théorème de Wedderburn Simplicité de $SO_3(\mathbf{R})$
104	Conditions de cyclicité de $(\mathbf{Z}/n\mathbf{Z})^\times$ Isométries du cube Polynômes cyclotomiques et théorème de Wedderburn
105	Théorème de structure des polynômes symétriques Isométries du cube
106	Morphismes continus de $\mathbf{S}^1$ dans $GL_n(\mathbf{R})$ $SO_3(\mathbf{R})$ et les quaternions
108	Générateurs des groupes linéaire et spécial linéaire, application à la connexité Conditions de cyclicité de $(\mathbf{Z}/n\mathbf{Z})^\times$ Équation de Pell-Fermat Générateurs de $O(E)$, $SO(E)$
120	Système de congruences Conditions de cyclicité de $(\mathbf{Z}/n\mathbf{Z})^\times$
121	Loi de réciprocité quadratique Conditions de cyclicité de $(\mathbf{Z}/n\mathbf{Z})^\times$ Borel-Cantelli et application aux nombres premiers
122	Développement Développement
123	Loi de réciprocité quadratique Dénombrement des polynômes irréductibles unitaires sur un corps fini Polynômes cyclotomiques et théorème de Wedderburn
125	Corps des nombres algébriques Dénombrement des polynômes irréductibles unitaires sur un corps fini Loi de reciprocite quadratique
126	Loi de réciprocité quadratique Système de congruences Équation de Pell-Fermat
141	Corps des nombres algébriques Dénombrement des polynômes irréductibles unitaires sur un corps fini
142	Système de congruences Développement
144	Corps des nombres algébriques Théorème de structure des polynômes symétriques
149	Convergence des méthodes itératives Algorithme de descente de gradient à pas optimal
150	$SO_3(\mathbf{R})$ et les quaternions Action de Steinitz
151	Sous-espace engendré par les translatées d'une fonction Générateurs de $O(E)$, $SO(E)$
152	Déterminant de Gram et inégalité d'Hadamard Ellipsoïde de John-Loewner
153	Développement alternatif : image de l'exponentielle matricielle Codiagonalisation d'une famille d'endomorphismes
154	Générateurs de $O(E)$, $SO(E)$ Codiagonalisation d'une famille d'endomorphismes

155	Codiagonalisation d'une famille d'endomorphismes Enveloppe convexe de $\exp(M_n(\mathbf{R}))$ Warning
156	Enveloppe convexe de $\exp(M_n(\mathbf{R}))$ Morphismes continus de $\mathbf{S}^1$ dans $GL_n(\mathbf{R})$
157	Codiagonalisation d'une famille d'endomorphismes Morphismes continus de $\mathbf{S}^1$ dans $GL_n(\mathbf{R})$
158	Ellipsoïde de John-Loewner Algorithme de descente de gradient à pas optimal Enveloppe convexe de $O_n(\mathbf{R})$
159	Sous-espace engendré par les translatées d'une fonction Enveloppe convexe de $O_n(\mathbf{R})$
160	Générateurs de $O(E)$, $SO(E)$ Enveloppe convexe de $O_n(\mathbf{R})$
161	$SO_3(\mathbf{R})$ et les quaternions Générateurs de $O(E)$, $SO(E)$ Enveloppe convexe de $O_n(\mathbf{R})$ Isométries du cube
162	Convergence des méthodes itératives Générateurs des groupes linéaire et spécial linéaire, application à la connexité
170	Générateurs de $O(E)$, $SO(E)$ Développement
171	Équation de Pell-Fermat Ellipsoïde de John-Loewner
181	Enveloppe convexe de $O_n(\mathbf{R})$ Ellipsoïde de John-Loewner
190	Dénombrement des polynômes irréductibles unitaires sur un corps fini Nombres de Bell
191	Isométries du cube Équation de Pell-Fermat

1.2 Leçons d'analyse et probabilités

Leçon	Développements
201	Compacité dans un espace de Banach Fonctions dont la série des coefficients de Fourier converge absolument Théorème de Fourier-Plancherel Résolution d'une équation aux dérivées partielles elliptiques
203	Compacité dans un espace de Banach Théorèmes de point fixe compact Théorème du point fixe de Brouwer
204	Hadamard-Lévy Théorème de Sharkowski Simplicité de $SO_3(\mathbf{R})$
205	Compacité dans un espace de Banach Inégalité de Hardy
207	Prolongement méromorphe de la fonction Gamma d'Euler Théorème de Fourier-Plancherel Inégalité de Hardy
208	Compacité dans un espace de Banach Théorème de Fourier-Plancherel Théorème ergodique de Von Neumann Inégalité de Hardy
209	Théorème de Weierstrass par les probabilités Théorème de Fourier-Plancherel Inégalité de Hardy
213	Théorème ergodique de Von Neumann Résolution d'une équation aux dérivées partielles elliptiques
214	Hadamard-Lévy Théorème du point fixe de Brouwer
215	Hadamard-Lévy Théorème du point fixe de Brouwer
219	Ellipsoïde de John-Loewner Algorithme de descente de gradient à pas optimal
220	Hadamard-Lévy Système différentiel de Lotka-Volterra
221	Théorème de Cauchy-Lipschitz linéaire Équation de la chaleur
222	Équation de la chaleur Résolution d'une équation aux dérivées partielles elliptiques
223	Moyenne arithmético-géométrique, application à la méthode des isopérimètres Théorèmes de point fixe compact
226	Théorème de Sharkowski Théorèmes de point fixe compact Algorithme de descente de gradient à pas optimal
228	Théorème de Sharkowski Système différentiel de Lotka-Volterra
229	Processus de branchement de Galton-Watson Warning Algorithme de descente de gradient à pas optimal Système différentiel de Lotka-Volterra Ellipsoïde de John-Loewner
230	Séries de Hardy Borel-Cantelli et application aux nombres premiers Permutations, convergence et somme
234	Inégalité de Hardy Théorème de Fourier-Plancherel
235	Formule des compléments Calcul de l'intégrale de Fresnel Théorème de Fourier-Plancherel
236	Formule des compléments Calcul de l'intégrale de Fresnel

239	Formule des compléments Calcul de l'intégrale de Fresnel
241	Équation de la chaleur Nombres de Bell Indécomposabilité de la loi de Poisson
243	Indécomposabilité de la loi de Poisson Nombres de Bell
245	Formule des compléments Indécomposabilité de la loi de Poisson Lemme de Schwarz et automorphismes bianalytiques du disque
246	Équation de la chaleur Fonctions dont la série des coefficients de Fourier converge absolument
250	Théorème de Fourier-Plancherel Théorème de Lévy et application au théorème central limite
253	Algorithme de descente de gradient à pas optimal Ellipsoïde de John-Loewner
261	Théorème de Lévy et application au théorème central limite Indécomposabilité de la loi de Poisson Processus de branchement de Galton-Watson
262	Inégalité de Le Cam Borel-Cantelli et application aux nombres premiers Théorème de Lévy et application au théorème central limite
264	Processus de branchement de Galton-Watson Indécomposabilité de la loi de Poisson Inégalité de Le Cam
265	Calcul de l'intégrale de Fresnel Borel-Cantelli et application aux nombres premiers
266	Borel-Cantelli et application aux nombres premiers Indécomposabilité de la loi de Poisson
267	Système différentiel de Lotka-Volterra Formule des compléments

2 Enveloppe convexe de $\exp(M_n(\mathbf{R}))$

Leçons : 153, 156, 157 ? 181 ?

Référence: Un max de maths, Zavidovique

| **Proposition** — L'enveloppe convexe de $\exp(M_n(\mathbf{R}))$ est $M_n(\mathbf{R})$ tout entier pour tout $n > 1$.

| **Application** — L'enveloppe convexe de $\{A^2, A \in M_n(\mathbf{R})\} = M_n(\mathbf{R})$.

| **Théorème** — (Variante du développement) $\exp(M_n(\mathbf{C})) = GL_n(\mathbf{C})$

Démonstration — Preuve de la proposition

- Toute matrice $M \in M_n(\mathbf{R})$ dont les coefficients diagonaux sont strictement positifs s'écrit comme somme de deux exponentielles.

Soit $M \in M_n(\mathbf{R})$ de coefficients diagonaux strictement positifs. On écrit

$$M = \begin{pmatrix} \alpha_1 & & & \\ & \ddots & & T_1 \\ & & \ddots & \\ & T_2 & & \ddots \\ & & & & \alpha_n \end{pmatrix}.$$

Soit $N > \max \left(n, \max \left(\frac{2}{|\alpha_i - \alpha_j|} \right) \right)$ pour i, j tels que $\alpha_i \neq \alpha_j$. On définit deux matrices :

$$M_1 = \begin{pmatrix} \frac{\alpha_1}{2} + \frac{1}{N^2} & & & \\ & \ddots & & T_1 \\ & & \ddots & \\ & 0 & & \ddots & \\ & & & & \frac{\alpha_n}{2} + \frac{n}{N^2} \end{pmatrix}, \quad M_2 = \begin{pmatrix} \frac{\alpha_1}{2} - \frac{1}{N^2} & & & \\ & \ddots & & 0 \\ & & \ddots & \\ & T_2 & & \ddots & \\ & & & & \frac{\alpha_n}{2} - \frac{n}{N^2} \end{pmatrix}.$$

On a bien $M = M_1 + M_2$ et M_1, M_2 sont triangulaires (l'une inférieure, l'autre supérieure) avec des termes diagonaux strictement positifs et deux-à-deux distincts. Elles sont donc diagonalisables à valeurs propres strictement positives. Les matrices diagonales de coefficients strictement positifs sont dans l'image de l'exponentielle donc par continuité de la conjugaison, M_1 et M_2 sont dans l'image de l'exponentielle, et *a fortiori* $2M_1$ et $2M_2$ le sont aussi. On en déduit que M est dans l'enveloppe convexe de l'image de l'exponentielle en écrivant

$$M = \frac{1}{2}(2M_1 + 2M_2)$$

.

- Si n est pair, alors $-\text{Id}_n$ est dans l'image de l'exponentielle.

Regardons le cas $n = 2$. Rappelons que dans $\mathbf{R}^2$, multiplier par $J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ revient à effectuer une multiplication par i . De la relation $e^{i\pi} = -1$, on déduit que

$$e^{\pi J} = -\text{Id}_2.$$

En dimension n paire quelconque, on vérifie que la matrice diagonale par blocs $J_n = \begin{pmatrix} J & & 0 \\ & \ddots & \\ 0 & & J \end{pmatrix}$ vérifie

$$e^{\pi J_n} = -\text{Id}_n.$$

- Si $n > 1$ impair, il existe une matrice dont les coefficients diagonaux sont strictement négatifs et qui appartient à l'enveloppe convexe de l'exponentielle.

On utilise deux fois la question précédente. On introduit les matrices

$$B_n^1 = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & -\text{Id}_{n-1} \end{pmatrix} = \exp \left(\begin{pmatrix} -\log(2) & 0 \\ 0 & \pi J_{n-1} \end{pmatrix} \right), \quad B_n^2 = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & -\text{Id}_{n-1} \end{pmatrix} = \exp \left(\begin{pmatrix} \pi J_{n-1} & 0 \\ 0 & -\log \pi J_{n-1}(2) \end{pmatrix} \right).$$

La demi-somme $B_n = \begin{pmatrix} -\frac{1}{2} & 0 & 0 \\ 0 & -\text{Id}_{n-2} & 0 \\ 0 & 0 & -\frac{1}{2} \end{pmatrix}$ de ces deux matrices est donc dans l'enveloppe convexe de l'exponentielle réelle.

• Conclusion

Notons B_n la matrice exhibée ci-dessus si n est impaire et $-\text{Id}_n$ si n est paire. Ainsi, dans tous les cas, la matrice B_n est à coefficients diagonaux strictement négatifs et dans l'enveloppe convexe de l'image de l'exponentielle.

Soit $M \in M_n(\mathbf{K})$ quelconque. Soit $K \in \mathbf{R}$ tel que les coefficients diagonaux de $M - KB_n$ est à coefficients diagonaux strictement positifs (il suffit de prendre $\frac{K}{2}$ plus grand que tous les coefficients diagonaux de M). Par le point 1, on peut donc écrire $M - KB_n$ comme somme de deux matrices M_1 et M_2 qui sont dans l'image de l'exponentielle. Mais alors,

$$M = \frac{1}{3}(3KB_n + 3M_1 + 3M_2)$$

est bien dans l'enveloppe convexe de l'image de l'exponentielle. □

Démonstration — Preuve de l'application

- Si $M \in M_n(\mathbf{R})$, il existe $\tilde{M}$ de valeurs propres toutes positives et telle que $M^2 = \tilde{M}^2$.

Posons $Q = \prod_{\lambda \in \text{sp}(M) \cap \mathbf{R}^+} (X - \lambda)$ et $R = \prod_{\lambda \in \text{sp}(M) \cap (\mathbf{C} \setminus \mathbf{R}^+)} (X - \lambda)$.

Les polynômes Q et R sont réels et premiers entre eux par construction, et $\chi_M = QR$. Par le théorème de Cayley-Hamilton, on a donc que $Q(M)R(M) = 0$, et par le lemme des noyaux, $E = \text{Ker}(Q(M)) \oplus \text{Ker}(R(M))$. En réécrivant M dans une base adaptée à cette décomposition, on a $M \sim \begin{pmatrix} M_Q & 0 \\ 0 & M_R \end{pmatrix}$, avec $\chi_{M_Q} = Q$ et $\chi_{M_R} = R$.

En posant

$$\tilde{M} = P^{-1} \begin{pmatrix} -M_Q & 0 \\ 0 & M_R \end{pmatrix} P,$$

on a le résultat.

- On a déjà que si l'on note C l'ensemble des carrés, alors $\exp(M_n(\mathbf{R})) \subset C$. En effet, pour tout $M \in M_n(\mathbf{R})$, $\exp(M) = \exp\left(\frac{M}{2}\right)^2$.

- Montrer que $C \subset \exp(M_n(\mathbf{R}))$

Soit à présent $M = A^2 \in C$ avec $A \in GL_n(\mathbf{R})$. Par le lemme, on peut supposer que A est à valeurs propres positives.

On note $A = D + N$ la décomposition de Dunford de A dans $\mathbf{C}$. On préférera ici l'écriture $A = UD$ avec $U = ND^{-1} + \text{Id}_n$ une matrice unipotente qui commute avec D . On admet (je l'ai mis dans le plan) qu'il existe $Q \in \mathbf{R}[X]$ tel que $\exp(Q(U)) = U$. De plus, on dispose d'une matrice inversible P telle que

$$D = P \text{diag}(\lambda_1, \lambda, \lambda_r, \mu_1, \overline{\mu_1}, \dots, \mu_s, \overline{\mu_s}) P^{-1}$$

avec les λ_i positifs. On pose, pour $i \in \llbracket 1, r \rrbracket$, $\alpha_i = \ln(\lambda_i)$ et pour $i \in \llbracket 1, s \rrbracket$, $\beta_i \in \mathbf{C}$ tel que $\exp(\beta_i) = \mu_i$. Posons enfin L le polynôme interpolateur de Lagrange tel que

$$\begin{cases} \forall i \in \llbracket 1, r \rrbracket, & L(\lambda_i) = \alpha_i, \\ \forall i \in \llbracket 1, s \rrbracket, & L(\mu_i) = \beta_i, \text{ et } L(\overline{\mu_i}) = \overline{\beta_i}. \end{cases}$$

On a alors que pour tout $i \in \llbracket 1, r \rrbracket$, $\overline{L}(\lambda_i) = L(\lambda_i)$ et pour tout $i \in \llbracket 1, s \rrbracket$, $\overline{L}(\mu_i) = L(\mu_i)$ donc par unicité du polynôme interpolateur, $L = \overline{L}$ et donc $L \in \mathbf{R}[X]$. On a donc que $D = \exp(L(D))$ et donc

$$A = \exp(L(D) + Q(U))$$

comme on a bien que les deux matrices commutent. Donc A est dans l'image de l'exponentielle, c'est donc aussi le cas de M . □

Démonstration — Preuve de la variante)

- De façon évidente, l'exponentielle de toute matrice est inversible.

On va montrer que toute matrice $M \in GL_n(\mathbf{C})$ s'écrit comme $M = \exp(P(M))$ avec P un polynôme.

- Cas M diagonalisable

$M = QDQ^{-1}$. Par surjectivité de l'exponentielle complexe, pour tout λ_i , il existe μ_i tel que $\exp(\mu_i) = \lambda_i$. On pose P le polynôme interpolateur de Lagrange qui à λ_i associe μ_i . Alors $D = \exp(P(D))$ et par continuité de la conjugaison, $M = \exp(P(M))$.

- Cas M unipotente

On pose $N = \sum_{i=0}^n (-1)^{i-1} \frac{M^i}{i}$ qui est nilpotente. On a bien $\exp(N) = M$ et N est un polynôme en M .

- Cas général

On considère la décomposition de Dunford de M : $M = DU$ avec D diagonalisable et U unipotente, qui commutent et qui sont des polynômes en M .

Alors,

$$M = \exp(P(D)) \exp(Q(U)) = \exp(P_1(M)) \exp(Q_1(M)) = \exp((P_1 + P_2)(M)).$$

□

3 Développement alternatif : image de l'exponentielle matricielle

Leçons : 153

Référence: Algèbre et géométrie, Rombaldi

| **Théorème** — $\exp : N_n(\mathbf{C}) \rightarrow U_n(\mathbf{C})$ réalise une bijection de réciproque $\log$.

| **Corollaire** —

1. $\exp(M_n(\mathbf{R})) = \{A^2 \mid A \in GL_n(\mathbf{R})\}$.
2. $\exp(M_n(\mathbf{C})) = GL_n(\mathbf{C})$.

Démonstration — Preuve du théorème

- Soit $A \in N_n(\mathbf{C})$ d'indice de nilpotence q . Alors $e^{\log(I_n + A)} = I_n + A$

On désigne par φ la fonction définie sur $\mathbf{R}$ par $\varphi(t) = \sum_{k=1}^q \frac{(-1)^{k-1}}{k} t^k A^k$. φ est polynômiale donc dérivable, et

$$\varphi'(t) = \sum_{k=1}^q (-1)^{k-1} t^{k-1} A^k = A \left(\sum_{k=0}^{q-1} (-1)^k t^k A^k \right) = A(I_n + tA)^{-1}$$

Posons à présent $\psi = \exp \circ \varphi$. ψ est dérivable et $\psi'(t) = \varphi'(t)\psi(t)$, i.e $(I_n + tA)\psi'(t) = A\psi(t)$. En dérivant une deuxième fois,

$$A\psi'(t) + (I_n + tA)\psi''(t) = A\psi'(t)$$

et comme $I_n + tA$ est inversible, $\psi'' = 0$. Comme $\psi'(0) = A$ et $\psi(0) = I_n$, on a $\exp(\log(I_n + tA)) = I_n + tA$.

- Pour toute matrice $A \in N_n(\mathbf{C})$, $\exp(A) \in U_n(\mathbf{C})$ et $\log(e^{tA}) = tA$.

$\exp(A) = I_n + \sum_{k=1}^q \frac{A^k}{k!}$ est bien unipotente. Notons $\exp(tA) = I_n + V(t)$. La fonction V est dérivable donc $\varphi = \log(I_n + V(t)) - tA$ l'est aussi et

$$\varphi'(t) = V'(t) \sum_{k=0}^{q-1} (-1)^k V(t)^k - A = V'(t)(I_n + V(t))^{-1} - A = V'(t)e^{-tA} - A.$$

Or, $V(t) = e^{tA} - I_n$ donc $V'(t) = Ae^{tA}$ et $\varphi' = 0$. Comme $\varphi(0) = 0$, on a le résultat.

- Conclusion

Le premier point donne la surjectivité, le second l'injectivité.

□

Démonstration — Preuve du corollaire

- Si $M \in M_n(\mathbf{R})$, il existe $\tilde{M}$ de valeurs propres toutes positives et telle que $M^2 = \tilde{M}^2$.

Posons $Q = \prod_{\lambda \in sp(M) \cap \mathbf{R}^+} (X - \lambda)$ et $R = \prod_{\lambda \in sp(M) \cap (\mathbf{C} \setminus \mathbf{R}^+)} (X - \lambda)$.

Les polynômes Q et R sont réels et premiers entre eux par construction, et $\chi_M = QR$. Par le théorème de Cayley-Hamilton, on a donc que $Q(M)R(M) = 0$, et par le lemme des noyaux, $E = \text{Ker}(Q(M)) \oplus \text{Ker}(R(M))$. En réécrivant M dans une base adaptée à cette décomposition, on a $M \sim \begin{pmatrix} M_Q & 0 \\ 0 & M_R \end{pmatrix}$, avec $\chi_{M_Q} = Q$ et $\chi_{M_R} = R$. En posant

$$\tilde{M} = P^{-1} \begin{pmatrix} -M_Q & 0 \\ 0 & M_R \end{pmatrix} P,$$

on a le résultat.

- On a déjà que si l'on note C l'ensemble des carrés, alors $\exp(M_n(\mathbf{R})) \subset C$. En effet, pour tout $M \in M_n(\mathbf{R})$, $\exp(M) = \exp\left(\frac{M}{2}\right)^2$.

- Montrer que $C \subset \exp(M_n(\mathbf{R}))$

Soit à présent $M = A^2 \in C$ avec $A \in GL_n(\mathbf{R})$. Par le lemme, on peut supposer que A est à valeurs propres positives.

On note $A = D + N$ la décomposition de Dunford de A dans $\mathbf{C}$. On préférera ici l'écriture $A = UD$ avec $U = ND^{-1} + \text{Id}_n$ une matrice unipotente qui commute avec D . On admet (je l'ai mis dans le plan) qu'il existe $Q \in \mathbf{R}[X]$ tel que $\exp(Q(U)) = U$. De plus, on dispose d'une matrice inversible P telle que

$$D = P \text{diag}(\lambda_1, \lambda, \lambda_r, \mu_1, \overline{\mu_1}, \dots, \mu_s, \overline{\mu_s}) P^{-1}$$

avec les λ_i positifs. On pose, pour $i \in \llbracket 1, r \rrbracket$, $\alpha_i = \ln(\lambda_i)$ et pour $i \in \llbracket 1, s \rrbracket$, $\beta_i \in \mathbf{C}$ tel que $\exp(\beta_i) = \mu_i$. Posons enfin L le polynôme interpolateur de Lagrange tel que

$$\begin{cases} \forall i \in \llbracket 1, r \rrbracket, & L(\lambda_i) = \alpha_i, \\ \forall i \in \llbracket 1, s \rrbracket, & L(\mu_i) = \beta_i, \text{ et } L(\overline{\mu_i}) = \overline{\beta_i}. \end{cases}$$

On a alors que pour tout $i \in \llbracket 1, r \rrbracket$, $\overline{L}(\lambda_i) = L(\lambda_i)$ et pour tout $i \in \llbracket 1, s \rrbracket$, $\overline{L}(\mu_i) = L(\mu_i)$ donc par unicité du polynôme interpolateur, $L = \overline{L}$ et donc $L \in \mathbf{R}[X]$. On a donc que $D = \exp(L(D))$ et donc

$$A = \exp(L(D) + Q(U))$$

comme on a bien que les deux matrices commutent. Donc A est dans l'image de l'exponentielle, c'est donc aussi le cas de M .

Preuve dans le cas complexe

- De façon évidente, l'exponentielle de toute matrice est inversible.

On va montrer que toute matrice $M \in GL_n(\mathbf{C})$ s'écrit comme $M = \exp(P(M))$ avec P un polynôme.

- Cas M diagonalisable

$M = QDQ^{-1}$. Par surjectivité de l'exponentielle complexe, pour tout λ_i , il existe μ_i tel que $\exp(\mu_i) = \lambda_i$. On pose P le polynôme interpolateur de Lagrange qui à λ_i associe μ_i . Alors $D = \exp(P(D))$ et par continuité de la conjugaison, $M = \exp(P(M))$.

- Cas M unipotente

On pose $N = \sum_{i=0}^n (-1)^{i-1} \frac{M^i}{i}$ qui est nilpotente. On a bien $\exp(N) = M$ et N est un polynôme en M .

- Cas général

On considère la décomposition de Dunford de M : $M = DU$ avec D diagonalisable et U unipotente, qui commutent et qui sont des polynômes en M .

Alors,

$$M = \exp(P(D)) \exp(Q(U)) = \exp(P_1(M)) \exp(Q_1(M)) = \exp((P_1 + P_2)(M)).$$

□

4 Corps des nombres algébriques

Leçons : 125, 141, 144, 151

Référence: Algèbre, Gourdon

Soient K et L deux corps avec L/K .

Proposition — $a \in L$ est algébrique sur K si et seulement si $K[a]$ est de dimension finie si et seulement si $K[a] = K(a)$.

Proposition — L l'ensemble A des nombres algébriques sur K est un corps. De plus, si L est algébriquement clos, alors A est une clôture algébrique de K . Enfin, A est dénombrable.

Démonstration — Preuve de la première proposition

Notons $\varphi_a : K[X] \rightarrow K[a]$ le morphisme évaluation en a .

- (1) $\Leftrightarrow$ (2)

On suppose que a est algébrique. $I_a = \text{Ker}(\varphi_a)$ est un idéal de l'anneau principal $K[X]$, donc il existe un unique polynôme $P \in K[X]$ unitaire tel que $I_a = \langle P \rangle$. P est irréductible dans $K[X]$, en effet si $P = QR$ alors $Q(a) = 0$ ou $R(a) = 0$ donc R ou Q est élément de $I_a = \langle P \rangle$ donc son degré est supérieur ou égal à celui de P , et donc il est égal à P à constante inversible près. Donc, $\text{Im}(\varphi) = K[a]$ est isomorphe à $K[X]/\langle P \rangle$. Comme P est irréductible, c'est un corps de dimension $\deg(P)$ en tant que K -espace vectoriel.

Supposons par contraposée que a est transcendant. Alors, φ_a est un isomorphisme et $K(T) \simeq K(a)$ et on a bien que les deux sont distincts.

- (1) $\Leftrightarrow$ (3)

Le sens direct résulte de l'isomorphisme $K[a] \simeq K[X]/(\mu_a)$.

Si $K[a]$ est un espace vectoriel de dimension finie n , alors $(1, a, \dots, a^n)$ est une famille liée et on a un polynôme annulateur.

□

Démonstration — Preuve de la deuxième proposition

- A est un corps

On a bien $0 \in A$. Soient donc x et y des éléments de A .

On a $K(x - y) \subset K(x, y)$ et comme $[K(x, y) : K] = [K(x, y) : K(x)][K(x) : K] < +\infty$, on a $[K(x - y) : K] < +\infty$ et $x - y$ est algébrique sur K .

De plus, si $y \neq 0$, comme $K(xy^{-1}) \subset K(x, y)$, $xy^{-1} \in A$. Donc A est un corps.

- A est dénombrable

Notons $E_{k,n} = \{P = \sum_j \lambda_j X^j \mid \deg(P) = k, \max |\lambda_j| = n\}$. On obtient alors que

$$A = \bigcup_{k \geq 1} \bigcup_{n \geq 1} \text{Zeros}(E_{k,n})$$

est dénombrable comme union dénombrable d'ensembles finis.

- Si L est algébriquement clos alors A est une clôture algébrique de K .

Soit $P = \sum_{k=0}^n a_k X^k \in A[X]$ avec $n \geq 1$. On a $P \in L[X]$ avec L algébriquement clos, donc il existe $\alpha \in L$ tel que $P(\alpha) = 0$. On a alors que α est algébrique sur $K(a_0, \dots, a_n)$, donc $[K(a_0, \dots, a_n, \alpha) : K(a_0, \dots, a_n)] < \infty$.

Or, comme $a_0, \dots, a_n \in A$, $[K(a_0, \dots, a_n) : K] < +\infty$, donc α est algébrique sur K car $K[\alpha] \subset K(\alpha) \subset K(a_0, \dots, a_n, \alpha)$ est bien de dimension finie sur K . Donc P admet une racine dans A . Donc A est algébriquement clos.

□

5 Loi de réciprocité quadratique

Leçons : 121, 123, 125

Référence: Un max de maths, Zavidovique

Proposition — Soient p et l deux nombres premiers impairs distincts. Alors

$$\left(\frac{p}{l}\right) \left(\frac{l}{p}\right) = (-1)^{\frac{(p-1)(l-1)}{4}}.$$

Théorème — Une équation diophantienne de la forme $x^2 + py = q$ avec p premier et $q \wedge p = 1$ admet une solution ssi $\left(\frac{q}{p}\right) = 1$. Dans ce cas, si on a une solution (x_0, y_0) , l'ensemble des solutions est $S = \left\{ \left(x, y_0 + \frac{x^2 - x_0^2}{p} \right) \mid x \equiv \pm x_0 [p] \right\}$.

Application — L'équation $x^2 + 31y = 21$ n'admet aucune solution.

- On commence par montrer que $x \in (\mathbf{Z}/p\mathbf{Z})^*$ est un carré dans $\mathbf{Z}/p\mathbf{Z}$ si et seulement si $x^{\frac{p-1}{2}} = 1$.

Posons $\varphi : (\mathbf{Z}/p\mathbf{Z})^* \rightarrow (\mathbf{Z}/p\mathbf{Z})^*; x \mapsto x^2$. Le noyau de φ est l'ensemble des classes x telles que $x^2 - 1 = (x-1)(x+1) = 0$ donc comme $\mathbf{Z}/p\mathbf{Z}$ est un corps, $\text{Ker}(\varphi) = \{\pm 1\}$. On en déduit que son image $\text{Im}(\varphi)$ est un sous-groupe de $(\mathbf{Z}/p\mathbf{Z})^*$ de cardinal $\frac{p-1}{2}$. Par le théorème de Lagrange, tout élément $x \in \text{Im}(\varphi)$ vérifie donc $x^{\frac{p-1}{2}} = 1$.

Comme $\mathbf{Z}/p\mathbf{Z}$ est un corps commutatif, le polynôme $X^{\frac{p-1}{2}}$ admet au plus $\frac{p-1}{2}$ racines. Il en admet donc exactement ce nombre car $\text{Im}(\varphi)$ est l'ensemble de ses racines. Il y a donc équivalence entre " x est un carré" et " $x^{\frac{p-1}{2}} = 1$ ".

Soit Ω une clôture algébrique de $\mathbf{Z}/p\mathbf{Z}$ et soit $w \in \Omega$ une racine l -ième de l'unité différente de 1. Posons enfin $y = \sum_{x \in \mathbf{Z}/l\mathbf{Z}} \left(\frac{x}{l}\right) w^x$.

Cette somme a bien un sens. En effet, comme w est une racine l -ième de l'unité, $w^l = 1$ et donc la valeur d'une puissance w^k de w ne dépend que de la classe de congruence de k modulo l .

- Montrer que $(-1)^{\frac{l-1}{2}} y^2 = l$.

On calcule que $y^2 = \sum_{x,z \in \mathbf{Z}/l\mathbf{Z}} \left(\frac{xz}{l}\right) w^{x+z} = \sum_{u \in \mathbf{Z}/l\mathbf{Z}} w^u \left(\sum_{t \in \mathbf{Z}/l\mathbf{Z}} \left(\frac{t(u-t)}{l}\right) \right)$.

Or, si $t \neq 0$, on a

$$\left(\frac{t(u-t)}{l}\right) = \left(\frac{-1}{l}\right) \left(\frac{t^2}{l}\right) \left(\frac{1-ut^{-1}}{l}\right) = (-1)^{\frac{l-1}{2}} \left(\frac{1-ut^{-1}}{l}\right).$$

En posant $C_u = \sum_{t \in (\mathbf{Z}/l\mathbf{Z})^*} \left(\frac{1-ut^{-1}}{l}\right)$, on obtient que

$$(-1)^{\frac{l-1}{2}} y^2 = \sum_{u \in \mathbf{Z}/l\mathbf{Z}} C_u w^u.$$

Pour $u = 0$, on a $C_0 = l - 1$. Pour $u \neq 0$, la quantité $s = 1 - ut^{-1}$ décrit l'ensemble $\mathbf{Z}/l\mathbf{Z} \setminus \{1\}$, et donc

$C_u = \left[\sum_{s \in (\mathbf{Z}/l\mathbf{Z})^*} \left(\frac{s}{l}\right) \right] - \left(\frac{1}{l}\right) = -1$ car il y a autant de carrés que de non carrés dans $(\mathbf{Z}/l\mathbf{Z})^*$ (remarquer que on

passse de $\mathbf{Z}/l\mathbf{Z} \setminus \{1\}$ à $(\mathbf{Z}/l\mathbf{Z})^* \setminus \{1\}$ en remarquant que $\left(\frac{0}{l}\right) = 0$).

- Montrer d'autre part que $y^{p-1} = \left(\frac{p}{l}\right)$.

Comme Ω est de caractéristique p , l'application $x \mapsto x^p$ est un morphisme de corps appelé morphisme de Frobenius. Donc, par le calcul,

$$\begin{aligned}
 y^p &= \sum_{x \in \mathbf{Z}/l\mathbf{Z}} \left(\frac{x}{l}\right) \omega^{px}, \\
 &= \sum_{x \in \mathbf{Z}/l\mathbf{Z}} \left(\frac{xp^{-1}}{l}\right) \omega^x, \\
 &= \left(\frac{p^{-1}}{l}\right) \sum_{x \in \mathbf{Z}/l\mathbf{Z}} \left(\frac{x}{l}\right) \omega^x, \\
 &= \left(\frac{p^{-1}}{l}\right) y, \\
 &= \left(\frac{p}{l}\right) y.
 \end{aligned}$$

Comme y est non nul,

$$y^{p-1} = \left(\frac{p}{l}\right).$$

- Conclure.

Par le point précédent, on a que

$$\left(\frac{(-1)^{\frac{l-1}{2}} l}{p}\right) = (y^2)^{\frac{p-1}{2}} = \left(\frac{p}{l}\right).$$

Par le premier point, $\left(\frac{(-1)^{\frac{l-1}{2}}}{p}\right) = ((-1)^{\frac{l-1}{2}})^{\frac{p-1}{2}} = (-1)^{\frac{(p-1)(l-1)}{4}}$, et donc puisque

$$\left(\frac{(-1)^{\frac{l-1}{2}}}{p}\right) = \left(\frac{(-1)^{\frac{l-1}{2}}}{p}\right) \left(\frac{l^2}{p}\right) = \left(\frac{(-1)^{\frac{l-1}{2}} l}{p}\right) \left(\frac{l}{p}\right) = \left(\frac{p}{l}\right) \left(\frac{l}{p}\right),$$

on conclut que

$$\left(\frac{p}{l}\right) \left(\frac{l}{p}\right) = (-1)^{\frac{(p-1)(l-1)}{4}}.$$

- Preuve du théorème

$x^2 + py = q$ a une solution (x, y) ssi $q \equiv x^2[p]$ ssi $\left(\frac{q}{p}\right) = 1$.

- Preuve de l'application

$\left(\frac{21}{31}\right) = \left(\frac{3}{31}\right) \left(\frac{7}{31}\right)$ car le symbole de Legendre est un morphisme pour le groupe multiplicatif $(\mathbf{Z}/31\mathbf{Z})^*$. Par la loi de réciprocité quadratique,

$$\begin{aligned}
 \left(\frac{21}{31}\right) &= (-1)^{\frac{2 \times 30}{4}} (-1)^{\frac{6 \times 30}{4}} \left(\frac{31}{3}\right) \left(\frac{31}{7}\right), \\
 &= \left(\frac{1}{3}\right) \left(\frac{3}{7}\right), \\
 &= -1
 \end{aligned}$$

6 Déterminant de Gram et inégalité d'Hadamard

Leçons : 152

Référence: Algèbre, Gourdon

Soit $(E, \langle \cdot, \cdot \rangle)$ un espace préhilbertien (réel ou complexe).

Théorème — Soit F un sous-espace vectoriel de E de dimension finie n muni d'une base $(e_1, \dots, e_n)$. Alors pour tout $x \in E$,

$$d(x, F)^2 = \frac{G(e_1, \dots, e_n, x)}{G(e_1, \dots, e_n)}.$$

Théorème — (Inégalité d'Hadamard)

1. Soient $x_1, \dots, x_n$ des vecteurs de E . Alors $G(x_1, \dots, x_n) \leq \prod_{i=1}^n \|x_i\|^2$.

2. Soient $x_1, \dots, x_n$ des vecteurs de $\mathbf{C}^n$. Alors $|\det(x_1, \dots, x_n)| \leq \prod_{i=1}^n \|x_i\|_2$.

Dans les deux points, on a égalité ssi la famille est orthogonale ou si l'un des vecteurs est nul.

• Première remarque sur le déterminant de Gram

Si la famille $(x_1, \dots, x_n)$ est liée, alors par linéarité du produit scalaire, les colonnes de la matrice de Gram sont liées et le déterminant de Gram est nul.

Réciproquement, si le déterminant de Gram est nul alors les colonnes sont liées donc pour tout $i \in \llbracket 1, n \rrbracket$, $\sum_{j=1}^n \lambda_j \langle x_i, x_j \rangle = 0$ avec $(\lambda_1, \dots, \lambda_n)$ non tous nuls. Quitte à diviser par un des coefficients non nuls, il existe $k \in \llbracket 1, n \rrbracket$ tel que

$$\forall i \in \llbracket 1, n \rrbracket, \langle x_i, x_k \rangle = \sum_{l \neq k} \langle x_i, x_l \rangle = \left\langle e_i, \sum_{l \neq k} \bar{\lambda}_l x_l \right\rangle.$$

Donc $x_k - \sum_{l \neq k} \bar{\lambda}_l x_l \in \text{Vect}(x_1, \dots, x_n)^\perp \cap \text{Vect}(x_1, \dots, x_n) = \{0\}$. La famille est donc liée.

• Preuve du premier théorème

Comme F est de dimension finie, on a que $d(x, F)$ est atteint en la projection $\pi_F(x)$ de x . On a $d(x, F) = \|x - \pi_F(x)\|$. Par définition de la projection orthogonale, pour tout $i \in \llbracket 1, n \rrbracket$,

$$\langle x, e_i \rangle = \langle \pi_F(x), e_i \rangle \text{ et } \|x\|^2 = \|\pi_F(x)\|^2 + \|x - \pi_F(x)\|^2.$$

On écrit ensuite

$$M_G(e_1, \dots, e_n, x) = \begin{pmatrix} & & \langle e_1, x \rangle \\ & M_G(e_1, \dots, e_n) & \vdots \\ \langle x, e_1 \rangle & \dots & \langle x, e_n \rangle \\ & & \|x\|^2 \end{pmatrix}.$$

Par linéarité du déterminant par rapport à la dernière colonne,

$$\begin{aligned} G(e_1, \dots, e_n, x) &= \begin{vmatrix} & & \langle e_1, \pi_F(x) \rangle \\ & M_G(e_1, \dots, e_n) & \vdots \\ \langle \pi_F(x), e_1 \rangle & \dots & \langle \pi_F(x), e_n \rangle \\ & & \|\pi_F(x)\|^2 \end{vmatrix} \\ &+ \begin{vmatrix} & & 0 \\ & M_G(e_1, \dots, e_n) & \vdots \\ \langle \pi_F(x), e_1 \rangle & \dots & \langle \pi_F(x), e_n \rangle \\ & & 0 \end{vmatrix}, \\ &= G(e_1, \dots, e_n, \pi_F(x)) + \|x - \pi_F(x)\|^2 G(e_1, \dots, e_n), \\ &= d(x, F)^2 G(e_1, \dots, e_n) \end{aligned}$$

car $\pi_F(x) \in \text{Vect}(e_1, \dots, e_n)$.

Démonstration — Preuve du second théorème

- Preuve du premier point

C'est vrai si la famille est liée par la remarque préliminaire.

On montre ensuite la relation sur les familles libres par récurrence sur $n \in \mathbf{N}^*$.

- Si $n = 1$, $G(x_1) = \|x_1\|^2$.
- Supposons la propriété vraie au rang n . Soient $x_1, \dots, x_{n+1}$ des vecteurs libres de E . Notons $F = \text{Vect}(x_1, \dots, x_n)$ et considérons $\pi_F(x_{n+1})$ la projection orthogonale de x_{n+1} sur F . Alors, par le premier théorème,

$$G(x_1, \dots, x_{n+1}) = G(x_1, \dots, x_n) \|x_{n+1} - \pi_F(x_{n+1})\|^2.$$

Par l'hypothèse de récurrence, on a donc que

$$G(x_1, \dots, x_{n+1}) \leq \prod_{i=1}^n \|x_i\|^2 \times \|x_{n+1} - \pi_F(x_{n+1})\|^2 \leq \prod_{i=1}^n \|x_i\|^2 \times \|x_{n+1}\|^2.$$

On a de plus égalité ssi la famille $(x_1, \dots, x_n)$ est orthogonale (par hypothèse de récurrence) et que $\|x_{n+1} - \pi_F(x_{n+1})\|^2 = \|x_{n+1}\|^2$, i.e $\pi_F(x_{n+1}) = 0$. D'où l'hérédité.

- Preuve du second point

Si on note A la matrice des vecteurs colonnes de $(x_1, \dots, x_n)$ dans la base canonique, alors $M_G(x_1, \dots, x_n) = {}^t \overline{A} A$. On applique alors le point précédent car $G(x_1, \dots, x_n) = |\det(M)|^2$.

□

7 $SO_3(\mathbf{R})$ et les quaternions

à reformuler en termes d'actions de groupes

Leçons : 161

Référence: Cours d'algèbre, Perrin

| **Théorème** —

$$SO_3(\mathbf{R}) \simeq G/\{\pm 1\}.$$

| **Corollaire** —

$$SO_3(\mathbf{R}) \simeq SU_2(\mathbf{C})/\{\text{Id}, -\text{Id}\}.$$

On pose, pour $q \in G$ et tout $q' \in \mathbf{H}$, $S_q(q') = qq'q^{-1} = qq'\bar{q}$.

- Étude de S_q pour $q \in G$.

Soit $q \in G$.

S_q est $\mathbf{R}$ -linéaire, bijective de réciproque $S_{\bar{q}}$. Elle conserve également la norme N naturelle sur les quaternions. En effet, pour tout $q' \in \mathbf{H}$,

$$N(S_q(q')) = N(Q)N(q')N(\bar{q}) = N(q')$$

car $q \in G$. On a donc $S_q \in O(N) \simeq O_4(\mathbf{R})$.

De plus, comme $\mathbf{R} = Z(\mathbf{H})$, $S_{q|\mathbf{R}} = \text{Id}_{\mathbf{R}}$ et donc comme P l'espace des quaternions purs est orthogonal à $\mathbf{R}$ pour le produit scalaire associé à N , on a P qui est stable par S_q et on peut donc définir pour tout q l'application $s_q = S_{q|_P}$ que l'on peut voir comme un élément de $O_3(\mathbf{R})$.

- Étude de $s : q \in G \mapsto s_q$.

Remarquons tout d'abord que $S : G \rightarrow O(N); q \mapsto S_q$ est un morphisme de groupes pour la multiplication, de noyau $Z(\mathbf{H}) \cap G = \{\pm 1\}$. Le noyau de s est donc aussi ± 1 .

s est continue. En effet, si l'on écrit $q = a + bi + cj + dk$, les coefficients de la matrice de s_q dans la base (i, j, k) de P sont des polynômes homogènes de degré 2 en a, b, c, d . Par exemple, si l'on note M cette matrice, $m_{1,1} = a^2 + b^2 - c^2 - d^2$. On en déduit que $\det \circ s : G \rightarrow \det(O_3(\mathbf{R})) = \{\pm 1\}$ est continue, et comme G est connexe (il est isomorphe à $\mathbf{S}^3$), on a $\det \circ s = \{1\}$ car $s(1) = \text{Id}$. Ainsi a-t-on montré que s est à valeurs dans $SO_3(\mathbf{R})$.

Soit $p \in P \cap G$. On a $s_p(p) = p$ donc p est un point fixe de s_p . $s_p \in SO_3(\mathbf{R})$ est donc une rotation d'axe $\langle p \rangle$. De plus, comme $p \in P \cap G$, on a $p^2 = -p\bar{p} = -1$ et $s_p^2 = s_{p^2} = s_{-1} = \text{Id}$ et s_p est une involution. Donc, s_p est le retournement d'axe $\langle p \rangle$. Tous les retournements de $SO_3(\mathbf{R})$ sont donc dans l'image de s . Comme ces derniers engendrent $SO_3(\mathbf{R})$, et que s est un morphisme, $s(G) = SO_3(\mathbf{R})$.

En passant au quotient, on obtient donc que $\bar{s} : G/\{\pm 1\} \rightarrow SO_3(\mathbf{R})$ est un isomorphisme.

- Preuve du corollaire

$\mathbf{H}$ a une structure de $\mathbf{C}$ -espace vectoriel pour la loi externe $(\lambda, q) \mapsto q\lambda$. Cet espace vectoriel est de dimension 2 et une base de cet espace est $(1, j) : a + bi + cj + dk = 1(a + bi) + j(c - di)$.

On fait alors opérer G par multiplication à gauche :

$$T_q(q') = qq', \quad q \in G, q' \in \mathbf{H}.$$

Pour tout $q \in G$, T_q est $\mathbf{C}$ -linéaire et inversible d'inverse $T_{\bar{q}}$ donc $T_q \in GL_2(\mathbf{C})$. On a donc un morphisme $T : G \rightarrow GL_2(\mathbf{C}) : q \mapsto T_q$. Ce morphisme est injectif de façon assez évidente.

Posons $q = \lambda 1 + \mu j \in G$, i.e $\lambda\bar{\lambda} + \mu\bar{\mu} = 1$. On vérifie que

$$\text{Mat}_{(1,j)}(T_q) = \begin{pmatrix} \lambda & -\bar{\mu} \\ \mu & \bar{\lambda} \end{pmatrix},$$

autrement dit pour tout $q \in G$, $T_q \in SU_2(\mathbf{C})$. De plus, l'écriture matricielle permet de voir que $T : G \rightarrow SU_2(\mathbf{C})$ est surjective donc est un isomorphisme.

Il vient donc que l'on a un isomorphisme

$$\mathrm{SO}_3(\mathbf{R}) \rightarrow \mathrm{SU}_2(\mathbf{C})/\{\mathrm{Id}, -\mathrm{Id}\}.$$

8 Compacité dans un espace de Banach

Leçons : 203,205,208

Référence: Analyse pour l'agrégation, Bernis

Théorème — Soit $(E, \|\cdot\|)$ un espace de Banach. Soit K une partie de E . Alors, K est compact si et seulement s'il est fermé, borné et plat.

Application au sens difficile du théorème d'Ascoli

- Sens direct

Supposons K compact. On a en particulier que K est fermé et borné, reste à montrer qu'il est plat.

Soit $\varepsilon \in \mathbf{R}_+^*$. Par précompacité de K , on dispose de $N_\varepsilon \in \mathbf{N}$ et de $(x_1, \dots, x_{N_\varepsilon}) \in E^{N_\varepsilon}$ tels que

$$K \subset \bigcup_{i=1}^{N_\varepsilon} B(x_i, \varepsilon).$$

Posons $F = \text{Vect}(x_1, \dots, x_{N_\varepsilon})$. C'est un espace vectoriel de dimension finie inférieure ou égale à N_ε , et on a bien $K \subset F_\varepsilon = F + B(0, \varepsilon)$. Donc K est plat.

- Sens indirect

Quitte à dilater notre ensemble, on suppose $K \subset \overline{B_E(0, 1)}$. Comme K est fermé inclus dans un espace de Banach, il est complet. Il reste donc à montrer qu'il est précompact.

Soit $\varepsilon \in \mathbf{R}_+^*$. Comme K est plat, on dispose d'un sous-espace vectoriel F de E de dimension finie tel que $K \subset F_\varepsilon = F + B_E(0, \varepsilon)$. Comme F est de dimension finie, le théorème de Riesz nous dit que $\overline{B_F(0, 1)}$ est compacte, donc il existe $N_\varepsilon \in \mathbf{N}$ et $(y_1, \dots, y_{N_\varepsilon}) \in F^{N_\varepsilon}$ tels que

$$\overline{B_F(0, 1)} \subset \bigcap_{i=1}^{N_\varepsilon} B_F(y_i, \varepsilon).$$

Soit $x \in K$. Comme K est plat, il existe $y \in F$ distant de x de moins de ε : $\|x - y\| < \varepsilon$. On en déduit que $\|y\| \leq 1 + \varepsilon$.

Comme $\frac{y}{1 + \varepsilon} \in B_F(0, 1)$, on dispose d'un indice $i_0 \in \llbracket 1, N_\varepsilon \rrbracket$ tel que $\frac{y}{1 + \varepsilon} \in B_F(y_{i_0}, \varepsilon)$. Par inégalité triangulaire, on obtient alors que

$$\begin{aligned} \|x - y_{i_0}\| &\leq \|x - y\| + \left\| y - \frac{y}{1 + \varepsilon} \right\| + \left\| \frac{y}{1 + \varepsilon} - y_{i_0} \right\|, \\ &\leq \varepsilon + (1 + \varepsilon) \left(1 - \frac{1}{1 + \varepsilon} \right) + \varepsilon, \\ &\leq 3\varepsilon. \end{aligned}$$

On obtient finalement que

$$K \subset \bigcap_{i=1}^{N_\varepsilon} B(y_i, 3\varepsilon),$$

donc K est précompact. D'où le résultat.

- Application au théorème d'Ascoli

On suppose que $\mathcal{A}$ est une partie fermée, bornée et équicontinue de l'espace des fonctions $\mathcal{C}^0(K, \mathbf{R})$ avec K un compact. **vérifier si c'est bien à valeurs dans $\mathbf{R}$** . On va montrer que $\mathcal{A}$ est compact, et pour cela il nous suffit de montrer, par le théorème précédent, qu'il est plat.

Soit $\varepsilon \in \mathbf{R}_+^*$. On pose, pour $\delta \in \mathbf{R}_+^*$, $\omega(\delta) = \sup\{|f(x) - f(y)|, f \in \mathcal{A}, d(x, y) \leq \delta\}$. Par le théorème de Heine, $\mathcal{A}$ est uniformément équicontinu et donc $\omega(\delta) \xrightarrow{\delta \rightarrow 0} 0$. En particulier, il existe δ_0 tel que pour tout $\delta \leq \delta_0$, $\omega(\delta) < \varepsilon$.

Par précompacité de K , on dispose de $N = N(\delta_0) \in \mathbf{N}$ et de $(x_1, \dots, x_N) \in K^N$ tels que

$$K \subset \bigcap_{i=1}^N B(x_i, \delta_0).$$

Posons, pour tout $j \in \llbracket 1, N \rrbracket$, $\varphi_j : K \rightarrow \mathbf{R}, x \mapsto \frac{d(x, K \setminus B(x_j, \delta_0))}{\sum_{i=1}^N d(x, K \setminus B(x_i, \delta_0))}$. Ces applications sont bien définies : en effet, comme $x \in K$, il y a forcément une boule dans laquelle il se trouve, donc le dénominateur ne s'annule jamais. De plus, ces applications sont positives, continues car la distance est 1-lipschitzienne, et elles sont nulles en-dehors de la boule $B(x_j, \delta_0)$. Enfin, pour tout $x \in K$, $\sum_{j=1}^N \varphi_j(x) = 1$.

Posons $L : \mathcal{C}^0(K, \mathbf{R}) \rightarrow \mathcal{C}^0(K, \mathbf{R}); f \mapsto \sum_{j=1}^N f(x_j) \varphi_j$. L est linéaire, de norme inférieure à 1 donc continue. Soient $f \in \mathcal{A}$ et $x \in K$. On a

$$\begin{aligned} |f(x) - L(f)(x)| &\leq \sum_{j=1}^N |f(x) - f(x_j)| \varphi_j(x), \\ &\leq \omega(\delta_0) \sum_{j=1}^N \varphi_j(x), \\ &\leq \omega(\delta_0), \\ &\leq \varepsilon. \end{aligned}$$

Ainsi, $\|f - L(f)\|_\infty \leq \varepsilon$ donc $\mathcal{A} \subset \text{Im}(L) + B(0, \varepsilon)$ et $\text{rg}(L) < +\infty$ donc $\mathcal{A}$ est plat.

9 Convergence des méthodes itératives et caractérisation du rayon spectral

Leçons : 149, 162

Référence: Algèbre et géométrie, Rombaldi

Théorème — Soit $A \in M_n(\mathbf{C})$. On a équivalence entre :

1. $\lim_{k \rightarrow +\infty} A^k = 0$,
2. $\forall x_0 \in \mathbf{C}^n$, la suite $(x_k)_{k \in \mathbf{N}}$ définie par $x_{k+1} = Ax_k$ converge vers 0,
3. $\rho(A) < 1$,
4. Il existe au moins une norme matricielle subordonnée telle que $\|A\| < 1$,
5. La matrice $I_n - A$ est inversible et la série de terme général A^k est convergente de somme $(I_n - A)^{-1}$,
6. La matrice $I_n - A$ est inversible et la série de terme général $\text{Tr}(A^k)$ converge de somme $\text{Tr}((I_n - A)^{-1})$,
7. $\lim_{k \rightarrow +\infty} \text{Tr}(A^k) = 0$,

Corollaire — Quelle que soit la norme choisie sur $M_n(\mathbf{C})$,

$$\rho(A) = \lim_{k \rightarrow +\infty} \|A^k\|^{\frac{1}{k}}.$$

Corollaire — Une méthode itérative converge si et seulement si $B = M^{-1}N$ vérifie le théorème précédent.

Démonstration — Preuve du théorème

• (1) $\Rightarrow$ (2)

Soit $\|\cdot\|$ une norme quelconque sur $\mathbf{R}^n$, on note de la même manière la norme matricielle subordonnée. Alors pour tout $v \in \mathbf{R}^n$,

$$\|B^k v\| \leq \|B^k\| \|v\| \xrightarrow[k \rightarrow +\infty]{} 0.$$

• (2) $\Rightarrow$ (3)

On raisonne par contraposée : si $\rho(B) \geq 1$, on peut trouver un vecteur p non nul tel que $Bp = \lambda p$ avec $|\lambda| \geq 1$. Donc $B^k p = \lambda^k p$ ne tend pas vers 0. Par contraposée, on a l'implication souhaitée.

• (3) $\Rightarrow$ (4)

Soit $\varepsilon \in \mathbf{R}_+^*$. On va montrer qu'on peut trouver une norme matricielle telle que $\|B\| \leq \rho(B) + \varepsilon$. Notons b l'endomorphisme canoniquement associé à B . En trigonalisant dans $\mathbf{C}$, on obtient une base $\mathcal{B} = (e_1, \dots, e_n)$ dans laquelle b est triangulaire supérieure. On note $b_{i,j}$ les coefficients de cette matrice :

$$\text{Mat}_{\mathcal{B}}(b) = \begin{pmatrix} b_{1,1} & \dots & b_{1,n} \\ 0 & \ddots & \vdots \\ 0 & 0 & b_{n,n} \end{pmatrix}.$$

Posons $\mathcal{B}' = (e'_1, \dots, e'_n) = (e_1, \delta e_2, \dots, \delta^{n-1} e_n)$. Dans cette base,

$$b(e'_j) = \delta^{j-1} \sum_{i=1}^j b_{i,j} e_i = \sum_{i=1}^j \delta^{j-i} b_{i,j} e'_i,$$

autrement dit la k -ième surdiagonale de la matrice est multipliée par δ^k . En prenant δ suffisamment petit (de sorte à avoir $\sum_{j=i+1}^n |\delta j - i b_{i,j}| < \varepsilon \forall i \in \llbracket 1, n \rrbracket$), on a, en posant $\|B\| = \|\text{Mat}_{\mathcal{B}'}(b)\|_{\infty}$, que

$$\|B\| < \rho(B) + \varepsilon.$$

Comme ε est quelconque, on a le résultat.

- (4) $\Rightarrow$ (1).

La norme construite au point précédent étant une norme subordonnée, elle est matricielle donc si on la choisit, $\|B^k\| \leq \|B\|^k$ et on a bien la convergence vers 0.

Conclu partielle : On a l'équivalence entre les quatre premiers items. On va maintenant montrer l'équivalence entre les items 3,5,6 et 7 par implications circulaires.

- (3) $\Rightarrow$ (5)

Si $\rho(A) < 1$, alors 1 n'est pas valeur propre de A donc $I_n - A$ est inversible. Notons, pour tout $p \in \mathbb{N}$,

$$S_p = \sum_{k=0}^p A^k.$$

On a $(I_n - A)S_p = I_n - A^{p+1}$, or $\lim_{p \rightarrow +\infty} I_n - A^{p+1} = I_n$, donc par continuité du produit matriciel,

$$\lim_{p \rightarrow +\infty} S_p = \lim_{p \rightarrow +\infty} (I_n - A)^{-1}(I_n - A^{p+1}) = (I_n - A)^{-1}.$$

- (5) $\Rightarrow$ (6)

Par convergence de la série $\sum_{k \geq 0} A^k$, on a que $A^k \xrightarrow{k \rightarrow +\infty} 0$ donc $\rho(A) < 1$. Notons $\lambda_1, \dots, \lambda_n$ les valeurs propres de A . On a

$$\sum_{k=0}^p \text{Tr}(A^k) = \sum_{k=0}^p \sum_{j=1}^n \lambda_j^k = \sum_{j=1}^n \sum_{k=0}^p \lambda_j^k = \sum_{j=1}^n \frac{1 - \lambda_j^{p+1}}{1 - \lambda_j}.$$

Or, pour tout $j \in \llbracket 1, n \rrbracket$, $|\lambda_j| < 1$, donc comme chaque terme de la somme finie converge, on a convergence de la série et

$$\sum_{k=0}^{\infty} \text{Tr}(A^k) = \sum_{j=1}^n \frac{1}{1 - \lambda_j}.$$

Il reste à remarquer que les $\frac{1}{1 - \lambda_j}$ sont exactement les valeurs propres de $(I_n - A)^{-1}$.

- (6) $\Rightarrow$ (7)

Découle directement de la convergence vers 0 du terme général d'une série convergente.

- (7) $\Rightarrow$ (3)

Supposons par l'absurde que $\rho(A) \geq 1$. Il existe une valeur propre λ_i de module supérieur ou égal à 1. Quitte à renuméroter, on prend $|\lambda_1| = \dots = |\lambda_p| = \rho(A) > |\lambda_j|$, $j \in \llbracket p+1, n \rrbracket$. Alors,

$$\sum_{j=1}^n \left(\frac{\lambda_j}{\rho(A)} \right)^k = \frac{1}{(\rho(A))^k} \text{Tr}(A^k) = \sum_{j=1}^p \left(\frac{\lambda_j}{\rho(A)} \right)^k + \sum_{j=p+1}^n \left(\frac{\lambda_j}{\rho(A)} \right)^k.$$

Alors, en laissant k tendre vers l'infini, on obtient

$$\sum_{j=1}^p \left(\frac{\lambda_j}{\rho(A)} \right)^k \xrightarrow{k \rightarrow +\infty} 0,$$

or en écrivant $\left\{ \frac{\lambda_j}{\rho(A)}, j = 1 \dots p \right\} = \{ \theta_l, l = 1 \dots q \}$, on a

$$\sum_{j=1}^p \left(\frac{\lambda_j}{\rho(A)} \right)^k = \sum_{l=1}^q a_l e^{ik\theta_l} \xrightarrow{k \rightarrow +\infty} 0,$$

avec $a_l > 0$, ce qui est absurde. Donc $\rho(A) < 1$.

□

Démonstration — Preuve du premier corollaire

- Cas d'une norme subordonnée à une norme vectorielle

Soit $\varepsilon \in \mathbf{R}_+^*$. Notons $A_\varepsilon = \frac{1}{\rho(A) + \varepsilon} A$. On a $\rho(A_\varepsilon) = \frac{\rho(A)}{\rho(A) + \varepsilon} < 1$, donc $\lim_{k \rightarrow +\infty} (A_\varepsilon^k) = 0$ et il existe $k_\varepsilon \in \mathbf{N}$ tel que pour tout $k \geq k_\varepsilon$,

$$\|A_\varepsilon^k\| < 1$$

Alors, pour tout $k \geq k_\varepsilon$, $\|A^k\| < (\rho(A) + \varepsilon)^k$, et comme $\rho(A) = (\rho(A^k))^{\frac{1}{k}} \leq \|A^k\|^{\frac{1}{k}}$, on obtient que

$$\rho(A) \leq \|A^k\|^{\frac{1}{k}} \leq \rho(A) + \varepsilon.$$

On a donc bien le résultat pour les normes subordonnées à une norme vectorielle.

- Cas général

Comme on se place en dimension finie, toutes les normes sont équivalentes : il existe donc $\alpha, \beta \in \mathbf{R}_+^*$ tels que $\alpha \|\cdot\|_1 \leq \|\cdot\| \leq \beta \|\cdot\|_1$. Alors, pour tout $k \in \mathbf{N}^*$,

$$\alpha^{\frac{1}{k}} \|A^k\|_1^{\frac{1}{k}} \leq \|A^k\|^{\frac{1}{k}} \leq \beta^{\frac{1}{k}} \|A^k\|_1^{\frac{1}{k}},$$

et donc en laissant k tendre vers $+\infty$, on obtient le résultat.

□

Démonstration — Preuve du second corollaire

Soit $(M - N)x = b$ un système linéaire. On rappelle que la méthode itérative associée est $x_{k+1} = \phi(x_k) = M^{-1}Nx_k + M^{-1}b$, et que la méthode itérative converge si $x_k \rightarrow x$.

Posons $B = M^{-1}N$ et pour tout $k \in \mathbf{N}$, $e_k = x - x_k$ l'erreur effectuée. Alors, la suite (e_k) vérifie l'équation

$$e_{k+1} = Be_k,$$

et la méthode itérative converge si $e_k = B^k e_0$ converge pour tout $e_0 \in \mathbf{R}^n$. On retrouve une des conditions du théorème, et on en déduit que la méthode itérative converge si et seulement si $\rho(B) < 1$.

□

10 Inégalité de Hardy

Leçons : 202,205,207,208,234

Référence: **Analyse pour l'agrégation, Bernis**

Proposition — Soit $p \in]1, +\infty[$. Pour toute fonction $f \in L^p(\mathbf{R}_+, \mathbf{R})$, on pose

$$T_f : \begin{array}{ccc} \mathbf{R}_+^* & \rightarrow & \mathbf{R} \\ x & \mapsto & \frac{1}{x} \int_0^x f(t) dt \end{array} .$$

Alors pour toute fonction $f \in L^p(\mathbf{R}_+)$, $T_f \in L^p(\mathbf{R}_+)$ et on a la majoration

$$\|T_f\|_p \leq \left(\frac{p}{p-1} \right) \|f\|_p.$$

• Cas des fonctions régulières positives

Soit $f \in \mathcal{C}_c(\mathbf{R}_+^*)$. On la prolonge à $\mathbf{R}_+$ par $f(0) = 0$. Comme f est positive, T_f l'est aussi donc ses fonctions puissance sont bien définies.

Par le théorème fondamental de l'analyse, comme f est continue, $T_f \in \mathcal{C}^1(\mathbf{R}_+^*)$ et pour tout $x \in \mathbf{R}_+^*$,

$$T_f'(x) = \frac{1}{x}(f(x) - T_f(x))$$

soit

$$T_f(x) = f(x) - xT_f'(x).$$

Soient $0 < \varepsilon < R < +\infty$ des réels. En multipliant la dernière équation par $T_f^{p-1}(x)$ et en intégrant, on a

$$\int_{\varepsilon}^R T_f^p(x) dx = \int_{\varepsilon}^R T_f^{p-1}(x) f(x) dx - \int_{\varepsilon}^R T_f^{p-1}(x) x T_f'(x) dx.$$

Comme $\frac{1}{p} T_f^p$ et Id sont de classe $\mathcal{C}^1$, par une intégration par parties,

$$\int_{\varepsilon}^R x T_f'(x) T_f^{p-1}(x) dx = \left[x \frac{1}{p} T_f^p(x) \right]_{\varepsilon}^R - \int_{\varepsilon}^R \frac{1}{p} T_f^p(x) dx.$$

Or, comme T_f est de limite nulle en 0 (il suffit de voir T_f comme la limite en 0 du taux d'accroissement pour une primitive de f), on peut laisser tendre ε vers 0.

De l'autre côté, comme p et $\frac{p}{p-1}$ sont conjugués, par l'inégalité de Hölder,

$$\int_0^R T_f^{p-1}(x) f(x) dx = \left(\int_0^R T_f^p(x) dx \right)^{\frac{p-1}{p}} \left(\int_0^R f(x)^p dx \right)^{\frac{1}{p}} \leq \left(\int_0^R T_f^p(x) dx \right)^{\frac{p-1}{p}} \|f\|_p.$$

Finalement, en réinjectant le tout, en réarrangeant l'équation ,

$$\frac{p-1}{p} \left(\int_0^R T_f^p(x) dx \right) \leq \left(\int_0^R T_f^p(x) dx \right)^{\frac{p-1}{p}} \|f\|_p - \frac{R T_f^p(R)}{p} \leq \left(\int_0^R T_f^p(x) dx \right)^{\frac{p-1}{p}} \|f\|_p.$$

Cela nous donne après division par le bon terme une borne indépendante de R à droite, donc comme T_f est positif, $T_f \in L^p(\mathbf{R}_+)$ et en laissant R tendre vers l'infini, on obtient l'inégalité désirée.

• Cas des fonctions régulières de signe quelconque

Pour tout $x \in \mathbf{R}_+^*$, $|T_f(x)| \leq T_{|f|}(x)$ par inégalité triangulaire, et comme $|f|$ est positive, on peut lui appliquer le résultat démontré précédemment. Comme $u \mapsto u^p$ et l'intégrale sont des fonctions croissantes, $T_f \in L^p(\mathbf{R}_+)$. Enfin, comme $\| |f| \|_p = \|f\|_p$, tout est bon.

- Prolongement de l'opérateur T

On a montré que $T : \mathcal{C}_c(\mathbf{R}_+^*) \rightarrow L^p(\mathbf{R}_+)$; $f \mapsto T_f$ est une application linéaire continue car $\frac{p}{p-1}$ -lipschitzienne. Elle est donc uniformément continue par linéarité, dans le Banach $(L^p(\mathbf{R}_+), \|\cdot\|_p)$ (théorème de Riesz-Fischer). Comme $\mathcal{C}_c(\mathbf{R}_+^*)$ est dense dans cet espace, par le théorème de prolongement des applications uniformément continues dans un Banach, il existe une unique application $\tilde{T}$ linéaire continue qui prolonge T à $L^p(\mathbf{R}_+)$. De plus,

$$\|\tilde{T}_f\|_p \leq \frac{p}{p-1} \|f\|_p.$$

- Prolongement de l'inégalité de Hardy

Il reste à montrer que l'inégalité est toujours vraie pour T_f , $f \in L^p$. Soit donc $f \in L^p$. Par densité, on dispose d'une suite (f_n) de fonctions $\mathcal{C}_c(\mathbf{R}_+^*)$ qui converge dans L^p vers f .

Soit $x \in \mathbf{R}_+^*$. Par l'inégalité de Hölder, pour tout $n \in \mathbf{N}$,

$$\begin{aligned} |T_f(x) - T_{f_n}(x)| &\leq \frac{1}{x} \int_0^x |f(t) - f_n(t)| dt, \\ &= \frac{1}{x} x^{\frac{p-1}{p}} \|f_n - f\|_p. \end{aligned}$$

Il vient donc que la suite (T_{f_n}) converge simplement vers T_f sur $\mathbf{R}_+^*$.

D'un autre côté, par continuité du prolongement $\tilde{T}$, $T_{f_n} = \tilde{T}_{f_n} \xrightarrow{L^p} \tilde{T}_f$. Comme L^p est complet par le théorème de Riesz-Fischer, quitte à extraire une sous-suite, la suite T_{f_n} converge presque partout vers $\tilde{T}$.

Donc, presque partout sur $\mathbf{R}_+$,

$$\tilde{T}_f(x) = T_f(x).$$

On en déduit que $T_f \in L^p$ et que

$$\|T_f\|_p \leq \frac{p}{p-1} \|f\|_p.$$

- Optimalité de la borne

Soit $R \in \mathbf{R}_+^*$. Pour tout $\eta \in \mathbf{R}_+^*$, on pose $f_\eta : \mathbf{R}_+ \rightarrow \mathbf{R}$; $t \mapsto \mathbb{1}_{]0,R[}(t) t^{\eta - \frac{1}{p}}$.

Comme T_{f_η} est positive, on a

$$\begin{aligned} \|T_{f_\eta}\|_p^p &\geq \int_0^R T_{f_\eta}^p(x) dx, \\ &\geq \int_0^R \frac{1}{x^p} \frac{1}{\left(\eta - \frac{1}{p} + 1\right)^p} \min(R, x)^{\eta p - 1 + p} dx, \\ &\geq \left(\frac{p}{\eta p + p - 1}\right)^p \int_0^R x^{\eta p - 1} dx, \\ &\geq \left(\frac{p}{\eta p + p - 1}\right)^p \|f_\eta\|_p^p. \end{aligned}$$

Au total, on a pour η quelconque,

$$\frac{p}{p-1+\eta p} \leq \|T\| \leq \frac{p}{p-1},$$

d'où l'optimalité de la borne.

11 Hadamard-Lévy

Leçons : 204,214,215,220

Référence: Analyse pour l'agrégation, Bernis

Théorème — Soient $n \in \mathbf{N}^*$ et $f \in \mathcal{C}^2(\mathbf{R}^n, \mathbf{R}^n)$. Alors f est un $\mathcal{C}^1$ -difféomorphisme si et seulement si f est propre et $df(x)$ est inversible pour tout $x \in \mathbf{R}^n$.

Le sens direct est le plus simple. En effet, si f est un difféomorphisme, alors sa réciproque f^{-1} est aussi $\mathcal{C}^1$. En particulier elle est continue, ce qui donne que f est propre. De plus, en différentiant la relation $f^{-1} \circ f = \text{Id}$, on a que pour tout $x \in \mathbf{R}^n$,

$$df^{-1}(f(x)) \circ df(x) = \text{Id},$$

d'où l'inversibilité de la différentielle en tout point.

Passons maintenant à la réciproque. Celle-ci se montre en plusieurs étapes.

- Construction d'un inverse à droite pour f

Quitte à translater la fonction f , on la prend nulle en 0. Le but est de construire $s : I \times \mathbf{R}^n \rightarrow \mathbf{R}^n$ avec I un intervalle ouvert contenant 0 et 1 et tel que pour tout $(t, x) \in I \times \mathbf{R}^n$,

$$f \circ s(t, x) = tx. \quad (1)$$

Soit $s : I \times \mathbf{R}^n \rightarrow \mathbf{R}^n$ une fonction dérivable. s vérifie (1) si et seulement si

$$\begin{cases} df(s(t, x)) \circ \partial_t s(t, x) = x, \\ f \circ s(0, x) = 0, \end{cases}$$

soit si et seulement si

$$\begin{cases} \partial_t s(t, x) = (df(s(t, x)))^{-1} \cdot x, \\ s(0, x) \in f^{-1}(\{0\}). \end{cases}$$

On considère donc, puisque $0 \in f^{-1}(\{0\})$, le problème de Cauchy suivant :

$$\begin{cases} \frac{dy}{dt} = (df(y))^{-1} \cdot x, \\ y(0) = 0. \end{cases} \quad (2)$$

Notons $F : \mathbf{R}^n \times \mathbf{R}^n \rightarrow \mathbf{R}^n; (x, y) \mapsto (df(y))^{-1} \cdot x$. F est $\mathcal{C}^1$, en effet

- $(x, y) \mapsto x$ et $(x, y) \mapsto y$ le sont,
- $y \mapsto df(y)$ l'est car f est $\mathcal{C}^2$,
- $M \in M_n(\mathbf{R}) \mapsto M^{-1}$ l'est,
- $(M, x) \mapsto Mx$ l'est.

En particulier $F(x, \cdot)$ est de classe $\mathcal{C}^1$ pour tout $x \in \mathbf{R}^n$ donc par le théorème de Cauchy-Lipschitz, il existe une unique solution de (2), notée s_x , et définie sur un intervalle ouvert $]t^-(x), t^+(x)[$ contenant 0. Soit $x_0 \in \mathbf{R}^n$. On suppose par l'absurde que $t^+(x_0) < 1$. Par le lemme de sortie de tout compact, $\|s(t, x_0)\| \xrightarrow{t \rightarrow t^+(x_0)} +\infty$.

La fonction f étant propre, $\|f \circ s(t, x_0)\| \xrightarrow{t \rightarrow t^+(x_0)} +\infty$, or par définition de s , $\|f \circ s(t, x_0)\| = \|tx_0\| \xrightarrow{t \rightarrow t^+(x_0)} t^+(x_0)\|x_0\| < +\infty$, ce qui est absurde. Donc, $t^+(x_0) \geq 1$. Posons $s_1 = s(1, \cdot)$. On obtient donc

$$f \circ s_1 = \text{Id}_{\mathbf{R}^n}.$$

Enfin, comme F est de classe $\mathcal{C}^1$, le théorème de Cauchy-Lipschitz à paramètre nous dit que $s_{|[0,1] \times \mathbf{R}^n}$ est de classe $\mathcal{C}^1$ et a fortiori s_1 l'est aussi. On a construit un inverse à droite $\mathcal{C}^1$ de f .

- f est surjective

En effet, f admet un inverse à droite donc est surjective.

- f est injective

On montre que s_1 est surjective par connexité.

Soit $(x_k)_{k \in \mathbf{N}}$ tel que $s_1(x_k) \rightarrow y \in \mathbf{R}^n$. Par continuité de f , $f \circ s_1(x_k) = x_k \rightarrow f(y)$ et donc finalement,

$$y = \lim s_1(x_k) = \lim s_1(f \circ s_1(x_k)) = s_1(f(y)).$$

$s_1(\mathbf{R}^n)$ est donc fermé.

Soit $y \in s_1(\mathbf{R}^n)$. Il existe $x \in \mathbf{R}^n$ tel que $y = s_1(x)$. Comme $df(y)$ est inversible, par le théorème d'inversion locale, il existe un voisinage ouvert U de x et V un voisinage ouvert de y tel que f induit un $\mathcal{C}^1$ -difféomorphisme ϕ de V sur U . Par continuité de s_1 , on dispose de plus d'un voisinage ouvert de x inclus dans U tel que $s_1(U') \subset V$. Alors,

$$s_1(U') = \phi^{-1}(\phi(s_1(U'))) = \phi^{-1}(U').$$

Or, $\phi^{-1}(U')$ est un ouvert car ϕ est continue, donc $s_1(U')$ est un ouvert inclus dans $s_1(\mathbf{R}^n)$. Cet ensemble est donc ouvert.

Comme $\mathbf{R}^n$ est connexe, s_1 est surjective. Soient $y_1, y_2 \in \mathbf{R}^n$ tels que $f(y_1) = f(y_2)$. On considère x_1 et x_2 des antécédents de y_1 et y_2 par s_1 . Alors,

$$x_1 = f \circ s_1(x_1) = f(y_1) = f(y_2) = f \circ s_1(x_2) = x_2.$$

D'où l'injectivité de f .

- Conclusion

f est bijective, de classe $\mathcal{C}^1$ et s_1 est un inverse à droite. On en déduit que $s_1 = f^{-1}$ et comme on a montré que s_1 est de classe $\mathcal{C}^1$, f est un $\mathcal{C}^1$ -difféomorphisme.

12 Processus de branchement de Galton-Watson

Leçons : 264

Référence: Probabilités pour non probabilistes, Appel

Proposition — Soit $(X_{i,n})_{i,n \geq 1}$ une suite de v.a i.i.d à valeurs dans $\mathbf{N}$ et d'espérance finie notée m . On pose $Z_0 = 1$ et $Z_{n+1} = \sum_{i=1}^{Z_n} X_{i,n+1}$ et $Ext = \{\exists n \in \mathbf{N}^*, Z_n = 0\}$. On note enfin $\rho = \mathbb{P}(Ext)$. Alors,

- $\rho = 1$ si $m \leq 1$ ou $m = 1$ et $\mathbb{P}(X_{1,1} = 1) \neq 1$.
- $\rho < 1$ sinon.

Notons μ la loi des variables $X_{i,n}$. On pose G la fonction génératrice de $X_{1,1}$: $G(t) = \sum_{n=0}^{+\infty} \underbrace{\mathbb{P}(X = n)}_{p_n} t^n$.

- G est croissante, convexe sur $[0, 1]$ et strictement convexe si $\mu([2, \infty[) > 0$.

Comme les p_n , $n \geq 0$, sont positifs, G est bien croissante sur $[0, 1]$.

De plus, comme G est la somme d'une série entière absolument convergente en $t = 1$, son rayon de convergence est strictement supérieur à 1 et G est donc de classe $\mathcal{C}^\infty$ sur $[0, 1[$. On a donc, pour $s \in [0, 1[$,

$$G''(s) = \sum_{k=0}^{\infty} k(k-1)p_k s^{k-2} \geq 0.$$

Donc G est convexe sur $[0, 1]$. De plus, si $\mu([2, \infty[) > 0$, alors il existe $k \geq 2$ tel que $p_k > 0$ et donc $G''(s) > 0$ sur $]0, 1[$ et la convexité est stricte sur cet ensemble.

- $G_{Z_n} = G^{\circ n} = \underbrace{G \circ \dots \circ G}_{n \text{ fois}}$

On procède par récurrence sur $n \in \mathbf{N}$.

$G_{Z_0} = \text{Id} = G^{\circ 0}$ donc la propriété est vraie à l'ordre 0.

Supposons que la propriété est vraie à l'ordre n . Montrons qu'elle est vraie à l'ordre $n+1$. On écrit

$$\begin{aligned} G_{Z_{n+1}}(s) &= E \left[s^{\sum_{i=1}^{Z_n} X_{i,n+1}} \right], \\ &= E \left[\sum_{z=0}^{\infty} s^{\sum_{i=1}^{Z_n} X_{i,n+1}} \mathbb{1}_{Z_n=z} \right], \\ &\stackrel{\text{Fubini}}{=} \sum_{z=0}^{\infty} E \left[s^{\sum_{i=1}^z X_{i,n+1}} \mathbb{1}_{Z_n=z} \right], \\ &\stackrel{\text{indépendance}}{=} \sum_{z=0}^{\infty} \left(\prod_{i=1}^z E \left[s^{X_{i,n+1}} \right] \right) \mathbb{P}(Z_n = z), \\ &\stackrel{\text{même loi}}{=} \sum_{z=0}^{\infty} G(s)^z \mathbb{P}(Z_n = z), \\ &= E \left[G(s)^{Z_n} \right], \\ &= G_{Z_n} \circ G(s), \\ &\stackrel{\text{HR}}{=} G^{\circ(n+1)}(s). \end{aligned}$$

- ρ est le plus petit point fixe de G

Par définition de l'événement Ext , $\rho = \limsup_{n \rightarrow +\infty} \mathbb{P}(Z_n = 0)$ car la suite d'événements $\{Z_n = 0\}$ est croissante. Ainsi ρ est-il un point fixe de G , en effet

$$\rho = \limsup_{n \rightarrow +\infty} G^{\circ n}(0) = \limsup_{n \rightarrow +\infty} G^{\circ(n+1)}(0) = G(\rho),$$

par continuité de G .

De plus, si $t \in [0, 1]$ est un point fixe de G , alors par croissance de G sur $[0, 1]$, on a $G^{circn}(0) \leq G^{on}(t) = t$, donc en passant à la limite supérieure,

$$\rho \leq t.$$

- Conclusion

Si $m > 1$, alors $G(1) = 1$ et $G'(1) > 1$, donc il existe $\eta \in [0, 1[$ tel que pour tout $s > \eta$, $G(s) < s$. Comme $G(0) \leq 0$, le théorème des valeurs intermédiaires nous donne l'existence d'un point fixe G pour un $s \in [0, \eta[$. Donc $\rho < 1$.

Si $m < 1$, $G'(1) < 1$ et comme G reste au-dessus de sa corde, le seul point fixe de G dans $[0, 1]$ est 1. Donc $\rho = 1$.

Si $m = 1$, alors on distingue deux cas. Si $\mu = \delta_1$, alors Z_n est constante de valeur 1 et la probabilité d'extinction est nulle : $\rho = 0$.

Sinon, il existe $k \in \llbracket 2, \infty \rrbracket$ tel que $p_k > 0$, car $m = 1$. Donc G est strictement convexe et donc $\rho = 1$.

13 Formule des compléments

Leçons : 236, 239, 245

Référence: Analyse complexe, Amar et Matheron

Proposition — On note $\Gamma : z \mapsto \int_0^\infty t^{z-1} e^{-t} dt$ la fonction holomorphe sur $\{z \in \mathbf{C}, \Re(z) > 0\}$. Alors, pour tout z de partie réelle strictement comprise entre 0 et 1,

$$\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin(\pi z)}.$$

- Simplification du problème

Par le principe du prolongement analytique, il suffit en réalité de montrer cette relation pour tout $\alpha \in]0, 1[$. Comme les intégrandes sont positives, le théorème de Fubini-Tonelli nous dit que

$$\Gamma(\alpha)\Gamma(1-\alpha) = \int_{t,s>0} \left(\frac{t}{s}\right)^\alpha e^{-(s+t)} ds \frac{dt}{t}.$$

Posons $\varphi : (\mathbf{R}_+^*)^2 \rightarrow (\mathbf{R}_+^*)^2; (t, s) \mapsto \left(\frac{t}{s}, s\right)$. C'est un $\mathcal{C}^1$ -difféomorphisme, de bijection réciproque $\varphi^{-1} : (u, v) \mapsto (uv, v)$. On a donc

$$Jac_{\varphi^{-1}}(u, v) = \begin{pmatrix} v & u \\ 0 & 1 \end{pmatrix},$$

de déterminant v . Par changement de variables,

$$\Gamma(\alpha)\Gamma(1-\alpha) = \int_{u,v>0} u^{\alpha-1} e^{-v(1+u)} du dv.$$

Par un second changement de variables $(u, v) \mapsto (x, y) = (u, v(1+u))$, dont la jacobienne de l'inverse est $\begin{pmatrix} 1 & 0 \\ -\frac{y}{(1+x)^2} & \frac{1}{1+x} \end{pmatrix}$, on a

$$\Gamma(\alpha)\Gamma(1-\alpha) = \int_{x,y>0} x^{\alpha-1} e^{-y} dy \frac{dx}{1+x}.$$

Or, $\int_0^\infty e^{-y} dy = 1$, et comme le terme de gauche est invariant par la transformation $\alpha \leftarrow 1 - \alpha$,

$$\Gamma(\alpha)\Gamma(1-\alpha) = \int_0^\infty \frac{dx}{x^\alpha(1+x)} =: I(\alpha).$$

- Application du théorème des résidus sur un bon contour

On vérifie tout d'abord que $I(\alpha)$ est bien définie (**est-ce vraiment nécessaire vu que je l'ai déduite de la première partie**).

Posons ensuite $\Omega = \mathbf{C} \setminus \mathbf{R}_+$ et $f : \Omega \setminus \{-1\} \rightarrow \frac{1}{z^\alpha(1+z)}$. f est holomorphe sur son domaine de définition et a un pôle simple en -1 . On calcule le résidu de f en -1 :

$$Rs_{-1}(f) = \lim_{z \rightarrow -1(1+z)} f(z) = \frac{1}{(-1)^\alpha} = e^{-i\alpha\pi}.$$

Soient à présent $0 < \varepsilon < 1 < R$. On introduit le compact $K_{\varepsilon,R}$ suivant :

Comme $(-1) \in K_{\varepsilon, R}^\circ$, le théorème des résidus nous dit que

$$\int_{\partial K_{\varepsilon, R}} f(z) dz = 2i\pi e^{-i\pi\alpha}.$$

• Calcul des différentes intégrales

Sur $C_\varepsilon : \gamma(\theta) = \varepsilon e^{i(\pi-\theta)}$ avec $\theta \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$. Par inégalité triangulaire,

$$\left| \int_{C_\varepsilon} f(z) dz \right| = \left| \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \frac{\varepsilon^{1-\alpha} e^{i(1-\alpha)(\pi-\theta)}}{(1 + \varepsilon e^{i(\pi-\theta)})} d\theta \right| \leq \frac{\pi \varepsilon^{1-\alpha}}{1 - \varepsilon} \xrightarrow{\varepsilon \rightarrow 0} 0.$$

Sur $\Gamma_{\varepsilon, R} : \gamma(\theta) = R e^{i\theta}$ avec $\theta \in [\theta_{\varepsilon, R}, 2\pi - \theta_{\varepsilon, R}]$. Alors,

$$\int_{\Gamma_{\varepsilon, R}} f(z) dz = \int_{\theta_{\varepsilon, R}}^{2\pi - \theta_{\varepsilon, R}} \frac{i R^{1-\alpha} e^{i(1-\alpha)\theta}}{1 + R e^{i\theta}} d\theta = F(2\pi - \theta_{\varepsilon, R}) - F(\theta_{\varepsilon, R}),$$

où F est la primitive de l'intégrande nulle en 0. L'intégrande étant continue, F est de classe C^1 et quand $\varepsilon \rightarrow 0$,

$$\int_{\Gamma_{\varepsilon, R}} f(z) dz \xrightarrow{\varepsilon \rightarrow 0} F(2\pi) = i \int_0^{2\pi} \frac{R^{1-\alpha} e^{i(1-\alpha)\theta}}{1 + R e^{i\theta}} d\theta.$$

Sur $I_{\varepsilon, R}^\pm$: Remarquons que pour tout $t \in \mathbf{R}_+^*$, $\begin{cases} (t + i\varepsilon)^\alpha \rightarrow t^\alpha, \\ (t - i\varepsilon)^\alpha \rightarrow e^{2i\pi\alpha} t^\alpha \end{cases}$ et $|f(t + iy)| \leq |f(t)|$. Compte tenu de l'orientation des segments, par le théorème de convergence dominée,

$$\int_{I_{\varepsilon, R}^+} f(z) dz \xrightarrow{\varepsilon \rightarrow 0} \int_0^R \frac{dt}{t^\alpha(1+t)} \quad \text{et} \quad \int_{I_{\varepsilon, R}^-} f(z) dz \xrightarrow{\varepsilon \rightarrow 0} -e^{-2i\pi\alpha} \int_0^R \frac{dt}{t^\alpha(1+t)}.$$

Si l'on reprend le théorème des résidus, quand $\varepsilon \rightarrow 0$,

$$(1 - e^{-2i\pi\alpha}) \int_0^R \frac{dt}{t^\alpha(1+t)} + i \int_0^{2\pi} \frac{R^{1-\alpha} e^{i(1-\alpha)\theta}}{1 + R e^{i\theta}} d\theta = 2i\pi e^{-i\pi\alpha}.$$

Or,

$$\left| \int_0^{2\pi} \frac{R^{1-\alpha} e^{i(1-\alpha)\theta}}{1 + R e^{i\theta}} d\theta \right| \leq 2\pi \frac{R^{1-\alpha}}{R-1} \xrightarrow{R \rightarrow +\infty} 0.$$

. On peut donc laisser R tendre vers l'infini, ce qui nous donne

$$I(\alpha) = 2i\pi \frac{e^{-i\pi\alpha}}{1 - e^{-2i\pi\alpha}} = \frac{\pi}{\sin(\pi\alpha)}.$$

14 Générateurs de $O(E)$, $SO(E)$

remarque : faire gaffe dans la 170 à bien le faire pour $O(q)$ avec q forme quadratique quelconque.

Leçons : 108,161,170

Référence: Cours d'algèbre, Perrin

| **Théorème** — Soit $u \in O(E)$. On pose $F_u = \text{Ker}(u - \text{Id}_E)$ et on note $r_u = n - \dim(F_u) = \text{rg}(u - \text{Id}_E)$.
| Alors, u est le produit d'au plus r_u réflexions.

| **Lemme** — Soient τ_1 et τ_2 des réflexions orthogonales. Il existe θ_1 et θ_2 deux retournements tels que
| $\theta_1\theta_2 = \tau_1\tau_2$.

| **Corollaire** — $SO(E)$ est engendré par les retournements.

Démonstration — Preuve du théorème

On procède par récurrence sur r_u . On admet que Id_E (i.e le cas où $r_u = 0$) s'écrit comme produit de zéro réflexions orthogonales.

Supposons le résultat établi jusqu'au rang $r_u - 1$.

□

15 Générateurs des groupes linéaire et spécial linéaire, application à la connexité

Leçons : 108,162

Référence: ,

Théorème —

1. $\mathrm{SL}_n(\mathbf{K})$ est engendré par les transvections.
2. $\mathrm{GL}_n(\mathbf{K})$ est engendré par les transvections et au plus une dilatation.

Corollaire —

1. $\mathrm{SL}_n(\mathbf{R}), \mathrm{SL}_n(\mathbf{C})$ et $\mathrm{GL}_n(\mathbf{C})$ sont connexes.
2. $\mathrm{GL}_n(\mathbf{R})$ admet deux composantes connexes.

Dans toute cette preuve, on parlera d'opérations sur les lignes et les colonnes plutôt que de produits par des matrices.

Preuve du théorème

On effectue la démonstration pour $\mathrm{SL}_n(\mathbf{K})$ et on se ramène au cas du groupe linéaire par produit par une matrice de dilatation. On raisonne par récurrence.

L'initialisation est immédiate car si $M \in \mathrm{SL}_1(\mathbf{K})$, $M = (1)$ est une matrice de transvection.

Passons à l'hérédité. On suppose le résultat vrai à l'ordre n , montrons qu'il l'est toujours à l'ordre $n + 1$. Soit $M \in \mathrm{SL}_{n+1}(\mathbf{K})$.

- Se ramener au cas $m_{1,1} = 1$.

Si $m_{1,1} \neq 0$, on effectue l'opération $L_1 \leftarrow L_1 - \frac{m_{1,1} - 1}{m_{2,1}} L_2$ (si besoin, i.e si $m_{2,1} = 0$, on fait d'abord $L_2 = L_1 + L_2$).

Si $m_{1,1} = 0$, comme M est inversible, il va exister un terme non nul $m_{j,1}$ dans la première colonne, donc on effectue l'opération $L_1 \leftarrow L_1 + \frac{1}{m_{j,1}} L_j$.

- Virer le reste de la ligne / colonne

On pose

$$M'' = T_{n+1,1}(-a_{n+1,1}) \dots T_{2,1}(-a_{2,1}) M T_{1,2}(-a_{1,2}) \dots T_{1,n+1}(-a_{1,n+1}) = \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & M' \end{array} \right)$$

où $M' \in \mathrm{SL}_n(\mathbf{K})$.

- Hypothèse de récurrence

Par hypothèse de récurrence, il existe $P_1, \dots, P_r, Q_1, \dots, Q_s$ des matrices de transvection telles que

$$P_1 \dots P_r M' Q_1 \dots Q_s = I_n.$$

En posant

$$T_i = \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & P_i \end{array} \right), U_j = \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & Q_j \end{array} \right)$$

pour obtenir

$$T_1 \dots T_r M'' U_1 \dots U_s = I_{n+1}.$$

Par récurrence, on a montré que le groupe spécial linéaire est engendré par les transvections.

Preuve du corollaire

- Pour le groupe spécial linéaire

Soit $M \in \mathrm{SL}_n(\mathbf{K})$.

Par le théorème, on écrit $M = \prod_{k=1}^r T_{i_k, j_k}(\lambda_k)$. Posons

$$\varphi : [0, 1] \rightarrow \mathrm{SL}_n(\mathbf{K}); t \mapsto \prod_{k=1}^r T_{i_k, j_k}(t\lambda_k).$$

φ est continue, à valeurs dans $\mathrm{SL}_n(\mathbf{K})$, vaut I_n en 0 et M en 1. D'où la connexité par arcs.

- Pour $GL_n(\mathbf{C})$

On écrit $M = \prod_{k=1}^r T_{i_k, j_k}(\lambda_k) D_n(\rho e^{i\theta})$ où $\rho e^{i\theta} = \det(M) \neq 0$. On pose

$$\varphi : [0, 1] \rightarrow GL_n(\mathbf{C}); t \mapsto \prod_{k=1}^r T_{i_k, j_k}(t\lambda_k) D_n((tr + (1-t)) e^{it\theta}).$$

C'est un chemin continu qui relie M à I_n .

- Pour $GL_n(\mathbf{R})$

Soit $\varepsilon = \pm 1$. On écrit $M = \prod_{k=1}^r T_{i_k, j_k}(\lambda_k) D_n(\det(M))$. On pose

$$\varphi^\varepsilon : [0, 1] \rightarrow GL_n^\varepsilon(\mathbf{R}); t \mapsto \prod_{k=1}^r T_{i_k, j_k}(t\lambda_k) D_n((1-t)\varepsilon + t\det(M)).$$

φ est un chemin continu qui relie M à $\mathrm{diag}(1, \dots, 1, \varepsilon)$. Donc $GL_n(\mathbf{R})$ a deux composantes connexes qui sont $GL_n^+(\mathbf{R})$ et $GL_n^-(\mathbf{R})$.

16 Théorème du point fixe de Brouwer

Leçons : 203, 214, 215

Référence: Calcul différentiel, Gonnord, Tosel

Théorème — (Théorème de Brouwer) Soit $n \geq 1$. On pose B la boule unité de $\mathbf{R}^n$. Toute fonction $f : B \rightarrow B$ continue admet un point fixe.

Supposons par l'absurde qu'il existe $f : B \rightarrow B$ qui n'admet aucun point fixe.

- Se ramener au cas où f est $\mathcal{C}^1$.

Nous allons approcher f par un polynôme qui n'admet aucun point fixe sur B .

L'application $x \mapsto f(x) - x$ est continue sur le compact B et ne s'annule jamais, donc il existe $\varepsilon \in \mathbf{R}_+^*$ tel que pour tout $x \in B$, $\|f(x) - x\| > \varepsilon$, où $\|\cdot\|$ est la norme euclidienne sur $\mathbf{R}^n$. Par le théorème de Weierstrass, on dispose de $P : \mathbf{R}^n \rightarrow \mathbf{R}^n$ à coordonnées polynômiales tel que $\|f - P\|_\infty \leq \frac{\varepsilon}{2}$. On en déduit que pour tout $x \in B$, par inégalité triangulaire,

$$\|P(x)\| \leq \|P(x) - f(x)\| + \|f(x)\| \leq \frac{\varepsilon}{2} + 1.$$

Posons à présent $Q = \frac{1}{1 + \frac{\varepsilon}{2}} P$. Q est $\mathcal{C}^1$ et $Q(b) \subset B$. De plus, Q est distant de f de moins de ε pour la norme uniforme, donc par inégalité triangulaire, pour tout $x \in B$,

$$\|Q(x) - x\| \geq \|f(x) - x\| - \|Q(x) - f(x)\| > 0.$$

Donc Q n'admet pas de point fixe.

- Montrer l'existence d'une rétraction $\varphi : B \rightarrow S = S^{n-1}$ de classe $\mathcal{C}^1$ tel que $\varphi|_S = \text{Id}_S$.

On cherche φ sous la forme

$$\begin{cases} \varphi(x) &= f(x) + \lambda(x)(x - f(x)), \text{ où } \lambda(x) > 0, \\ \|\varphi(x)\| &= 1. \end{cases}$$

Géométriquement, $\varphi(x)$ est l'intersection de la sphère et de la demi-droite $[f(x), x]$. De plus, comme φ est à valeurs dans S ,

$$\begin{aligned} & \|f(x) + \lambda(x)(x - f(x))\|^2 - 1 = 0, \\ \text{donc } & \underbrace{\|x - f(x)\|^2 \lambda(x)^2 + 2 \langle f(x), x - f(x) \rangle \lambda(x) + \|f(x)\|^2 - 1}_{R(\lambda(x))} = 0. \end{aligned}$$

Comme $R(0) \leq 0$ et $R(1) \leq 0$ par simple vérification, et que $R(x) \xrightarrow{|x| \rightarrow +\infty} +\infty$, $\|x - f(x)\|^2 > 0$ et R admet deux racines distinctes dont une plus grande que 1. On choisit donc $\lambda(x)$ comme étant cette racine :

$$\lambda(x) = \frac{-\langle f(x), x - f(x) \rangle + \sqrt{\Delta(x)}}{\|x - f(x)\|^2}.$$

On en déduit que l'application $x \mapsto \lambda(x)$ est $\mathcal{C}^1$ et φ est donc $\mathcal{C}^1$ sur B .

On a $\varphi(x) \in S$ pour tout $x \in B$ et si $x \in S$, $R(1) = 0$ donc $\lambda(x) = 1$ et $\varphi(x) = x$. On a bien

$$\varphi|_S = \text{Id}_S.$$

Dorénavant, on note, pour $t \in [0, 1]$, $\varphi_t : B \rightarrow B; x \mapsto (1 - t)x + t\varphi(x)$. Pour tout t , φ_t est $\mathcal{C}^1$ sur B . De plus, $\varphi_0 = \text{Id}$ et $\varphi_1 = \varphi$. On notera également $P(t) = \int_B \det J_{\varphi_t}(x) dx$ qui est un polynôme en t .

- Préparer la contradiction du raisonnement par l'absurde

Soit $x \in B$. En différentiant la relation $\|\varphi(x)\|^2 = 1$, on obtient que pour tout $h \in \mathbf{R}^n$,

$$\langle \varphi(x), d\varphi(x) \cdot h \rangle = 0,$$

donc $\text{Im}(d\varphi(x)) \subset \varphi(x)^\perp (\neq \{0\})$. On en déduit que $\text{rg}(d\varphi(x)) \leq n - 1$ dont $d\varphi(x)$ n'est pas injective. Donc $\det J_{\varphi_1}(x) = \det J_{\varphi(x)} = 0$ et $P(1) = 0$.

- Montrer que φ_t est injective pour t petit

Soient $t \in [0, 1]$ et $x, y \in B$ tels que $\varphi_t(x) = \varphi_t(y)$. Alors,

$$(1 - t)\|x - y\| = t\|\varphi(x) - \varphi(y)\|.$$

Or, φ est $\mathcal{C}^1$ donc puisque B est un convexe compact, l'application du théorème des accroissements finis nous donne que

$$\|\varphi(x) - \varphi(y)\| \leq M\|x - y\|,$$

où $M = \sup_{\zeta \in B} \|\mathrm{d}\varphi(\zeta)\| \geq 0$. Donc, en prenant $0 \leq t < \alpha = \frac{1}{1 + M} \leq 1$, l'inégalité

$$\|x - y\| \leq \frac{tM}{1 - t}\|x - y\|$$

nous donne nécessairement que $x = y$ et donc que φ_t est injective.

Or, pour tout $x \in S$, $\varphi_t(x) = x$, donc $\varphi_t|_S = \mathrm{Id}_S$ et par injectivité, on obtient que pour tout $t \in [0, \alpha[$, $\varphi_t(\overset{\circ}{B}) \subset \overset{\circ}{B}$.

- Montrer que φ_t est un $\mathcal{C}^1$ -difféomorphisme de $\overset{\circ}{B}$ sur son image

Soient $t \in [0, \alpha[$ et $x \in B$. On écrit $\det J_{\varphi_t}(x) = a_n(x)t^n + \dots + a_1(x)t + 1$ (le terme d'ordre 0 vaut 1 car $J_{\varphi_0} = \mathrm{Id}$).

Posons $\beta = \min\left(\alpha, \frac{1}{m}\right)$ où $m = \sup_{x \in B, t \in [0, 1]} |a_n(x)t^{n-1} + \dots + a_1(x)|$ et prenons $t < \beta$. Alors

$$|a_n(x)t^n + \dots + a_1(x)t| \leq mt < 1$$

donc $\det J_{\varphi_t}(x) > 0$ pour tout $x \in \overset{\circ}{B} \subset B$.

φ_t étant injective pour $t < \beta \leq \alpha$, par le théorème d'inversion globale, φ_t réalise un $\mathcal{C}^1$ -difféomorphisme de $\overset{\circ}{B}$ sur $\varphi_t(\overset{\circ}{B}) \subset \overset{\circ}{B}$ et $\varphi_t(\overset{\circ}{B})$ est ouvert.

- Montrer que $\varphi_t(\overset{\circ}{B}) = \overset{\circ}{B}$ pour $t < \beta$ par connexité

On a vu que $\varphi_t(\overset{\circ}{B}) \subset \overset{\circ}{B}$ est non vide et est ouvert dans $\mathbf{R}^n$ donc dans $\overset{\circ}{B}$ pour $t < \beta$. Il reste à montrer qu'il est fermé.

Soit $(y_k)_{k \in \mathbf{N}}$ une suite de $\varphi_t(\overset{\circ}{B})$ et soit $y \in \overset{\circ}{B}$ telle que $y_k \xrightarrow[k \rightarrow +\infty]{} y$. On note x_k l'antécédent de y_k par φ_t . (x_k)

est une suite de $\overset{\circ}{B} \subset B$ compact, donc quitte à extraire on peut supposer qu'elle converge vers une limite $x \in B$. Par continuité de φ_t , on a donc que $\varphi_t(x) = y$.

Or, $\begin{cases} \varphi_t(x) = y \notin S, \\ \varphi_t|_S = \mathrm{Id}_S, \end{cases}$ donc $x \in \overset{\circ}{B}$ et $y = \varphi_t(x) \in \varphi_t(\overset{\circ}{B})$. Donc $\varphi_t(\overset{\circ}{B})$ est fermé dans $\overset{\circ}{B}$.

Enfin, $\overset{\circ}{B}$ est convexe donc connexe, donc $\varphi_t(\overset{\circ}{B}) = \overset{\circ}{B}$.

Pour $t < \beta$, φ_t réalise donc un $\mathcal{C}^1$ -difféomorphisme de $\overset{\circ}{B}$ sur $\overset{\circ}{B}$.

- Montrer que P est constant sur $[0, \beta[$

Pour $t < \beta$, on a que

$$P(t) = \int_{\overset{\circ}{B}} \det J_{\varphi_t}(x) \, dx$$

, donc puisque l'intégrande est strictement positive en tout point d'après l'étape 5, un changement de variables nous donne que

$$P(t) = \int_{\overset{\circ}{B}} |\det J_{\varphi_t}(x)| \, dx = \int_{\overset{\circ}{B}} dy = \lambda(\overset{\circ}{B}).$$

Donc P est un polynôme constant strictement positif sur $[0, \beta[$, il est donc constant sur $[0, 1]$. Cela contredit le point 3 où nous avons montré que $P(1) = 0$.

f admet donc au moins un point fixe.

17 Calcul de l'intégrale de Fresnel

Leçons : 239

Référence: Analyse, Gourdon

Soit $\alpha \in]0, 1[$.

Alors, $J(\alpha) = \int_0^{+\infty} t^{\alpha-1} e^{it} dt = \Gamma(\alpha) e^{i\alpha \frac{\pi}{2}}$.

Application : $\int_0^{+\infty} e^{ix^2} dx = \frac{\sqrt{\pi}}{2} e^{i\frac{\pi}{4}}$.

• Introduction des données du problème

Pour tout $\alpha \in]0, 1[$, $J(\alpha)$ est bien définie : en 0 car $1 - \alpha < 1$ et en $+\infty$ par IPP.

Posons, pour $x \in \mathbf{R}_+^*$, $I(x) = \int_0^{+\infty} e^{-t} e^{ixt} t^{\alpha-1} dt$. Par un changement de variable $u = xt$,

$$I(x) = \frac{1}{x^\alpha} \int_0^{+\infty} e^{-\frac{u}{x}} e^{iu} u^{\alpha-1} du \quad \forall x \in \mathbf{R}_+^*.$$

• Montrer que $J(\alpha) = \lim_{x \rightarrow +\infty} x^\alpha I(x)$.

On ne peut pas le faire directement car en l'infini on ne peut pas dominer correctement. Posons donc $\tilde{I} : \mathbf{R}_+^* \rightarrow \mathbf{C}, y \mapsto \int_0^{+\infty} e^{-uy} e^{iu} u^{\alpha-1} du$. On va montrer que $\tilde{I}$ est définie et continue en 0 et on aura $J(\alpha) = \tilde{I}(0)$.

$\tilde{I}$ est bien définie et continue sur $\mathbf{R}_+^*$.

Posons $f : \mathbf{R}_+ \rightarrow \mathbf{R}; u \mapsto u^{\alpha-1}$ et $g : \mathbf{R}_+ \rightarrow \mathbf{R}; u \mapsto \cos(u)$.

f est $\mathcal{C}^1$ et décroissante de limite nulle, g est continue, et pour tout $x \in \mathbf{R}_+$, $\left| \int_0^x g(t) dt \right| \leq 2\pi$. Par le théorème d'Abel, $\int_0^{+\infty} f(u)g(u) du$ est bien définie. En procédant de la même façon avec $g = \sin$, on obtient que $\tilde{I}(0)$ est bien définie.

On va à présent montrer la continuité de $\tilde{I}$ en 0. On ne peut pas dominer correctement donc le théorème de continuité d'une intégrale à paramètre est inutilisable. Posons donc, pour tout $n \in \mathbf{N}^*$, $\tilde{I}_n(y) = \int_{\frac{1}{n}}^n e^{-uy} e^{iu} u^{\alpha-1} du$.

Soit $y \in \mathbf{R}_+$.

$$\begin{aligned} |\tilde{I}(y) - \tilde{I}_n(y)| &= \left| \int_0^n u^{\alpha-1} e^{-uy} e^{iu} du + \int_n^{+\infty} e^{-uy} e^{iu} u^{\alpha-1} du \right|, \\ &\leq \int_0^{\frac{1}{n}} u^{\alpha-1} du + \left| \int_0^{+\infty} e^{-uy} e^{iu} u^{\alpha-1} du \right|. \end{aligned}$$

On calcule la première intégrale par un calcul direct. Pour la deuxième, on procède par intégration par parties (bien penser à détailler avec la borne $A \in \mathbf{R}_+$ à faire tendre vers l'infini) :

$$|\tilde{I}(y) - \tilde{I}_n(y)| \leq \frac{1}{\alpha n^\alpha} + \left| \frac{1}{(i-y)n^{1-\alpha}} e^{n(i-y)} \right| + \int_n^\infty \frac{|\alpha-1|}{|i-y|} u^{\alpha-2} |e^{u(i-y)}| du.$$

Or, $|i-y| \geq 1$ donc

$$\begin{aligned} |\tilde{I}(y) - \tilde{I}_n(y)| &\leq \frac{1}{\alpha n^\alpha} + \frac{1}{n^{1-\alpha}} + (1-\alpha) \int_n^\infty u^{\alpha-2} du, \\ &\leq \frac{1}{\alpha n^\alpha} + \frac{1}{n^{1-\alpha}} - \left[u^{(\alpha-1)} \right]_n^\infty, \\ &\leq \frac{1}{\alpha n^\alpha} + \frac{1}{n^{1-\alpha}}, \\ &\xrightarrow{n \rightarrow +\infty} 0. \end{aligned}$$

On a montré que $\|\tilde{I} - \tilde{I}_n\|_\infty \xrightarrow{n \rightarrow +\infty} 0$, donc $\tilde{I}$ est continue en 0. On a donc que

$$\lim_{y \rightarrow 0} \tilde{I}(y) = \lim_{x \rightarrow +\infty} \frac{1}{x^\alpha} x^\alpha I(x) = J(\alpha).$$

- Calcul de $I(x)$

On va montrer que I est solution d'une EDO sur $\mathbf{R}_+$.

- L'intégrande est bien mesurable sur $\mathbf{R}_+$.
- L'intégrande est dérivable sur $\mathbf{R}_+^*$, de dérivée par rapport à x $t \mapsto e^{-t} t^\alpha i e^{ixt}$.
- Pour tout $(x, t) \in \mathbf{R}_+^2$, $|e^{-t} t^\alpha i e^{ixt}| = e^{-t} t^\alpha$ est bien intégrable.

Par le théorème de dérivation d'une intégrale à paramètre, I est dérivable sur $\mathbf{R}_+^*$ et par une IPP,

$$I'(x) = \int_0^\infty i e^{-t} e^{ixt} t^\alpha dt = -\frac{\alpha}{i+x} I(x).$$

On calcule que $\int \frac{dx}{i+x} = \int \frac{x-i}{x^2+1} dx = \frac{1}{2} \ln(x^2+1) - i \arctan(x) + k$. Donc pour tout $x \in \mathbf{R}_+^*$,

$$I(x) = C(x^2+1)^{-\frac{\alpha}{2}} e^{i\alpha \arctan(x)}.$$

Comme $I(0) = C = \Gamma(\alpha)$, en laissant x tendre vers l'infini,

$$J(\alpha) = \Gamma(\alpha) e^{i\alpha \frac{\pi}{2}}.$$

Pour l'intégrale de Fresnel, prenons $\alpha = \frac{1}{2}$. Par un changement de variables $x = \sqrt{t}$,

$$J\left(\frac{1}{2}\right) = \sqrt{\frac{\pi}{\sin\left(\frac{\pi}{2}\right)}} e^{i\frac{\pi}{4}} = 2 \int_0^{+\infty} e^{ix^2} dx.$$

D'où le résultat.

18 Moyenne arithmético-géométrique, application à la méthode des isopérimètres

19 Inégalité de Le Cam

Leçons : 262, 264

Référence: De l'intégration aux probabilités, Garet, Kurtzmann Soient $\lambda \in \mathbf{R}$ et $n \in \mathbf{N}^*$ tels que $0 < 2\lambda < n$.

Alors, si $X \sim \mathcal{B}\left(n, \frac{\lambda}{n}\right)$ et $Y \sim \mathcal{P}(\lambda)$, on a :

$$\sum_{k=0}^{+\infty} |\mathbb{P}(X = k) - \mathbb{P}(Y = k)| \leq \frac{4\lambda^2}{n}.$$

- Définition d'une loi de probabilités sur $\mathbf{N} \times \{0, 1\}$

Notons $p_n = \frac{\lambda}{n}$. On définit μ_n sur $\mathbf{N} \times \{0, 1\}$ par :

$Y \backslash X$	0	1	$k \in \mathbf{N} \setminus \{0, 1\}$
0	$e^{-p_n} - p_n(1 - e^{-p_n})$	0	$\frac{p_n^k}{k!} e^{-p_n}$
1	$p_n(1 - e^{-p_n})$	$p_n e^{-p_n}$	0

Cette loi est une loi de probabilités sur $\mathbf{N} \times \{0, 1\}$. En effet,

$$\begin{aligned} \sum_{k=0}^{\infty} \mathbb{P}(X = k, Y = 0) + \mathbb{P}(X = k, Y = 1) &= e^{-p_n} + \sum_{k=2}^{\infty} \mathbb{P}(X = k, Y = 0) + \mathbb{P}(X = k, Y = 1) + p_n e^{-p_n}, \\ &= e^{-p_n} + \left(\sum_{k=1}^{\infty} \frac{p_n^k}{k!} \right) e^{-p_n}, \\ &= e^{-p_n} \left(\sum_{k=0}^{\infty} \frac{p_n^k}{k!} \right), \\ &= 1. \end{aligned}$$

On est aussi en mesure de déterminer les lois marginales de cette loi :

- Pour tout $k \in \mathbf{N}$, $\mathbb{P}(X = k) = \frac{p_n^k}{k!}$ donc X suit une loi de Poisson de paramètre p_n .
- $\mathbb{P}(Y = 1) = p_n$ et $\mathbb{P}(Y = 0) = e^{-p_n} - p_n(1 - e^{-p_n}) + \sum_{k=2}^{\infty} \frac{p_n^k}{k!} e^{-p_n} = 1 - p_n$, donc Y suit une loi de Bernoulli de paramètre p_n .
- Petit lemme

Lemme — Soient X_1, X_2 deux variables aléatoires discrètes à valeurs dans $\mathbf{N}$. Alors pour tout $A \subset \mathbf{N}$,
 $|\mathbb{P}(X_1 \in A) - \mathbb{P}(X_2 \in A)| \leq \mathbb{P}(X_1 \neq X_2)$.

Démonstration — Soit $A \subset \mathbf{N}$. Comme les événements $\{X_1 = X_2\}$ et $\{X_1 \neq X_2\}$ forment un système complet d'événements,

$$\mathbb{P}(X_1 \in A) = \mathbb{P}(X_1 \in A \cap X_1 = X_2) + \mathbb{P}(X_1 \in A \cap X_1 \neq X_2) \leq \mathbb{P}(X_1 \neq X_2) + \mathbb{P}(X_2 \in A),$$

donc par symétrie des rôles, on a bien le résultat souhaité. $<$

□

- Retour à nos moutons

Soient $(X_1, Y_1), \dots, (X_n, Y_n)$ n couples de variables aléatoires indépendantes et identiquement distribuées de loi μ_n . Posons $Y = \sum_{i=1}^n Y_i$ et $X = \sum_{i=1}^n X_i$. Alors, $X \sim \mathcal{P}(\lambda)$ et $Y \sim \mathcal{B}\left(n, \frac{\lambda}{n}\right)$. Par le lemme, pour tout $A \subset \mathbf{N}$,

$$\begin{aligned} |\mathbb{P}(X \in A) - \mathbb{P}(Y \in A)| &\leq \mathbb{P}(X \neq Y), \\ &\leq \mathbb{P}(\exists i \in \llbracket 1, n \rrbracket, X_i \neq Y_i). \end{aligned}$$

Or, pour tout $i \in \llbracket 1, n \rrbracket$,

$$\begin{aligned}
 P(X_i = Y_i) &= \mathbb{P}(X_i = 0, Y_i = 0) + \mathbb{P}(X_i = 1, Y_i = 1), \\
 &= e^{-p_n} - p_n(1 - e^{-p_n}) + p_n e^{-p_n}, \\
 &= e^{-p_n}(1 + 2p_n) - p_n, \\
 &\geq (1 - p_n)(1 + 2p_n) - p_n, \\
 &\geq 1 - 2p_n^2.
 \end{aligned}$$

On en déduit que pour tout i , $\mathbb{P}(X_i \neq Y_i) \leq 2 \left(\frac{\lambda}{n}\right)^2$. Donc, pour tout $A \subset \mathbf{N}$,

$$\begin{aligned}
 |\mathbb{P}(X \in A) - \mathbb{P}(Y \in A)| &\leq \sum_{i=1}^n 2 \left(\frac{\lambda}{n}\right)^2, \\
 &\leq 2 \frac{\lambda^2}{n}.
 \end{aligned}$$

- Conclusion

Si on prend, dans l'étape précédente, $A = \{k \in \mathbf{N} \mid \mathbb{P}(X = k) \geq \mathbb{P}(Y = k)\}$ et $B = \mathbf{N} \setminus A$, on a un système complet d'événements et

$$\begin{aligned}
 \sum_{k=0}^{\infty} |\mathbb{P}(X = k) - \mathbb{P}(Y = k)| &= \sum_{k \in A} |\mathbb{P}(X = k) - \mathbb{P}(Y = k)| + \sum_{k \in B} |\mathbb{P}(X = k) - \mathbb{P}(Y = k)|, \\
 &= \sum_{k \in A} \mathbb{P}(X = k) - \mathbb{P}(Y = k) + \sum_{k \in B} \mathbb{P}(Y = k) - \mathbb{P}(X = k), \\
 &= \mathbb{P}(X \in A) - \mathbb{P}(Y \in A) - \mathbb{P}(Y \in B) + \mathbb{P}(X \in B), \\
 &\leq 4 \frac{\lambda^2}{n}.
 \end{aligned}$$

20 Sous-espace engendré par les translatées d'une fonction

Leçons : 151,159

Référence: Oaux X-ENS Algèbre 1, Francinou, Gianella, Nicolas

1. Soit K un corps commutatif et soient $f_1, \dots, f_n$ des applications de K dans K . Alors, $(f_1, \dots, f_n)$ est libre dans $\mathcal{F}(K, K)$ si et seulement s'il existe $(x_1, \dots, x_n) \in K^n$ tel que la matrice $(f_i(x_j))_{i,j}$ est inversible.
2. Prenons le $K = \mathbf{R}$. Si $f : \mathbf{R} \rightarrow \mathbf{R}$ est dérivable, alors f est solution d'une équation différentielle linéaire homogène à coefficients constants si et seulement si $\dim(\text{Vect}(f_a : x \mapsto f(x+a))) < +\infty$.

Preuve du premier point

- Sens indirect

Supposons par contraposée que $(f_1, \dots, f_n)$ est liée. Alors pour tout $(x_1, \dots, x_n)$, les colonnes de la matrice $(f_i(x_j))_{i,j}$ sont liées. Donc la matrice n'est pas inversible.

- Sens direct

Supposons que la famille est libre. Notons F le sous-espace vectoriel engendré par cette famille.

Alors, pour tout $a \in K$, $e_a : F \rightarrow K; f \mapsto f(a)$ est une forme linéaire et $A = (e_a)_{a \in K}$ engendre F^* . En effet, si $f \in A^\circ$, $e_a(f) = f(a) = 0$ pour tout $a \in K$ donc $f \equiv 0$. On en déduit que $A^\circ = \{0\}$ donc $\text{Vect}(A) = F^*$ car on travaille en dimension finie.

Soit $(x_1, \dots, x_n) \in K^n$ tel que $(e_{x_i})_i$ soit une base de F^* . Posons $M = (f_i(x_j)) = (L_i)$. Si les lignes de la matrice sont liées, alors pour tout $j \in \llbracket 1, n \rrbracket$, $\sum_{i=1}^n \lambda_i f_i(x_j) = 0$, autrement dit $e_{x_j} \left(\underbrace{\sum_{i=1}^n \lambda_i f_i}_g \right) = 0$. Donc $g \in (F^*)^\circ = \{0\}$ et

par liberté de $(f_1, \dots, f_n)$, $\lambda_1 = \dots = \lambda_n = 0$. D'où l'inversibilité de la matrice.

Preuve du second point

- Sens direct

Supposons f solution d'une équation différentielle linéaire homogène à coefficients constants d'ordre p . Alors, pour tout $a \in \mathbf{R}$, f_a vérifie la même équation. Comme l'ensemble des solutions de l'équation est un espace vectoriel de dimension p , $(f_a)_{a \in \mathbf{R}}$ engendre un sous-espace vectoriel de dimension inférieure ou égale à p .

- Sens indirect

Supposons que $F = \text{Vect}(f_a)$ soit de dimension finie n . Remarquons que tout élément de F est dérivable car f l'est. Soient $a_1, \dots, a_n$ des réels tels que $(f_{a_1}, \dots, f_{a_n})$ soit une base de F .

Par le premier point, on dispose de $x_1, \dots, x_n \in K$ tels que $M = (f_{a_i}(x_j))_{i,j}$ est inversible.

Soit $g \in F$. On va montrer que $g' \in F$, autrement dit que F est stable par dérivation.

Pour tout $a \in \mathbf{R}$, $g_a \in \text{Vect}(f_{a_1+a}, \dots, f_{a_n+a}) \subset F$, donc il existe une famille $(\lambda_1(a), \dots, \lambda_n(a))$ tels que

$$g(a) = \sum_{i=1}^n \lambda_i(a) f_{a_i}.$$

Alors, pour tout $j \in \llbracket 1, n \rrbracket$, $g(a + x_j) = g_a(x_j) = \sum_{i=1}^n \lambda_i f_i(x_j)$, ce qui se réécrit sous la forme

$$\begin{pmatrix} g_a(x_1) \\ \vdots \\ g_a(x_n) \end{pmatrix} = {}^t M \begin{pmatrix} \lambda_1(a) \\ \vdots \\ \lambda_n(a) \end{pmatrix}.$$

Comme M est inversible, on peut exprimer les $\lambda_i(a)$ comme combinaisons linéaires des $g_a(x_j) = g_{x_j}(a)$, donc les λ_i sont des fonctions dérivables. En dérivant la relation $g(a+x) = \sum_{i=1}^n \lambda_i(a) f_{a_i}(x)$ par rapport à a , on obtient donc que

$$g'(x+a) = \sum_{i=1}^n \lambda'_i(a) f_{a_i}(x).$$

En prenant $a = 0$, on obtient que $g' \in F$.

De là, il vient que g est de classe $\mathcal{C}^\infty$ et que pour tout $k \in \mathbf{N}$, $g^{(k)} \in F$. C'est en particulier vrai pour f . Or, comme F est de dimension finie, la famille $(f^{(k)})_k$ engendre un sous-espace vectoriel de dimension finie p , autrement dit f est solution d'une équation différentielle linéaire à coefficients constants.

21 Morphismes continus de $\mathbf{S}^1$ dans $GL_n(\mathbf{R})$.

Leçons : 102, 106, 156

Référence: Oaux X-ENS Algèbre ??, Francinou, Gianella, Nicolas

1. Soit f un sous-groupe à un paramètre de $GL_n(\mathbf{C})$. Il existe $A \in M_n(\mathbf{C})$ tel que $f(t) = e^{tA}$ pour tout $t \in \mathbf{R}$.
2. Les morphismes continus $(\mathbf{S}^1, \times) \rightarrow (GL_n(\mathbf{R}), \times)$ sont exactement les applications de la forme $e^{it} \mapsto Q \operatorname{diag}(R_{tk_1}, \dots, R_{tk_r}, 1, \dots, 1) Q^{-1}$ avec $Q \in GL_n(\mathbf{R})$.

Preuve du premier point

- Se ramener au cas où f est dérivable.

Posons $F : \mathbf{R} \rightarrow M_n(\mathbf{C}); x \mapsto \int_0^x f(t) dt$. Par le théorème fondamental de l'analyse, F est de classe $\mathcal{C}^1$ sur $\mathbf{R}$.

Tout d'abord, il existe $a \in \mathbf{R}$ tel que $F(a)$ est inversible. En effet, on a $\frac{F(t)}{t} \xrightarrow[t \rightarrow 0]{} f(0) \in GL_n(\mathbf{C})$ et $GL_n(\mathbf{C})$ est ouvert, donc il existe $a \in \mathbf{R}$ suffisamment proche de 0 pour que $F(a)$ soit inversible.

Ensuite, comme f est un morphisme, pour tout $x, u \in \mathbf{R}$, $f(x+u) = f(x)f(u)$, donc en intégrant par rapport à la variable u ,

$$\underbrace{\int_0^a f(x+u) du}_{g(x)} = f(x)F(a).$$

Or, par un changement de variable affine, $g(x) = F(x+a) - F(a)$ qui est dérivable, donc $f(x) = g(x)F(a)^{-1}$ est également dérivable.

- Conclusion

On dérive la relation $f(s+t) = f(s)f(t)$ par rapport à t . Cela donne que $f'(s+t) = f(s)f'(t)$, donc en prenant $t = 0$, on voit que f vérifie l'équation $f'(s) = f'(0)f(s)$ et donc en notant $A = f'(0)$, et en posant $g(s) = f(s)e^{-sA}$, on a que g est dérivable et $g' = 0$ donc g est constante de valeur $f(0) = \operatorname{Id}$ donc

$$f : s \mapsto e^{sA}.$$

Preuve du second point Soit $\varphi : (\mathbf{S}^1, \times) \rightarrow (GL_n(\mathbf{R}), \times)$ un morphisme de groupes continu.

- Premières propriétés

On munit $M_n(\mathbf{C})$ de la norme $\|\cdot\|$.

Comme $\det \circ \varphi : \mathbf{S}^1 \rightarrow \mathbf{R}^*$ est une fonction continue, comme $\mathbf{S}^1$ est connexe et compact et que $\det \circ \varphi(1) = 1$, on sait que $\det \circ \varphi(\mathbf{S}^1)$ est un segment contenu dans $\mathbf{R}_+^*$. Or, comme $\det \circ \varphi$ est un morphisme de groupes, son image est un sous-groupe de $\mathbf{R}_+^*$, donc forcément réduit à $\{1\}$ (tout sous-groupe non trivial de $\mathbf{R}_+^*$ n'est pas borné).

De plus, comme $\mathbf{S}^1$ est compact, $\varphi(\mathbf{S}^1)$ l'est aussi et il existe $M \in \mathbf{R}_+$ tel que pour tout $z \in \mathbf{S}^1$, $\|\varphi(z)\| \leq M$. Soit λ une valeur propre complexe de $\varphi(z)$. Alors, $|\lambda| \leq C\|\varphi(z)\|$ pour une certaine constante C et donc l'ensemble $\{\lambda \text{ valeur propre de } \varphi(\mathbf{S}^1)\}$ est borné.

Comme pour tout $p \in \mathbf{Z}$, λ^p est valeur propre de $\varphi(z)^p = \varphi(z^p)$, $(|\lambda|^p)_{p \in \mathbf{Z}}$ est bornée, ce qui implique que $|\lambda| = 1$. Donc toutes les valeurs propres de $\varphi(z)$ sont de module 1.

- Utilisation du premier point

Posons $\psi : \mathbf{R}_+ \rightarrow GL_n(\mathbf{R}); t \mapsto \varphi(e^{it})$. Par le premier point, comme ψ est un morphisme continu de $\mathbf{R}_+$ dans $GL_n(\mathbf{C})$, il existe $A \in M_n(\mathbf{C})$ tel que pour tout $t \in \mathbf{R}$, $\psi(t) = e^{tA}$. Or, ψ étant à valeurs dans $GL_n(\mathbf{R})$, $A = \psi'(0)$ est réelle. Enfin, ψ est périodique de période 2π , donc $e^{2\pi A} = \operatorname{Id}$. Les valeurs propres complexes de A sont donc imaginaires pures.

- Dunford

On pose $A = D + N$ la décomposition de Dunford de A . En passant à l'exponentielle, puisque D et N commutent, $e^{2\pi A} = e^{2\pi D} e^{2\pi N}$. Or, comme D est diagonalisable et a les mêmes valeurs propres que A , $e^{2\pi D} = \text{Id}$. On en déduit que $e^{2\pi N} = \text{Id}$.

Montrons que $N = 0$. Par l'absurde, on suppose que ce n'est pas le cas. On a alors que $\text{Ker}(N^2) \neq \text{Ker}(N)$. Soit $X \in \text{Ker}(N^2) \setminus \text{Ker}(N)$. Alors,

$$e^{2\pi N} X = X + 2\pi N X \neq X,$$

ce qui est absurde. Donc $N = 0$ et A est diagonalisable de valeurs propres imaginaires purs. Comme A est réelle, ses valeurs propres sont deux-à-deux conjuguées et on a

$$A = P \text{diag}(ik_1, -ik_1, \dots, ik_r, -ik_r, 0, \dots, 0) P^{-1}, \quad P \in GL_n(\mathbf{C}), k_j \in \mathbf{Z}^*.$$

La conjugaison par une matrice étant continue, par passage à l'exponentielle, pour tout $t \in \mathbf{R}_+$,

$$e^{tA} = P \text{diag}(e^{tik_1}, e^{-itk_1}, \dots, e^{itk_r}, e^{-itk_r}, 1, \dots, 1) P^{-1}.$$

- Conclusion

Par les formules d'Euler, on effectue un changement de base qui nous donne $Q \in GL_n(\mathbf{C})$ indépendante de t telle que

$$e^{tA} = Q \text{diag}(R_{tk_1}, \dots, R_{tk_r}, 1, \dots, 1) Q^{-1}.$$

Notons B_t la matrice conjuguée à e^{tA} . On va montrer que l'on peut prendre en réalité Q dans $GL_n(\mathbf{R})$. Notons $Q = Q_1 + iQ_2$. Alors,

$$\begin{cases} e^{tA} Q_1 &= Q_1 B_t, \\ e^{tA} Q_2 &= Q_2 B_t. \end{cases}$$

En notant $P(x) = \det(Q_1 + xQ_2)$, on a un polynôme non nul sur $\mathbf{C}$ donc avec un nombre fini de racines. Comme $\mathbf{R}$ est infini, il existe x tel que $P(x) \neq 0$ et en posant $Q_x = Q_1 + xQ_2$, on obtient $Q_x \in GL_n(\mathbf{R})$, indépendante de t , telle que pour tout $t \in \mathbf{R}_+$,

$$e^{tA} = Q_x \text{diag}(R_{tk_1}, \dots, R_{tk_r}, 1, \dots, 1) Q_x^{-1}.$$

- Réciproque

On vérifie que $e^{it} \mapsto QBQ^{-1}$ est bien un morphisme de groupes continus.

1. L'application est bien définie car R_{tk} ne dépend que de $t[2\pi]$.
2. C'est un morphisme car $R_{(t+t')k} = R_{tk} R_{t'k}$.
3. C'est continu car $\left| e^{ikt} - e^{ikt'} \right| \leq |k| \left| e^{it} - e^{it'} \right|$, donc ça fonctionne aussi pour cos et sin, et a fortiori pour les R_{tk} .

Donc tout est bon.

22 Codiagonalisation d'une famille d'endomorphismes

Leçons : 155

Référence: Algèbre linéaire, Cognet

Proposition — Si $v \in \text{End}(E)$ commute avec u et si u et v sont diagonalisables, alors ils sont diagonalisables dans une même base (ou codiagonalisables).

Soient $u_1, \dots, u_p$ sont des endomorphismes diagonalisables qui commutent deux à deux, alors ils sont codiagonalisables.

Proposition — Supposons que $\mathbf{K}$ est de caractéristique nulle. Soit A une sous-algèbre de $\text{End}(E)$ contenant Id et dont le seul élément nilpotent est 0. Alors il existe une base de E formée de vecteurs propres communs pour tous les endomorphismes de A .

• Démonstration du premier point

Comme u et v commutent, les sous-espaces propres de l'un sont stables par l'autre. Soient donc $\lambda \in \text{Sp}(u)$ et $E_u(\lambda)$ le sous-espace propre associé. On considère v' l'endomorphisme induit par v sur $E_u(\lambda)$. Comme le polynôme minimal de v est à racines simples (v est diagonalisable), le polynôme minimal de v' , qui divise celui de v , est forcément scindé à racines simples. Ainsi v' est-il diagonalisable. On considère donc une base $\mathcal{B}_\lambda$ de $E_u(\lambda)$ constituée de vecteurs propres de v' (donc de v). Cette base diagonalise également l'endomorphisme induit par u sur son espace propre, à savoir $\lambda \text{Id}_{E_u(\lambda)}$. Comme $E = \bigoplus_{\lambda \in \text{Sp}(u)} E_u(\lambda)$, en complétant les vecteurs de chaque base par des 0

et en considérant la concaténée des bases, on obtient une base qui diagonalise simultanément u et v .

• Cas d'une famille finie d'endomorphismes qui commutent deux-à-deux

On raisonne par récurrence sur le nombre p d'endomorphismes considérés.

Si $p = 1$, le résultat est évident en prenant une base de diagonalisation de l'endomorphisme. Le cas $p = 2$ a été traité plus tôt.

Supposons la propriété vraie au rang k , montrons qu'elle est toujours vraie au rang $k + 1$.

Posons $u = u_{k+1}$. Pour tout $j \in \llbracket 1, k \rrbracket$, u_j et u commutent donc les sous-espaces stables de u sont stables par tous les u_j . On pose donc u'_j les endomorphismes induits par les u_j sur $E_u(\lambda)$, $\lambda \in \text{Sp}(u)$. Ces k endomorphismes commutent deux-à-deux donc il existe une base de diagonalisation simultanée $\mathcal{B}(\lambda)$ constituée de vecteurs propres pour les endomorphismes $(u'_j)_{j=1, \dots, k}$. En concaténant les bases comme au point précédent, on obtient l'hérédité et on peut conclure.

• Cas d'une famille infinie

Soit $(u_i)_{i \in I}$ une famille d'endomorphismes commutant deux-à-deux et tous diagonalisables. Posons $F = \text{Vect}(u_i, i \in I)$. F est de dimension finie comme sous-espace de $\text{End}(E)$, qui est de dimension finie. On peut donc considérer une base $(u_1, \dots, u_p)$ de cet espace, et les codiagonaliser par le point précédent.

• Preuve de la deuxième proposition

Soit $u \in \text{End}(E)$. On commence par montrer que u est diagonalisable.

Soit $\pi_u = \prod_{i=1}^p (X - \lambda_i)^{m_i}$ le polynôme minimal de u . Posons $m = \max m_i$ et $P = \prod_{i=1}^p (X - \lambda_i)$. Alors, $P(u) \in \mathcal{A}$ et $P(u)^m = 0$ donc $P(u)$ est nilpotent. Donc $P(u) = 0$ donc toutes les racines du polynôme minimal sont simples et u est diagonalisable.

Posons $L_u : \text{End}(E) \rightarrow \text{End}(E); v \mapsto uv - vu$. Soit $B = (e_1, \dots, e_n)$ une base de E formée de vecteurs propres pour u , on note λ_j la valeur propre de u associée au vecteur propre e_j . On pose $(e_{i,j})$ la base de $\text{End}(E)$ canoniquement associée à la base $B : e_{i,j}(e_k) = \delta_{j,k}e_i$. On en déduit que pour tout $(i, j) \in \llbracket 1, n \rrbracket^2$,

$$L_u(e_{i,j}) = u \circ e_{i,j} - e_{i,j} \circ u = (\lambda_j - \lambda_i)e_{i,j}.$$

On a donc une base de $\text{End}(E)$ constituée de vecteurs propres pour $L_u : L_u$ est diagonalisable.

Posons à présent L'_u l'endomorphisme induit par L_u sur A . Soit λ une valeur propre de L'_u et v un vecteur propre associé. Pour tout $p \in \mathbf{N}$,

$$L'_u(v^{p+1}) = L'_u(v^p) \circ v + v^p \circ L'_u(v).$$

Par une récurrence immédiate, on voit que $L'_u(v^p) = \lambda p v^p$. Or, v étant diagonalisable et non nul, il n'est pas nilpotent, donc v^p est un vecteur propre associé à la valeur propre λp . Or, $\text{Sp}(L'_u)$ est un ensemble fini, donc nécessairement, $\lambda = 0$. Donc, $\text{Sp}(L'_u) = \{0\}$.

Comme L_u est diagonalisable, L'_u l'est aussi, donc $L'_u = 0$ et tout élément de A commute avec u . Par le point précédent, il existe une base de A constituée de vecteurs propres communs à tous les endomorphismes.

23 Séries de Hardy

Leçons : 230

Référence: Oraux X-ENS, Analyse 1, Francinou, Gianella, Nicolas

Proposition — *L a série de Hardy $\sum_{n \geq 1} \frac{\sin(\pi\sqrt{n})}{n^\alpha}$:*

1. *Converge absolument si $\alpha > 1$,*
2. *Converge si $\frac{1}{2} < \alpha \leq 1$,*
3. *Diverge pour $\alpha = \frac{1}{2}$,*
4. *Diverge pour $\alpha < \frac{1}{2}$.*

Notons u_n le terme général de la série de Hardy.

- Cas $\alpha > 1$

Pour tout $n \in \mathbf{N}^*$, $|u_n| \leq \frac{1}{n^\alpha}$ et comme $\alpha > 1$, la série de terme général $\frac{1}{n^\alpha}$ converge. On a donc convergence absolue de la série.

- Cas $\frac{1}{2} < \alpha \leq 1$

On considère l'intégrale $\int_1^\infty \frac{\sin(\pi\sqrt{t})}{t^\alpha} dt = \lim_{x \rightarrow +\infty} \int_1^x \frac{\sin(\pi\sqrt{t})}{t^\alpha} dt$. Soit $x \geq 1$. En effectuant le changement de variables $u = \sqrt{t}$, on obtient que

$$\begin{aligned} \int_1^x \frac{\sin(\pi\sqrt{t})}{t^\alpha} dt &= 2 \int_1^{\sqrt{x}} \frac{\sin(\pi u)}{u^{2\alpha-1}} du, \\ &= 2 \left[-\frac{\cos(\pi u)}{\pi u^{2\alpha-1}} \right]_1^{\sqrt{x}} - \frac{2(2\alpha-1)}{\pi} \int_1^{\sqrt{x}} \frac{\cos(\pi u)}{u^{2\alpha}} du, \\ &\xrightarrow{x \rightarrow +\infty} -\frac{2}{\pi} - \frac{2(2\alpha-1)}{\pi} \int_1^\infty \frac{\cos(\pi u)}{u^{2\alpha}} du, \end{aligned}$$

car la fonction $u \mapsto \frac{\cos(\pi u)}{u^{2\alpha}}$ est intégrable sur $[1, +\infty[$ ($2\alpha > 1$).

Posons, pour tout $n \in \mathbf{N}^*$, $v_n = \int_n^{n+1} \frac{\sin(\pi\sqrt{t})}{t^\alpha} dt$. Par le calcul effectué juste avant, on sait que la série de terme général v_n converge. On va donc montrer que la série de terme général $u_n - v_n$ converge. Posons, pour tout $t \in [1, \infty[$, $\varphi(t) = \frac{\sin(\pi\sqrt{t})}{t^\alpha}$ pour $t \geq 1$. On a alors que pour tout $n \in \mathbf{N}^*$,

$$|u_n - v_n| = \left| \int_n^{n+1} (\varphi(t) - \varphi(n)) dt \right| \leq \int_n^{n+1} |\varphi(t) - \varphi(n)| dt.$$

Comme φ est de classe $\mathcal{C}^1$ (et même lisse) sur $[1, +\infty[$, de dérivée

$$\varphi'(t) = \frac{\frac{\pi}{2\sqrt{t}} \cos(\pi\sqrt{t}) t^\alpha - \alpha t^{\alpha-1} \sin(\pi\sqrt{t})}{t^{2\alpha}} = O\left(\frac{1}{t^{\alpha+\frac{1}{2}}}\right),$$

on majore

$$|\varphi'(t)| \leq \frac{K}{n^{\alpha+\frac{1}{2}}}$$

avec K positive. Par le théorème des accroissements finis, $|u_n - v_n| \leq \frac{K}{n^{\alpha+\frac{1}{2}}}$ et la série converge absolument par théorème de comparaison des séries à termes positifs. On en déduit la convergence de la série de Hardy converge.

- Cas $\alpha = \frac{1}{2}$

On calcule le développement asymptotique de $d_n = e^{i\pi\sqrt{n+1}} - e^{i\pi\sqrt{n}}$:

$$\begin{aligned}
d_n &= e^{i\pi\sqrt{n}}(e^{i\pi(\sqrt{n+1}-\sqrt{n})} - 1), \\
&= e^{i\pi\sqrt{n}}(e^{i\pi\sqrt{n}(\sqrt{1+\frac{1}{n}}-1)} - 1), \\
&= e^{i\pi\sqrt{n}}(e^{i\pi\sqrt{n}(\frac{1}{2n}+O(\frac{1}{n^2}))} - 1), \\
&= e^{i\pi\sqrt{n}}(e^{i\pi\sqrt{n}(\frac{1}{2\sqrt{n}}+O(\frac{1}{n^{\frac{3}{2}}}))} - 1), \\
&= e^{i\pi\sqrt{n}}\left(\frac{i\pi}{2\sqrt{n}} - \frac{\pi^2}{8n} + O\left(\frac{1}{n^{\frac{3}{2}}}\right)\right), \\
&= \frac{i\pi e^{i\pi\sqrt{n}}}{2\sqrt{n}} - \frac{\pi^2 e^{i\pi\sqrt{n}}}{8n} + O\left(\frac{1}{n^{\frac{3}{2}}}\right).
\end{aligned}$$

En prenant la partie réelle, on obtient alors que

$$\cos(\pi\sqrt{n+1}) - \cos(\pi\sqrt{n}) = -\frac{\pi \sin(\pi\sqrt{n})}{2\sqrt{n}} - \frac{\pi^2 \cos(\pi\sqrt{n})}{8n} + O\left(\frac{1}{n^{\frac{3}{2}}}\right).$$

Comme la série de terme général $O\left(\frac{1}{n^{\frac{3}{2}}}\right)$ converge absolument, et que, comme pour le sinus auparavant, on peut montrer que la série de terme général $\frac{\cos(\pi\sqrt{n})}{n}$ converge, on a que la série de terme général $\frac{\sin(\pi\sqrt{n})}{\sqrt{n}}$ est de même nature que la série de terme général $\cos(\pi\sqrt{n+1}) - \cos(\pi\sqrt{n})$. Par télescopage, on voit que cette série ne converge pas (la suite extraite n^2 donne $(-1)^n$ qui ne converge pas), donc on a divergence de la série de Hardy pour $\alpha = \frac{1}{2}$.

- Cas $\alpha < \frac{1}{2}$

Supposons par l'absurde que la série converge. On note A_n la somme partielle d'ordre n de la série de Hardy. Par une transformation d'Abel,

$$\begin{aligned}
\sum_{k=1}^n \frac{\sin(\pi\sqrt{k})}{\sqrt{k}} &= \sum_{k=1}^n \frac{\sin(\pi\sqrt{k})}{k^\alpha} \frac{1}{k^{\frac{1}{2}-\alpha}}, \\
&= \sum_{k=1}^n (A_k - A_{k-1}) \frac{1}{k^{\frac{1}{2}-\alpha}}, \\
&= \sum_{k=1}^n \frac{A_k}{k^{\frac{1}{2}-\alpha}} - \sum_{k=0}^{n-1} \frac{A_k}{k^{\frac{1}{2}-\alpha}}, \quad (A_0 = 0), \\
&= \frac{A_n}{n^{\frac{1}{2}-\alpha}} + \sum_{k=1}^{n-1} A_k \left(\frac{1}{k^{\frac{1}{2}-\alpha}} - \frac{1}{(k+1)^{\frac{1}{2}-\alpha}} \right).
\end{aligned}$$

La suite (A_n) étant bornée, le premier terme converge vers 0. Le second terme est la somme partielle d'une série absolument convergente (en utilisant encore une fois le caractère borné de la suite (A_n)). On a donc convergence de la série $\sum_{n \geq 1} \frac{\sin(\pi\sqrt{n})}{\sqrt{n}}$, ce qui est absurde car sa divergence a été prouvée au point précédent.

Au total, la série de Hardy converge si et seulement si $\alpha > \frac{1}{2}$.

24 Permutations, convergence et somme

Leçons : 230

Référence: Un max de maths, Zavidovique

Définition — Soit σ une permutation de $\mathbf{N}$. Pour tout $n \in \mathbf{N}$, on peut écrire $\{\sigma(0), \dots, \sigma(n)\}$ comme une union disjointe de "paquets" :

$$\{\sigma(0), \dots, \sigma(n)\} = \llbracket c_1^n, d_1^n \rrbracket \cup \dots \cup \llbracket c_{b_n}^n, d_{b_n}^n \rrbracket$$

avec $c_i^n \leq d_i^n \leq c_{i+1}^n - 2$. Notons finalement $M_n = d_{b_n}^n + 1$.

- On dit que σ est paquet-bornée si la suite $(b_n)_{n \in \mathbf{N}}$ est bornée.
- On dit que σ conserve la convergence si pour toute série réelle convergente $\sum_{n \geq 0} u_n$, la série $\sum_{n \geq 0} u_{\sigma(n)}$ converge.
- On dit que σ conserve la somme si elle préserve la convergence et que pour toute série réelle convergente $\sum_{n \geq 0} u_n$, $\sum_{n=0}^{\infty} u_n = \sum_{n=0}^{\infty} u_{\sigma(n)}$.

Proposition — Une permutation préserve la somme si et seulement si elle préserve la convergence.

- Montrer que toute permutation paquet-bornée préserve la somme.

Soit σ une permutation de $\mathbf{N}$ paquet-bornée. Soit $\sum_{n \geq 0} u_n$ une série convergente, de somme $l \in \mathbf{R}$. On note $(S_n)_{n \in \mathbf{N}}$ la suite de ses sommes partielles.

Comme σ est surjective, pour n assez grand (supérieur à $\sigma^{-1}(0)$), on a $c_1^n = 0$. On peut donc écrire

$$\sum_{k=0}^n u_{\sigma(k)} = \sum_{k=c_1^n}^{d_1^n} u_k + \sum_{i=2}^{b_n} \sum_{k=c_i^n}^{d_i^n} u_k = S_{d_1^n} + \sum_{i=2}^{b_n} (S_{d_i^n} - S_{c_i^n-1}).$$

Or, comme $d_1^n \xrightarrow{n \rightarrow +\infty} +\infty$, il en va de même pour tous les d_i^n et c_i^n . Comme b_n est borné, on peut passer à la limite dans l'égalité précédente et obtenir que

$$\lim_{n \rightarrow +\infty} \sum_{k=0}^n u_{\sigma(k)} = \lim_{n \rightarrow +\infty} (S_{d_1^n} + \sum_{i=2}^{b_n} (S_{d_i^n} - S_{c_i^n-1})) = l + \sum_{i=2}^{b_n} (l - l) = l.$$

Ainsi σ préserve-t-elle la somme.

- Toute permutation qui préserve la convergence est paquet-bornée.

On raisonne par contraposée. Supposons que σ soit une permutation de $\mathbf{N}$ qui n'est pas paquet-bornée. On dispose encore d'un entier n_1 à partir duquel $c_1^n = 0$. On définit alors, pour $k \leq M_{n_1} = d_{b_{n_1}}^{n_1} + 1$,

$$u_k = \begin{cases} 1 & \text{si } k = d_i^{n_1} \text{ pour un certain } i \in \llbracket 1, b_{n_1} \rrbracket, \\ -1 & \text{si } k = d_i^{n_1} + 1 \text{ pour un certain } i \in \llbracket 1, b_{n_1} \rrbracket, \\ 0 & \text{sinon.} \end{cases}$$

On remarque que

$$\sum_{i=0}^{n_1} u_{\sigma(i)} = \sum_{k=1}^{b_{n_1}} \sum_{i=c_k^{n_1}}^{d_k^{n_1}} u_i = b_{n_1} \text{ geqslant } 1,$$

alors que $\sum_{i=0}^{M_{n_1}} u_i = 0$. De plus, pour tout $n \leq M_{n_1}$, $\sum_{i=0}^n u_i$ vaut soit 0 soit 1.

On procède ensuite par récurrence. Supposons que l'on a construit une famille $(n_i)_{1 \leq i \leq j-1}$ telle que pour tout $i \in \llbracket 1, j-1 \rrbracket$,

$$\sum_{k=0}^{n_i} u_{\sigma(k)} \geq i \text{ et } \sum_{k=0}^{M_{n_i}} u_k = 0.$$

À l'étape j , comme (b_n) n'est pas bornée, on choisit un entier n_j suffisamment grand pour avoir $d_{n_j}^1 > M_{n_{j-1}}$ et $b_{n_j} \geq j^2$. Pour tout $k \in \llbracket M_{n_{j-1}}, M_{n_j} \rrbracket$, on définit

$$u_k = \begin{cases} \frac{1}{j} & \text{si } k = d_i^{n_j} \text{ pour un certain } i \in \llbracket 1, b_{n_j} \rrbracket, \\ -\frac{1}{j} & \text{si } k = d_i^{n_j} + 1 \text{ pour un certain } i \in \llbracket 1, b_{n_j} \rrbracket, \\ 0 & \text{sinon.} \end{cases}$$

On a bien que

$$\sum_{k=0}^{n_j} u_k = \sum_{l=0}^{M_{n_{j-1}}} u_l + \sum_{k=M_{n_{j-1}}+1}^{d_1^{n_j}} u_k + \sum i = 2^{b_{n_j}} \sum_{k=c_i^{n_j}}^{d_i^{n_j}} u_k = \frac{b_{n_j}}{j} \leq j,$$

alors que $\sum_{k=0}^n u_k$ vaut soit 0 soit $\frac{1}{j}$ pour tout $n \in \llbracket 0, M_{n_j} \rrbracket$. On a bien construit le terme général d'une série convergente alors que la série des permutés diverge grossièrement.

- Conclusion

On a montré que si une permutation préserve la convergence, alors elle est paquet-bornée, donc elle préserve la somme.

Comme il est évident que si une permutation préserve la somme, alors elle préserve la convergence, on a équivalence des deux notions. De plus, les seules permutations à vérifier ces propriétés sont les permutations paquet-bornées.

25 Théorème de Lévy et application au théorème central limite (non rédigé)

Leçons : 261,262

Référence: Analyse pour l'agrégation, Queffelec, Zuily

Théorème — (Lévy) Soient $X_1, \dots, X_n$ des variables aléatoires réelles.

1. Si X est une variable aléatoire réelle, on a équivalence entre :

- X_n converge en loi vers X ;
- φ_{X_n} converge simplement vers φ_X .

2. Si φ_{X_n} converge simplement vers ψ , avec ψ continue, alors ψ est la fonction caractéristique d'une variable aléatoire X et X_n converge en loi vers X .

Théorème — (Central Limite) Soient X_n des variables aléatoires réelles i.i.d, d'espérance μ et d'écart-type

σ . Posons $S_n = \sum_{k=1}^n X_k$.

Alors, $\frac{S_n - n\mu}{\sqrt{n}\sigma}$ converge en loi vers une variable aléatoire de loi $\mathcal{N}(0, 1)$.

Preuve du théorème de Lévy

• Preuve du premier point

Supposons que X_n converge en loi vers X .

Par définition, pour toute fonction $f \in \mathcal{C}_b$ (continue bornée), $E[f(X_n)] \xrightarrow{n \rightarrow +\infty} E[f(X)]$. Comme, pour tout $t \in \mathbf{R}$, $f_t : x \rightarrow e^{-ixt}$ est continue bornée,

$$\varphi_{X_n}(t) = E[f_t(X_n)] \xrightarrow{n \rightarrow +\infty} E[f_t(X)] = \varphi_X(t).$$

Supposons à présent que la suite des fonctions caractéristiques converge simplement vers φ_X . Soit $f \in L^1(\mathbf{R})$, posons $g = \hat{f}$ sa transformée de Fourier. g est continue et bornée par construction. Alors, par un théorème de Fubini,

$$\begin{aligned} E[g(X_n)] &= \int_{\mathbf{R}} \left(\int_{\mathbf{R}} e^{-itx} f(t) dt \right) dx, \\ &= \int_{\mathbf{R}} f(t) \left(\int_{\mathbf{R}} e^{-itx} dx \right) dt, \\ &= \int_{\mathbf{R}} f(t) \varphi_{X_n}(-t) dt. \end{aligned}$$

Par le théorème de convergence de dominée, on obtient alors que $E[g(X_n)] \xrightarrow{n \rightarrow +\infty} E[g(X)]$. Cela est en particulier vrai pour les fonctions $s \in \mathcal{S}(\mathbf{R})$ (espace de Schwarz), qui est laissé stable par la transformée de Fourier. Comme l'espace de Schwarz est dense dans $(\mathcal{C}_0(\mathbf{R}), \|\cdot\|_\infty)$, on obtient que pour tout $f \in \mathcal{C}_0(\mathbf{R})$, (continues nulles en l'infini), par des inégalités triangulaires,

$$E[f(X_n)] \xrightarrow{n \rightarrow +\infty} E[f(X)].$$

Donc la suite $(X_n)_{n \in \mathbf{N}}$ converge en loi vers X .

• Preuve du second point

Pas utile pour montrer le TCL ! on y reviendra si on voit qu'il manque du temps.

Preuve du Théorème central limite.

• Petit lemme préliminaire

Lemme — Soit $(z_n)_{n \in \mathbb{N}}$ une suite de complexes de limite $z \in \mathbb{C}$. Alors

$$\lim_{n \rightarrow +\infty} \left(1 + \frac{z_n}{n}\right)^n = e^z.$$

Commençons par étudier la fonction $e^z - \left(1 + \frac{z}{n}\right)^n$ pour $z \in \mathbb{C}$. Pour n suffisamment grand (plus grand que $|z|$), on a la décomposition en série entière :

$$e^z - \left(1 + \frac{z}{n}\right)^n = \sum_{k=0}^{\infty} a_k^{(n)} z^k,$$

$$\text{avec } a_k^{(n)} = \begin{cases} \frac{1}{k!} \left(1 - \frac{n(n-1) \dots (n-k+1)}{n^k}\right) & \text{si } k \leq n, \\ \frac{1}{k!} & \text{sinon.} \end{cases}.$$

Dans tous les cas, $a_k^{(n)} \geq 0$. En posant $r = |z|$, on en déduit que

$$\begin{aligned} \left| e^z - \left(1 + \frac{z}{n}\right)^n \right| &\leq \sum_{k=0}^{\infty} a_k^{(n)} r^k, \\ &\leq e^r - \left(1 + \frac{r}{n}\right)^n, \\ &\leq e^r - e^{n \ln\left(1 + \frac{r}{n}\right)}, \\ &\leq e^r - \exp\left[n \left(\frac{r}{n} - \frac{r^2}{2n^2}\right)\right], \\ &\leq e^r \left[1 - e^{-\frac{r^2}{2n}}\right], \\ &\leq \frac{r^2}{2n} e^r. \end{aligned}$$

Dans notre cas, par une inégalité triangulaire,

$$\begin{aligned} \left| e^z - \left(1 + \frac{z_n}{n}\right)^n \right| &\leq |e^z - e^{z_n}| + \left| e^{z_n} - \left(1 + \frac{z_n}{n}\right)^n \right|, \\ &\leq |e^z - e^{z_n}| + \frac{|z_n|^2 e^{|z_n|}}{2n}, \\ &\leq |e^z - e^{z_n}| + O\left(\frac{1}{n}\right). \end{aligned}$$

En laissant tendre n vers l'infini, on a bien la convergence de $\left(1 + \frac{z_n}{n}\right)^n$ vers e^z .

• Preuve du TCL

On peut supposer $\mu = 0$ et $\sigma = 1$ sans perdre de généralité. Notons φ la fonction caractéristique de X_1 (donc de tout X_n car elles sont identiquement distribuées). Comme les (X_n) admettent des moments d'ordre 2, φ est de classe $\mathcal{C}^2$ et on a $\varphi'(0) = E[iX] = 0$ et $\varphi''(0) = E[-X^2] = -1$. De plus, par indépendance et identique distribution,

$$E \left[e^{it \frac{S_n}{\sqrt{n}}} \right] = E \left[\prod_{k=1}^n e^{it \frac{X_k}{\sqrt{n}}} \right] = \prod_{k=1}^n E \left[e^{it \frac{X_k}{\sqrt{n}}} \right] = \left(\varphi \left(\frac{t}{\sqrt{n}} \right) \right)^n.$$

Par un développement de Taylor en 0, à t fixé,

$$\varphi \left(\frac{t}{\sqrt{n}} \right) = \varphi(0) - \frac{t^2}{2n} + \frac{\varepsilon_n}{n},$$

où $\varepsilon_n \xrightarrow[n \rightarrow +\infty]{} 0$.

En appliquant le lemme à $z_n = -\frac{t^2}{2} + \varepsilon$, on a que

$$\left(\varphi \left(\frac{t}{\sqrt{n}} \right) \right)^n \xrightarrow[n \rightarrow +\infty]{} e^{-\frac{t^2}{2}}.$$

On reconnaît dans le terme de droite la fonction caractéristique d'une variable aléatoire de loi $\mathcal{N}(0, 1)$. Par le théorème de Lévy, on a la convergence en loi de $\frac{S_n}{\sqrt{n}}$ vers une variable aléatoire X de loi normale.

26 Borel-Cantelli et application aux nombres premiers

Ref : maths agreg ; si on parle de la fonction zeta de Riemann, elle peut se recaser à la 265 en sus.

Leçons : 266

Référence: De l'intégration aux probabilités, Garet, Kurtzmann

Proposition — On munit $\mathbf{N}^*$ de la tribu totale $\mathcal{P}(\mathbf{N}^*)$ et on pose, pour tout $n \in \mathbf{N}^*$, l'événement $A(n) = n\mathbf{N}^*$ "être multiple de n ".

Il n'existe pas de mesure de probabilité $\mathbb{P}$ sur $\mathbf{N}^*$ "bien répartie" au sens où $\mathbb{P}(A(n)) = \frac{1}{n}$ pour tout $n \in \mathbf{N}^*$.

Notons, pour $s \in]1, +\infty[$, $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ la fonction zêta de Riemann. On définit une mesure $\mathbb{P}$ par $\mathbb{P}(\{x\}) = \frac{1}{\zeta(s)} x^{-s}$ pour $x \in \mathbf{N}^*$.

- $\mathbb{P}$ est une mesure de probabilités

$\mathbb{P}$ est une mesure par construction, on va donc montrer que $\mathbb{P}(\mathbf{N}^*) = 1$.

Soit $p \in \mathbf{N}^*$. On écrit $p\mathbf{N}^* = \bigcup_{k=1}^{\infty} \{pk\}$. Comme la réunion est disjointe,

$$\begin{aligned} P(p\mathbf{N}^*) &= \sum_{k=1}^{\infty} \mathbb{P}(\{pk\}), \\ &= \frac{1}{\zeta(s)} \frac{1}{p^s} \sum_{k=1}^{\infty} \frac{1}{k^s}, \\ &= \frac{1}{p^s}. \end{aligned}$$

En prenant $p = 1$, $\mathbb{P}(\mathbf{N}^*) = 1$. On a bien une mesure de probabilités.

- Si $p_1, \dots, p_k$ sont premiers distincts, alors $A(p_1), \dots, A(p_k)$ donc indépendants.

En particulier, les p_i sont premiers entre eux, donc

$$\bigcap_{i=1}^k A(p_i) = \bigcap_{i=1}^k p_i \mathbf{N}^* = \left(\prod_{i=1}^k p_i \right) \mathbf{N}^*.$$

On en déduit que

$$\mathbb{P} \left(\bigcap_{i=1}^k A(p_i) \right) = \mathbb{P} \left(\left[\prod_{i=1}^k p_i \right] \mathbf{N}^* \right) = \frac{1}{\left(\prod_{i=1}^k p_i \right)^s} = \prod_{i=1}^k \mathbb{P}(A(p_i)).$$

On a l'indépendance des événements.

- Notons $(p_k)_{k \in \mathbf{N}^*}$ la suite des nombres premiers et on note $A_k = A(p_k)$. Alors $\frac{1}{\zeta(s)} = \lim_{n \rightarrow +\infty} \prod_{k=1}^n \mathbb{P}(A_k^c)$.

On regarde l'événement $\bigcap_{k=1}^{\infty} A_k^c$. C'est l'ensemble des nombres entiers naturels non nuls qui ne sont multiples d'aucun nombre premier. Le seul nombre qui vérifie cela est 1, donc

$$\{1\} = \bigcap_{k=1}^{\infty} A_k^c.$$

Posons $B_n = \bigcap_{k=1}^n A_k^c$ pour tout $n \in \mathbf{N}^*$. La suite $(B_n)_{n \geq 1}$ est décroissante et son intersection vaut $\{1\}$. Par le théorème de **continuité monotone ? à vérifier**,

$$\lim_{n \rightarrow +\infty} \mathbb{P}(B_n) = \mathbb{P}(\{1\}) = \frac{1}{\zeta(s)}.$$

D'où le résultat par indépendance des A_k^c .

- La série de terme général $\frac{1}{p_k}$ diverge.

Par le point précédent, on a

$$\frac{1}{\zeta(s)} = \lim_{n \rightarrow +\infty} \prod_{k=1}^n (1 - p_k^{-s}).$$

Par continuité de $x \rightarrow -\ln(x)$,

$$\ln(\zeta(s)) = -\ln\left(\frac{1}{\zeta(s)}\right) = \lim_{n \rightarrow +\infty} \sum_{k=1}^n -\ln\left(1 - \frac{1}{p_k^s}\right).$$

Or, pour tout $s > 1$, $\zeta(s) \geq \sum_{k=1}^n \frac{1}{k^s}$, donc

$$\liminf_{s \rightarrow 1^+} \zeta(s) \geq \liminf_{s \rightarrow 1^+} \sum_{k=1}^n \frac{1}{k^s} = \lim_{s \rightarrow 1^+} \sum_{k=1}^n \frac{1}{k^s} = \sum_{k=1}^n \frac{1}{k}.$$

Par divergence de la série harmonique, on voit donc que pour tout $A \in \mathbf{R}_+$, il suffit de prendre un n suffisamment élevé pour avoir $\liminf_{s \rightarrow 1^+} \zeta(s) \geq A$. Donc $\liminf_{s \rightarrow 1^+} \zeta(s) = +\infty$.

Soit $A \in \mathbf{R}_+$. Grâce au calcul effectué précédemment, il existe $s \in]1, +\infty[$ tel que $\zeta(s) > e^A$. Ainsi,

$$\sum_{k=1}^{\infty} -\ln\left(1 - \frac{1}{p_k}\right) \geq \sum_{k=1}^{\infty} -\ln\left(1 - \frac{1}{p_k^s}\right) > A$$

. Comme A est quelconque, la série de terme général $-\ln\left(1 - \frac{1}{p_k}\right)$ diverge.

Or, puisque $-\ln\left(1 - \frac{1}{p_k}\right) \underset{k \rightarrow +\infty}{\sim} \frac{1}{p_k}$, que la série diverge et est à termes positifs, par théorèmes de sommation des relations d'équivalence pour les séries à termes positifs, on a la divergence de la série de terme général $\frac{1}{p_k}$.

• Conclusion

Supposons par l'absurde qu'il existe une loi de probabilité μ qui fonctionne. En procédant comme précédemment, les événements A_k sont indépendants sous μ , donc leurs complémentaires le sont aussi.

Soient $l > n \geq 1$ des entiers. Comme $\{n\} \subset \bigcap_{i=n}^l A_k^c$ ($p_i > i \forall i \in \mathbf{N}^*$),

$$\mu(\{n\}) \leq \prod_{i=n}^l \mu(A_i^c).$$

Or, $\lim_{l \rightarrow +\infty} \prod_{i=n}^l \left(1 - \frac{1}{p_i}\right) = 0$, car si on en prend le logarithme, cela tend par le point précédent vers $-\infty$. On en déduit que pour tout $n \geq 1$,

$$\mu(\{n\}) = 0.$$

Comme μ est une loi de probabilités, on a forcément $\mu = \delta_0$, ce qui est absurde car on avait supposé que $\mu(2\mathbf{N}^*) = \frac{1}{2}$.

Il n'existe donc pas de loi de probabilités sur $\mathbf{N}^*$ qui vérifie $\mu(n\mathbf{N}^*) = \frac{1}{n}$.

27 Équation de la chaleur

Commentaires : on parle de dérivées partielles sur un fermé, voir les valeurs aux bords comme des limites à droite ou à gauche (à mentionner).

Comprendre pourquoi on prend u continue et qu'ensuite on détaille à outrance le bordel. Regarder aussi pourquoi parfois on inclut l'infini et parfois non

Leçons : 209, 222, 241, 246, 247

Référence: Analyse pour l'agrégation de mathématiques, Bernis

Théorème — Soit $f \in \mathcal{C}^1([0, 1], \mathbf{R})$ telle que $f(0) = f(\pi) = 0$. Il existe une unique application $u : \mathbf{R}_+ \times [0, \pi] \rightarrow \mathbf{R}$, $(t, x) \mapsto u(t, x)$ continue telle que :

1. $\partial_x u$ et $\partial_t u$ existent et sont continues sur $\mathbf{R}_+^* \times [0, \pi]$,
2. $\partial_x^2 u$ existe et est continue sur $\mathbf{R}_+^* \times [0, \pi]$,
3. $\forall t \in \mathbf{R}_+$, $u(t, 0) = u(t, \pi)$,
4. $\forall (t, x) \in \mathbf{R}_+^* \times [0, \pi]$, $\partial_t u(t, x) = \partial_x^2 u(t, x)$,
5. $\forall x \in [0, \pi]$, $u(0, x) = f(x)$.

Démonstration de l'existence

- Séparation des variables

Soit u une application non identiquement nulle de la forme $u(t, x) = T(t)X(x)$ avec $T \in \mathcal{C}^1(\mathbf{R}_+, \mathbf{R})$ et $X \in \mathcal{C}^2([0, \pi], \mathbf{R})$. Cette application est clairement continue et vérifie les deux premières conditions (de dérivabilité). On va exhiber par analyse et synthèse des conditions sur X et T pour que u vérifie les points 3 et 4 de l'énoncé.

Supposons que u vérifie ces points. Par 4, pour tout $(t, x) \in \mathbf{R}_+^* \times [0, \pi]$,

$$X(x)T'(t) = X''(x)T(t).$$

Comme u est non identiquement nulle, il existe un point $(t_0, x_0 \in \mathbf{R}_+ \times]0, \pi[$ où elle est non nulle. Par continuité de u , on prend $t_0 > 0$. Alors, $X(x_0)$ et $T(t_0)$ sont non nuls, donc on obtient

$$\begin{cases} X''(x) &= \frac{T'(t_0)}{T(t_0)} X(x), \quad \forall x \in [0, \pi], \\ T'(t) &= \frac{X''(x_0)}{X(x_0)} T(t), \quad \forall t \in \mathbf{R}_+^*. \end{cases}$$

En regardant les égalités ci-dessus en $t = t_0$, $x = x_0$, on obtient que $k := -\frac{T'(t_0)}{T(t_0)} = -\frac{X''(x_0)}{X(x_0)}$. Ainsi a-t-on, pour tout $(t, x) \in \mathbf{R}_+^* \times [0, \pi]$,

$$\begin{cases} X''(x) &= -kX(x), \\ T'(t) &= -kT(t). \end{cases}$$

Si $k < 0$, alors il existe $\alpha, \beta \in \mathbf{R}$ tels que

$$X(x) = \alpha \cosh(\sqrt{-k}x) + \beta \sinh(-\sqrt{-k}x).$$

Or, $X(0) = \alpha = 0$, et $X(\pi) = \beta \sinh(-\sqrt{-k}\pi) = 0$. Comme le sinus hyperbolique ne s'annule qu'en 0, $\beta = 0$ donc X est identiquement nulle, absurde car u est supposée non nulle.

Si $k = 0$, X est une application affine non nulle ce qui contredit les conditions au bord décrites en 3.

Si $k > 0$, alors il existe $\alpha, \beta \in \mathbf{R}$ non nuls tels que

$$X(x) = \alpha \cos(\sqrt{k}x) + \beta \sin(\sqrt{k}x).$$

Si l'on regarde les conditions au bord, on trouve $\alpha = 0$ et $\beta \sin(\sqrt{k}\pi) = 0$. Comme on ne veut pas de solution nulle, nécessairement il existe $n \in \mathbf{N}^*$ tel que $\sqrt{k} = n$ et donc,

$$X(x) = \beta \sin(nx)$$

. En résolvant l'équation de degré 1 dont T est solution, on obtient l'existence d'une constante $C \in \mathbf{R}^*$ telle que pour tout $(t, x) \in \mathbf{R}_+^* \times [0, \pi]$,

$$u(t, x) = C \sin(nx) e^{-n^2 t}.$$

Par continuité de u , l'égalité est toujours vérifiée sur $\mathbf{R}_+ \times [0, \pi]$.

Réciproquement, on vérifie qu'une telle fonction vérifie les quatre premiers points de l'énoncé. Dorénavant, on notera u_n l'application exhibée dans cette partie.

• Superposition des solutions

Comme $f(0) = 0$, on peut la prolonger à $[-\pi, \pi]$ en une fonction impaire. Comme $f(\pi) = 0 = f(-\pi)$, on peut la prolonger en une fonction $\tilde{f} \in \mathcal{C}^1$ par morceaux et 2π -périodique sur $\mathbf{R}$. On peut donc considérer sa série de Fourier réelle, $\sum_{n \geq 1} b_n \sin(nx)$. Plus précisément, on s'intéressera ici à la série $\sum_{n \geq 1} b_n u_n$.

Comme $\tilde{f}$ est continue et $\mathcal{C}^1$ par morceaux, la famille (b_n) est sommable (autrement dit $\sum_{n \geq 1} b_n$ est absolument convergente). De plus, pour tout $n \in \mathbf{N}^*$,

$$\|b_n u_n\|_\infty \leq |b_n|,$$

donc la série $\sum_{n \geq 1} b_n u_n$ converge normalement donc uniformément, on note S sa somme. La continuité des u_n nous assure ainsi la continuité de S sur $\mathbf{R}_+ \times [0, \pi]$.

On déduit de cette convergence que pour tout $t \in \mathbf{R}_+$, $S(t, 0) = S(t, \pi) = 0$. S vérifie donc les conditions au bord.

Soit $\varepsilon \in \mathbf{R}_+^*$.

- Pour tout $x \in [0, \pi]$, tout $t \in [\varepsilon, \infty]$ et tout $n \in \mathbf{N}^*$, $u_n(\cdot, x)$ est $\mathcal{C}^1$.
- Pour tout $x \in [0, \pi]$, tout $t \in [\varepsilon, \infty]$ et tout $n \in \mathbf{N}^*$,

$$|\partial_t (b_n u_n)(t, x)| \leq |b_n| n^2 \exp(-n^2 \varepsilon).$$

Or, comme $n^2 \exp(-n^2 \varepsilon)$ tend vers 0 quand n tend vers l'infini, le terme de droite devient un $O(b_n)$, or la série de terme général b_n converge absolument. On obtient donc la convergence normale de la série $\sum b_n \partial_t u_n(\cdot, x)$ sur $[\varepsilon, +\infty]$, et ce pour tout $x \in [0, \pi]$. Comme ε est quelconque, S est dérivable par rapport à t sur $\mathbf{R}_+^* \times [0, \pi]$ et $\partial_t S$ s'obtient en dérivant S terme-à-terme.

Enfin, comme les $b_n \partial_t u_n$ sont continues sur $\mathbf{R}_+^* \times [0, \pi]$, et que la majoration effectuée est indépendante de x et de t , on a la convergence normale de la série sur $[\varepsilon, +\infty] \times [0, \pi]$ et donc la continuité de $\partial_t S$.

On procède de même pour obtenir l'existence et la continuité de $\partial_x S$ et $\partial_x^2 S$, ainsi que leur expression (toujours par dérivation terme-à-terme) sur $\mathbf{R}_+^* \times [0, \pi]$. Comme l'équation de la chaleur est linéaire, on déduit du fait que les u_n vérifient le quatrième point que S le vérifie aussi.

Enfin, pour tout $x \in [0, \pi]$, $S(0, x)$ est la somme de la série de Fourier de $\tilde{f}$, donc comme cette dernière est continue et $\mathcal{C}^1$ par morceaux, le théorème de convergence normale nous donne que pour tout $x \in [0, \pi]$, $S(0, x) = f(x)$.
mais c'est aussi vrai pour $\tilde{f}$ sur tout les réels, non ?

S vérifie donc toutes les conditions de l'énoncé.

Démonstration de l'unicité

Soient u_1 et u_2 des solutions du problème. Posons $u = u_1 - u_2$. Par linéarité de l'équation de la chaleur, u est solution du problème pour des conditions initiales nulles.

Posons, pour $t \in \mathbf{R}_+$,

$$H(t) = \int_0^\pi u^2(t, x) dx.$$

Comme u est continue que $\mathbf{R}_+ \times [0, \pi]$, H est continue sur $\mathbf{R}_+$. L'existence et la continuité de $\partial_t u$ sur $\mathbf{R}_+^* \times [0, \pi]$ nous dit que H est $\mathcal{C}^1$ sur $\mathbf{R}_+^*$ et que pour tout $t \in \mathbf{R}_+^*$,

$$H'(t) = \int_0^\pi 2\partial_t u(t, x)u(t, x) dx = \int_0^\pi 2\partial_x^2 u(t, x)u(t, x) dx,$$

donc par une intégration par parties, en utilisant les conditions au bord,

$$H'(t) = -2 \int_0^\pi (\partial_x u(t, x))^2 dx \leq 0.$$

Si l'on récapitule, H est décroissante sur $\mathbf{R}_+$, et positive, nulle en 0. Elle est donc nulle sur $\mathbf{R}_+$. Comme u^2 est positive et continue, $u = 0$ donc $u_1 = u_2$.

28 Fonctions dont la série des coefficients de Fourier converge absolument

Leçons : 205, 241, 246

Référence: Analyse 2, Francinou, Gianella, Nicolas

Soit $\mathcal{B}$ l'ensemble des applications continues 2π -périodiques de $\mathbf{R}$ dans $\mathbf{C}$ dont la série des coefficients de Fourier converge absolument. Il existe une norme sous-multiplicative qui rend $\mathcal{B}$ complet.

Dans ce développement, on note $\mathcal{C}$ l'ensemble des applications continues et 2π -périodiques de $\mathbf{R}$ dans $\mathbf{C}$.

- $\mathcal{B}$ est un sous-espace vectoriel de $\mathcal{C}$ dont tous les éléments sont sommes de leur série de Fourier.

Soient $f, g \in \mathcal{B}$ et soit $\lambda \in \mathbf{R}$.

Pour tout $n \in \mathbf{N}$, $c_n(f + g) = c_n(f) + c_n(g)$ et $c_n(\lambda f) = \lambda c_n(f)$.

Comme les séries $\sum c_n(f)$ et $\sum c_n(g)$ convergent absolument, il en va donc de même pour $\sum c_n(f + g)$ et $\sum c_n(\lambda f)$, donc $f + g$ et λf sont dans $\mathcal{B}$.

Soit $f \in \mathcal{B}$. On pose $g : \mathbf{R} \rightarrow \mathbf{C}; x \mapsto \sum_{n \in \mathbf{Z}} c_n(f) e^{inx}$. g est bien définie car la série qui la définit converge normalement par hypothèse. Ce même argument nous donne la continuité de g sur $\mathbf{R}$. De plus, pour tout $k \in \mathbf{Z}$, le coefficient de Fourier d'ordre k de g est

$$c_k(g) = \frac{1}{2\pi} \int_{-\pi}^{\pi} \sum_{n \in \mathbf{Z}} c_n(f) e^{i(n-k)x} dx.$$

Par convergence normale des fonctions sur le segment $[-\pi, \pi]$, on peut intervertir la série et l'intégrale, ce qui nous donne pour tout $k \in \mathbf{Z}$

$$c_k(g) = \sum_{n \in \mathbf{Z}} \frac{1}{2\pi} \int_{-\pi}^{\pi} c_n(f) e^{i(n-k)x} dx = c_k(f).$$

Donc, g et f ont les mêmes coefficients de Fourier, et comme elles sont continues, la formule de Parseval nous dit que

$$\int_{-\pi}^{\pi} |f - g|^2(t) dt = \sum_{n \in \mathbf{Z}} c_n(f - g)^2 = 0,$$

donc $f - g = 0$ et f est bien égale à la somme de sa série de Fourier.

- Il existe une norme rendant $\mathcal{B}$ complet.

Posons $\|\cdot\| : f \in \mathcal{B} \mapsto \sum_{n \in \mathbf{Z}} |c_n(f)| \in \mathbf{R}$. On vérifie rapidement que $\|\cdot\|$ est une norme :

- Pour tout $f \in \mathcal{B}$, $\|f\| \geq 0$,
- Pour tout $\lambda \in \mathbf{R}$, $\|\lambda f\| = |\lambda| \|f\|$,
- Pour tout $(f, g) \in \mathcal{B}^2$, $\|f + g\| \leq \|f\| + \|g\|$,
- Si $\|f\| = 0$ alors $c_n(f) = 0$ pour tout $n \in \mathbf{Z}$ donc $f = 0$ par la formule de Parseval (f est continue).

Soit $(f_k)_{k \in \mathbf{N}}$ une suite de Cauchy de $\mathcal{B}$. Comme, pour tout $(k, l) \in \mathbf{N}^2$, et tout $n \in \mathbf{Z}$,

$$|c_n(f_k) - c_n(f_l)| \leq \|f_k - f_l\|,$$

la suite $(c_n(f_k))_{k \in \mathbf{N}}$ est de Cauchy pour tout $n \in \mathbf{N}$. Comme $\mathbf{C}$ est complet, pour tout $n \in \mathbf{N}$, ces suites convergent vers des complexes c_n .

Montrons que $\sum_n |c_n|$ converge. Comme la suite (f_k) est de Cauchy, elle est bornée pour $\|\cdot\|$, donc il existe $M \in \mathbf{R}_+$ tel que pour tout $k \in \mathbf{N}$, $\|f_k\| \leq M$. Pour $N \in \mathbf{N}$ et $k \in \mathbf{N}$,

$$\sum_{n=-N}^N |c_n(f_k)| \leq \|f_k\| \leq M.$$

En laissant k tendre vers l'infini dans l'inégalité précédente,

$$\sum_{n=-N}^N |c_n| \leq M.$$

Comme N est quelconque, on a la convergence absolue de la série de terme général $|c_n|$.

Posons, pour tout $x \in \mathbf{Z}$, $f(x) = \sum_{n \in \mathbf{Z}} c_n e^{inx}$. Par le même raisonnement qu'au point précédent, on montre que l'on a construit une fonction continue sur $\mathbf{R}$ et dont les coefficients de Fourier sont les c_n . On va montrer que c'est la limite de la suite $(f_k)_{k \in \mathbf{N}}$.

Soit $\varepsilon \in \mathbf{R}_+^*$. Il existe $k_0 \in \mathbf{N}$ tel que $\|f_k - f_l\| = \sum_{n \in \mathbf{Z}} |c_n(f_k) - c_n(f_l)| \leq \varepsilon$ si $k, l \geq k_0$. Pour tout $N \in \mathbf{N}$, on a alors

$\sum_{n=-N}^N |c_n(f_k) - c_n(f_l)| \leq \varepsilon$. En faisant tendre l vers $+\infty$, on obtient que

$$\sum_{n=-N}^N |c_n(f_k) - c_n| \leq \varepsilon.$$

Comme N est quelconque, on en déduit que pour tout $k \geq k_0$,

$$\sum_{n \in \mathbf{Z}} |c_n(f_k) - c_n| = \|f_k - f\| \leq \varepsilon.$$

On a donc la convergence de (f_k) vers f dans $\mathcal{B}$. D'où la complétude de l'espace.

- La norme est sous-multiplicative.

Soient f et g deux éléments de $\mathcal{B}$. On décompose f et g en série de Fourier : pour tout $x \in \mathbf{R}$, $f(x) = \sum_{n \in \mathbf{Z}} c_n(f) e^{inx}$

et $g(x) = \sum_{n \in \mathbf{Z}} c_n(g) e^{inx}$.

Ces deux séries étant absolument convergentes, on peut considérer leur produit de Cauchy et écrire

$$\begin{aligned} f(x)g(x) &= \sum_{p \in \mathbf{Z}} \left(\sum_{m+n=p} c_n(f) e^{inx} c_m(g) e^{imx} \right), \\ &= \sum_{p \in \mathbf{Z}} \underbrace{\left(\sum_{m+n=p} c_n(f) c_m(g) \right)}_{a_p} e^{ipx}. \end{aligned}$$

De plus, comme les séries $\sum c_n(f)$ et $\sum c_n(g)$ convergent absolument, on peut aussi considérer leur produit de Cauchy, qui est donc égal à $\|f\| \|g\|$:

$$\|f\| \|g\| = \sum_{p \in \mathbf{Z}} \left(\sum_{m+n=p} |c_n(f)| |c_m(g)| \right).$$

Comme, par inégalité triangulaire, $|a_p| \leq \sum_{m+n=p} |c_n(f)| |c_m(g)|$, et que le terme de droite est sommable, on obtient

la convergence absolue de la série $\sum_p a_p$, donc la convergence normale de la série $\sum_{p \in \mathbf{Z}} a_p e^{ipx}$ sur tout $\mathbf{R}$. On peut

donc montrer comme dans le premier point que les a_p sont les coefficients de Fourier de fg et que $fg \in \mathcal{B}$. Enfin, par définition des a_p et inégalité triangulaire,

$$\|fg\| = \sum_p |a_p| \leq \sum_{p \in \mathbf{Z}} \left(\sum_{m+n=p} |c_n(f)| |c_m(g)| \right) = \|f\| \|g\|.$$

29 Théorème ergodique de Von Neumann

Leçons : 208,213

Référence: Objectif Agrégation, Beck, Malick, Peyré

Théorème — (Théorème ergodique de Von Neumann)

Soit H un espace de Hilbert. Soit T un opérateur de norme inférieure ou égale à 1. On note p la projection orthogonale sur $\text{Ker}(T - \text{Id})$. Alors,

$$\forall x \in H, T_n(x) := \frac{1}{n+1} \sum_{k=0}^n T^k(x) \xrightarrow{n \rightarrow +\infty} p(x).$$

Application — Soit $\alpha \in \mathbf{R} \setminus 2\pi\mathbf{Q}$, alors

$$\forall f \in L^2(\mathbf{T}), \frac{1}{n+1} \sum_{k=0}^n f(x + k\alpha) \xrightarrow{n \rightarrow +\infty} \frac{1}{2\pi} \int_0^{2\pi} f(t) dt.$$

- Pour tout $x \in H$, $Tx = x \Leftrightarrow \langle Tx, x \rangle = \|x\|^2 \Leftrightarrow \langle x, Tx \rangle = \|x\|^2$.

La deuxième équivalence vient du fait que, puisque $\|x\|$ est une grandeur réelle,

$$\|x\|^2 = \langle Tx, x \rangle = \overline{\langle x, Tx \rangle} = \|x\|^2.$$

L'implication $Tx = x \Leftarrow \langle Tx, x \rangle = \|x\|^2$ est immédiate. Supposons donc que la deuxième assertion est vérifiée pour $x \in H$. Si $x = 0$ le résultat est vrai car T est un opérateur. Supposons donc que $x \neq 0$. Alors, par l'inégalité de Cauchy-Schwarz, et comme T est de norme inférieure ou égale à 1,

$$\|x\|^2 = \langle Tx, x \rangle \leq \|x\| \|Tx\| \leq \|x\|^2.$$

On est donc dans le cas d'égalité de Cauchy-Schwarz, donc Tx et x sont positivement proportionnels. Le facteur multiplicatif est donc égal à -1 car $\langle Tx, x \rangle = \|x\|^2 = |\lambda| \|x\|^2$.

- Montrer que $\text{Ker}((\text{Id} - T)) = \text{Ker}((\text{Id} - T)^*)$ et en déduire le théorème quand $x \in \text{Ker}((\text{Id} - T)^*)$.

Comme $\|T\| = \|T^*\| \leq 1$, on peut appliquer le résultat de la question précédente à T^* . Or, par définition de l'adjoint, pour tout $x \in H$,

$$\langle T^*x, x \rangle = \langle x, Tx \rangle,$$

donc par la première équivalence montrée au point précédent,

$$\text{Ker}((\text{Id} - T)) = \text{Ker}((\text{Id} - T)^*).$$

Soit donc $x \in \text{Ker}((\text{Id} - T)^*)$. Par l'égalité ci-dessus, $T^k(x) = x$ pour tout $k \in \mathbf{N}$ et donc $T_n(x) = x$ pour tout $n \in \mathbf{N}$. Comme p est la projection orthogonale sur $\text{Ker}(\text{Id} - T)$, x est un point fixe de p , d'où

$$T_n(x) = x = p(x) \quad \forall n \in \mathbf{N}.$$

- Montrer que $T_n(x) \xrightarrow{n \rightarrow +\infty} 0$ si $x \in \overline{\text{Im}(\text{Id} - T)}$.

Commençons par le cas où $x \in \text{Im}(\text{Id} - T)$. Soit $y \in H$ tel que $x = y - T(y)$. Alors pour tout $n \in \mathbf{N}$,

$$T_n(x) = \frac{1}{n+1} \left(\sum_{k=0}^n T^k(y) - \sum_{k=1}^{n+1} T^k(y) \right) = \frac{1}{n+1} (T^{n+1}(y) - y).$$

Or, comme T est de norme inférieure à 1,

$$\|T_n(x)\| \leq \frac{2\|y\|}{n+1} \xrightarrow{n \rightarrow +\infty} 0.$$

Soit $\varepsilon \in \mathbf{R}_+^*$ et soit à présent $x \in \overline{\text{Im}(\text{Id} - T)}$. Soit $y \in \text{Im}(\text{Id} - T)$ tel que $\|x - y\| \leq \varepsilon$. Par inégalité triangulaire, linéarité de T_n et comme $\|T_n\| \leq 1$ par inégalité triangulaire,

$$\|T_n(x)\| \leq \|x - y\| + \|T_n(y)\|.$$

En prenant n suffisamment grand pour avoir $\|T_n(y)\| \leq \varepsilon$, on a

$$\|T_n(x)\| \leq 2\varepsilon.$$

D'où la convergence vers 0.

- Conclusion

Comme $\text{Ker}((\text{Id} - T)^*)^\perp = \overline{\text{Im}(\text{Id} - T)}$, on a

$$H = \text{Ker}((\text{Id} - T)^*) \overset{\perp}{\oplus} \overline{\text{Im}(\text{Id} - T)} = \text{Ker}(\text{Id} - T) \overset{\perp}{\oplus} \overline{\text{Im}(\text{Id} - T)}.$$

Soit $z \in H$. Conformément à la décomposition ci-dessus, on écrit $z = x + y$ avec $x \in \text{Ker}(\text{Id} - T)$ et $y \in \overline{\text{Im}(\text{Id} - T)}$. Par linéarité de T_n ,

$$T_n(z) = T_n(x) + T_n(y),$$

et par passage à la limite,

$$\lim_{n \rightarrow +\infty} T_n(z) = \lim_{n \rightarrow +\infty} T_n(x) + T_n(y) = x = p(z).$$

On a montré le théorème d'ergodicité de Von Neumann.

- Preuve de l'application

Notons $H = L^2(\mathbf{T})$ et munissons-le de son produit scalaire canonique $\langle f, g \rangle = \frac{1}{2\pi} \int_0^{2\pi} f(t) \overline{g(t)} dt$. posons $T : H \rightarrow H; f \mapsto f_\alpha$, où $f_\alpha : x \mapsto f(x + \alpha)$. T est un opérateur continu de norme 1, et c'est même une isométrie (vérification immédiate).

On montre que $\text{Ker}(\text{Id} - T)$ est l'ensemble des fonctions constantes dans H . Nous avons une inclusion évidente. Soit $f \in H$ et posons $g = T(f)$. Par un changement de variables, en notant $c_n(\cdot)$ les coefficients de Fourier, on a

$$\forall n \in \mathbf{N}, c_n(g) = e^{-in\alpha} c_n(f).$$

Ainsi, si $f \in \text{Ker}(\text{Id} - T)$, on a $g = f$ et donc égalité des coefficients de Fourier à tout ordre. Comme $\alpha \notin 2\pi\mathbf{Q}$, on a la nullité des coefficients de Fourier de f d'ordre supérieur ou égal à 1. Donc f est constante.

Par le théorème de Von Neumann, pour tout $f \in H$, $T_n(f) : x \mapsto \frac{1}{n} \sum_{k=0}^{n-1} f(x + k\alpha)$ converge dans H vers

$$p(f) = c_0(f) = \frac{1}{2\pi} \int_0^{2\pi} f(t) dt.$$

30 Résolution d'une équation aux dérivées partielles elliptiques

Leçons : 202,213,222

Référence: Analyse pour l'agrégation de mathématiques, Bernis

Soient $f \in L^2([0, 1], \mathbf{R})$, $\alpha \in L^\infty([0, 1], \mathbf{R})$ et $\beta \in C^1([0, 1], \mathbf{R})$. On suppose que :

1. Il existe $\alpha_{min} \in \mathbf{R}_+^*$ tel que pour λ -presque tout $x \in [0, 1]$, on ait $\alpha(x) \geq \alpha_{min}$;
2. Pour tout $x \in [0, 1]$, $\beta'(x) \leq 2$.

Alors, il existe un unique $u \in H_0^1([0, 1], \mathbf{R})$ qui soit solution au sens des distributions de l'équation

$$-(\alpha u')' + \beta u' + u = f.$$

Notons $\mathcal{S}$ l'ensemble (éventuellement vide) des éléments de $H_0^1([0, 1], \mathbf{R}) = H$ qui sont solutions de l'équation. Rappelons d'ores et déjà que H est un espace de Hilbert.

- Formulation variationnelle du problème.

Soit $u \in H$. Comme $u' \in L^2$ et α est bornée, $\alpha u' \in L^2 \subset L_{loc}^1$, donc définit bien une distribution. Il en va de même pour $\beta u' \in L_{loc}^1$, u et f . On a donc que $u \in \mathcal{S}$ si et seulement si pour toute fonction-test $\varphi \in \mathcal{D}([0, 1], \mathbf{R})$,

$$\underbrace{\langle \alpha u', \varphi' \rangle + \langle \beta u', \varphi \rangle + \langle u, \varphi \rangle}_{a(u, \varphi)} = \underbrace{\langle f, \varphi \rangle}_{L(\varphi)}.$$

De plus, comme toutes nos fonctions sont dans L_{loc}^1 , les applications a et L s'expriment sous la forme :

$$\forall u, v \in H, \begin{cases} a(u, v) &= \int_0^1 \alpha(x) u'(x) v'(x) + \beta(x) u'(x) v(x) + u(x) v(x) \, dx, \\ L(v) &= \int_0^1 f(x) v(x) \, dx. \end{cases}$$

On voit donc par linéarité de la dérivation et de l'intégrale que a est bilinéaire sur $H \times H$ et L est linéaire sur H .

- Continuité de a et L

Attention abus de notation : β est bornée donc a une norme uniforme, mais α a une norme L^∞ , que j'écris de la même manière ici par flemme.

Soient v_1, v_2 des éléments de H . Comme β est continue sur le segment $[0, 1]$, elle y est bornée et par inégalité triangulaire,

$$|a(v_1, v_2)| \leq \|\alpha\|_\infty \int_0^1 |v_1'(x) v_2'(x)| \, dx + \|\beta\|_\infty \int_0^1 |v_1'(x) v_2(x)| \, dx + \int_0^1 |v_1(x) v_2(x)| \, dx.$$

Par l'inégalité de Cauchy-Schwarz,

$$|a(v_1, v_2)| \leq \|\alpha\|_\infty \|v_1'\|_2 \|v_2'\|_2 + \|\beta\|_\infty \|v_1'\|_2 \|v_2\|_2 + \|v_1\|_2 + \|v_2\|_2,$$

et donc en majorant toutes les normes par la norme dans H^1 ,

$$|a(v_1, v_2)| \leq (\|\alpha\|_\infty + \|\beta\|_\infty + 1) \|v_1\|_{H^1} \|v_2\|_{H^1}.$$

D'où la continuité de a .

Par un calcul similaire, on a la majoration

$$|L(v)| \leq \|f\|_2 \|v\|_{H^1}$$

et donc la continuité de L .

Nous avons donc montré, en plus de cela, que u est dans $\mathcal{S}$ si et seulement si pour tout $v \in H$ (et non plus seulement les fonctions-test), $a(u, v) = L(v)$. En effet, $\mathcal{D}([0, 1], \mathbf{R})$ étant dense dans H , la continuité de a et L nous permet de conclure.

- Coercivité de a

Soit $v \in H$. On dispose d'une suite φ_n de fonctions-test qui converge dans H vers v . On prolonge tous les φ_n à $[0, 1]$ par continuité avec $\varphi_n(0) = \varphi_n(1) = 0$. Par une intégration par parties, pour tout $n \in \mathbf{N}$,

$$\int_0^1 \beta(x) \varphi_n'(x) \varphi_n(x) \, dx = -\frac{1}{2} \int_0^1 \beta'(x) \varphi_n(x)^2 \, dx.$$

Or, le terme de droite converge vers $a(v, v)$: en effet,

$$\begin{aligned} |a(v, v) - a(\varphi_n, \varphi_n)| &\leq \|\beta\|_\infty \int_0^1 |\varphi_n'(x) \varphi_n(x) - v'(x) v(x)| \, dx, \\ &\leq \|\beta\|_\infty \int_0^1 |\varphi_n(x) - v(x)| |\varphi_n'(x)| + |\varphi_n'(x) - v'(x)| |v(x)| \, dx, \\ &\leq \|\beta\|_\infty (\|\varphi_n - v\|_2 \|\varphi_n'\|_2 + \|\varphi_n' - v'\|_2 \|v\|_2). \end{aligned}$$

Or, en majorant le terme de droite par les normes dans H^1 , la suite (φ_n) converge dans H donc est bornée par M dans H , donc pour n assez grand on voit que la différence tend vers 0. De plus, il est facile de voir que le terme de droite est également continu en φ_n ce qui donne la convergence dans H vers $-\frac{1}{2} \int_0^1 \beta'(x) v(x)^2 \, dx$.

Si l'on revient à a , on a donc que

$$\begin{aligned} a(v, v) &= \int_0^1 \alpha(x) v'(x)^2 - \frac{1}{2} \beta'(x) v(x)^2 + v(x)^2 \, dx, \\ &\geq \alpha_{\min} \|v'\|_2^2 + (-1 + 1) \|v\|_2^2, \end{aligned}$$

donc par l'inégalité de Poincaré,

$$a(v, v) \geq \frac{\alpha_{\min}}{2} (4\pi^2 \|v\|_2^2 + \|v'\|_2^2) \geq C \|v\|_{H^1}^2.$$

Ainsi a est-elle coercive.

- Lax-Milgram

D'après le théorème de Lax-Milgram, il existe un unique élément u de H qui vérifie que pour tout $v \in H$, $a(u, v) = L(v)$, c'est-à-dire que $u \in \mathcal{S}$.

31 Lemme de Schwarz et automorphismes bianalytiques du disque

Leçons : 245

Référence: Analyse complexe, Amar et Matheron

Lemme — (Schwarz) Soit $\mathbb{D} = B(0,1) \subset \mathbb{C}$ le disque (ouvert) unité, soit $f \in \mathcal{H}(\mathbb{D})$. On suppose que $f(\mathbb{D}) \subset \mathbb{D}$ et $f(0) = 0$. Alors,

1. $\forall z \in \mathbb{D}, |f(z)| \leq |z|$.

2. $|f'(0)| \leq 1$.

De plus, s'il existe $z \in \mathbb{D} \setminus \{0\}$ tel que $|f(z)| = |z|$ ou si $|f'(0)| = 1$, alors il existe $\alpha \in \mathbb{U}$ tel que pour tout $z \in \mathbb{D}$, $f(z) = \alpha z$.

Application — On reprend les notations $\mathbb{D}$ et $\mathbb{U}$.

1. Pour tout $a \in \mathbb{D}$ et tout $\alpha \in \mathbb{U}$, il existe un unique automorphisme bianalytique φ de $\mathbb{D}$ tel que $\varphi(0) = a$ et $\varphi'(0) \in \mathbf{R}_+^* \alpha$.

2. Les automorphismes bianalytiques de $\mathbb{D}$ sont $\text{Aut}(\mathbb{D}) = \left\{ \lambda \varphi_a; \lambda \in \mathbb{U}, \varphi_a : z \mapsto \frac{z-a}{1-\bar{a}z}, a \in \mathbb{D} \right\}$.

Preuve du lemme

- Définition de la fonction auxiliaire par le principe du maximum

Posons $g : \mathbb{D} \rightarrow \mathbb{C}; z \mapsto \begin{cases} \frac{f(z)}{z} & \text{si } z \neq 0, \\ f'(0) & \text{sinon.} \end{cases}$. g est bien définie car $f \in \mathcal{H}(\mathbb{D})$ et g est holomorphe sur $\mathbb{D}$ car au

voisinage de 0, $f(z) = zf'(0) + z^2 \frac{f''(0)}{2} + O(z^3)$.

Soit $r < 1$. Comme pour tout $z \in \mathbb{D}$, $|f(z)| \leq 1$, on a que si $|z| > r$, $|g(z)| \leq \frac{1}{r}$. Par le principe du maximum global, l'inégalité est en fait vraie pour tout $z \in \mathbb{D}$. En laissant tendre r vers 1, on a que $g(\mathbb{D}) \subset \mathbb{D}$.

- Conclusion

Comme g est à valeurs dans le disque, pour tout $z \in \mathbb{D}$, $|f(z)| \leq |z|$ et $|f'(0)| = |g(0)| \leq 1$.

De plus, s'il existe a tel que $|f(a)| = |a|$, alors $|g(a)| = 1$ et par le principe du maximum local, g est constante et $g(0) = f'(0)$ dont $f(z) = f'(0)z$. En prenant $z = a$, $|f'(0)| = 1$.

Preuve de l'application

- Les morphismes φ_a sont des automorphismes bianalytiques

Soit $a \in \mathbb{D}$. φ_a est bien définie car $|\bar{a}z| < |z| \leq 1$. Elle est donc également holomorphe.

Pour tout $t \in \mathbf{R}$, $|\varphi_a(e^{it})| = \left| \frac{e^{it}-a}{1-\bar{a}e^{it}} \right| = \left| \frac{e^{it}-a}{e^{-it}-\bar{a}} \right| = 1$. Par le principe du maximum, $\varphi_a(\mathbb{D}) \subset \mathbb{D}$.

Comme on remarque que $\varphi_a \circ \varphi_{-a} = \text{Id}$, $\varphi_a \in \text{Aut}(\mathbb{D})$ et tel est donc aussi le cas de $\lambda \varphi_a$ pour tout $\lambda \in \mathbb{U}$.

- Tout automorphisme bianalytique est de la forme $\lambda \varphi_a$

Soit $f \in \text{Aut}(\mathbb{D})$. Posons $a = f(0)$ et $g = \varphi_a \circ f$.

Alors, $g \in \text{Aut}(\mathbb{D})$, $g(0) = 0$ et donc par le lemme de Schwarz, pour tout $z \in \mathbb{D}$, $|g(z)| \leq |z|$. Or, g^{-1} vérifie la même propriété donc $|g(z)| \geq |z|$ pour tout $z \in \mathbb{D}$. Par le deuxième point du lemme, il existe $\lambda \in \mathbb{U}$ tel que $g(z) = \lambda z$, i.e $f(z) = \varphi_{-a}(\lambda z) = \lambda \varphi_{a\bar{\lambda}}(z)$.

Donc $\text{Aut}(\mathbb{D}) = \left\{ \lambda \varphi_a; \lambda \in \mathbb{U}, \varphi_a : z \mapsto \frac{z-a}{1-\bar{a}z}, a \in \mathbb{D} \right\}$.

ne pas oublier de conclure quant au premier point de l'application

- Complément : les automorphismes du demi-plan supérieur.

Notons $H = \{z \in \mathbf{C}, \Im(z) > 0\}$. Les fonctions $h : \mathbb{D} \rightarrow \mathbb{H}; z \mapsto i \frac{z+1}{1-z}$ et $l : H \rightarrow D; \xi \mapsto \frac{\xi-1}{\xi+i}$ sont holomorphes et bijections réciproques l'une de l'autre.

Soit $f \in \text{Aut}(H)$. Par le point précédent, il existe $a \in \mathbb{D}$ et $\lambda = e^{i\theta} \in \mathbb{U}$ tels que pour tout $z \in H$, $f(z) = h(e^{i\theta} \varphi_a(l(z)))$.

Après calculs, en utilisant le fait que $e^{i\theta} = \frac{e^{i\theta/2}}{e^{-i\theta/2}}$ et en posant $\alpha = e^{i\theta/2}(1-a)$ et $\beta = e^{i\theta/2}(1+a)$,

$$f(z) = \frac{(\alpha + \bar{\alpha})z + i(\bar{\beta} - \beta)}{-i(\bar{\alpha} - \alpha) + (\bar{\beta} - \beta)}.$$

De là, on déduit que $\text{Aut}(H) = \left\{ z \mapsto \frac{az+b}{cz+d}, ad-bc > 0. \right\}$.

32 Simplicité de $\mathrm{SO}_3(\mathbf{R})$

Leçons : 103, 204

Référence: Algèbre 3, Francinou, Gianella, Nicolas

| Théorème — $\mathrm{SO}_3(\mathbf{R})$ est simple.

Soit H un sous-groupe distingué de $\mathrm{SO}_3(\mathbf{R})$. On pose G_0 la composante connexe de I_3 dans H .

- Montrer que G_0 un sous-groupe de H distingué dans $\mathrm{SO}_3(\mathbf{R})$.

Soient A et B des éléments de G_0 . Par connexité par arcs de G_0 , il existe des chemins α et β qui lient respectivement A et B à l'identité. Posons $\gamma = \alpha \cdot \beta^{-1}$, où $\beta^{-1} : t \in [0, 1] \mapsto \beta(t)^{-1} \in \mathrm{SO}_3(\mathbf{R})$.

* γ est continue car α et β le sont et que le passage à l'inverse est une application continue (formule avec la comatrice : tous les coefficients sont polynômiaux).

* $\gamma(0) = \alpha(0)\beta(0)^{-1} = I_3$ et $\gamma(1) = \alpha(1)\beta(1)^{-1} = AB^{-1}$.

On a donc construit un chemin qui lie I_3 à AB^{-1} . Ainsi, $AB^{-1} \in G_0$. Donc G_0 est un sous-groupe de H .

Montrons à présent que G_0 est distingué. Soit $C \in \mathrm{SO}_3(\mathbf{R})$ et posons, pour tout $t \in [0, 1]$,

$$\delta(t) = C\alpha(t)C^{-1}.$$

δ est un chemin continu qui relie I_3 et $CAC^{-1} \in G_0$. Ainsi G_0 est-il distingué dans $\mathrm{SO}_3(\mathbf{R})$.

- Montrer que $\mathrm{SO}_3(\mathbf{R})$ ne contient pas de sous-groupe distingué connexe par arcs autre que lui-même

Soit G un sous-groupe distingué de $\mathrm{SO}_3(\mathbf{R})$ non réduit à l'identité et connexe par arcs. On va montrer que G contient un renversement, donc tous car les renversements sont conjugués et que G est normal.

Soit

$$f : \mathrm{SO}_3(\mathbf{R}) \rightarrow [-1, 1] ; M \mapsto \frac{\mathrm{Tr}(M) - 1}{2}.$$

L'application f est continue. Soit A une rotation non triviale de G . Quitte à travailler sur A^{-1} , on suppose que l'angle de rotation θ est compris entre 0 et π .

Dans une bonne base, la matrice A est de la forme

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix},$$

donc $f(A) = \cos(\theta)$.

Si $\theta = \pi$, on a un renversement et c'est fini.

Sinon, on va montrer qu'il existe une matrice $M \in G$ telle que $f(M) \leq 0$. Si $\cos(\theta) \leq 0$, alors A convient. Sinon, soit $n \in \mathbf{N}$ tel que

$$n\theta < \frac{\pi}{2} < (n+1)\theta < \pi.$$

Posons $M = A^n$. Ainsi, $M \in G$ et $f(M) \leq 0$. De plus, $f(I_3) = 1$. Comme G est connexe et un sous-groupe de $\mathrm{SO}_3(\mathbf{R})$, il est inclus dans la composante connexe de l'identité. Il existe donc un chemin γ qui relie I_3 et M . Donc, $f \circ \gamma$ est continue, vaut 1 en 0 et est négative en 1. Par le théorème des valeurs intermédiaires, il existe $t \in [0, 1]$ tel que $f \circ \gamma(t) = 0$. $\gamma(t)$ est donc une rotation d'angle $\frac{\pi}{2}$ et donc $\gamma^2(t) \in G$ est un renversement. D'où le résultat.

- Conclusion

On rappelle que G_0 est un sous-groupe distingué de H .

Or, par le point précédent, G_0 est soit réduit à l'identité soit est l'espace tout entier. Dans le deuxième cas, on a fini. Sinon, on peut en déduire que toutes les composantes connexes par arcs de $\mathrm{SO}_3(\mathbf{R})$ sont des singletons (car on peut se ramener à la composante connexe de l'identité en prenant A dans la composante et en multipliant par A^{-1}).

Soit $A \in H$. Soit B une rotation d'angle θ . On pose, pour $t \in [0, 1]$, B_t la rotation d'angle $t\theta$. Comme H est

distingué dans $SO_3(\mathbf{R})$, alors $B_t A B_t^{-1} \in H$ à tout temps, et ces matrices sont également dans la composante connexe de A qui est restreinte à A . Donc, $B A B^{-1} = A$, soit A commute avec toutes les rotations. On en déduit que $A = I_3$. Donc $H = \{I_3\}$. D'où la simplicité de $SO_3(\mathbf{R})$.

33 Polynômes cyclotomiques et théorème de Wedderburn

Leçons : 101, 102, 103, 104, 123

Référence: Cours d'Algèbre, Perrin

Lemme — Pour tout $n \in \mathbf{N}$,

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

Lemme — Soient $n, d, q \in \mathbf{N}^*$ avec $q \geq 2$.

Alors, $d|n$ si et seulement si $q^d - 1 | q^n - 1$. Le cas échéant, $\Phi_n(q)$ divise $\frac{q^n - 1}{q^d - 1}$ pour tout d diviseur strict de n .

Théorème — (Wedderburn) Tout corps fini est commutatif.

Démonstration — Preuve du premier lemme

Notons $\mathbf{U}_n$ l'ensemble des racines n -ièmes de l'unité et $\mathbf{U}_n^p$ l'ensemble des racines primitives n -ièmes de l'unité. Montrons que

$$\mathbf{U}_n = \bigsqcup_{d|n} \mathbf{U}_d^p.$$

Soit $\zeta \in \mathbf{U}_n$. Alors si on note d l'ordre de ζ , on a $d|n$ et $\zeta \in \mathbf{U}_d$. Donc $\zeta \in \mathbf{U}_d^p$. De plus, comme les éléments de $\mathbf{U}_d^p$ sont d'ordre d dans $\mathbf{C}^*$, les ensembles sont bien disjoints.

Réciproquement, comme tout élément de $\bigsqcup_{d|n} \mathbf{U}_d^p$ est racine n -ième de l'unité car son ordre divise n , on a bien la deuxième inclusion.

De cela, on déduit que

$$X^n - 1 = \prod_{\zeta \in \mathbf{U}_n} (X - \zeta) = \prod_{d|n} \prod_{\zeta \in \mathbf{U}_d^p} (X - \zeta) = \prod_{d|n} \Phi_d(X).$$

□

Démonstration — Preuve du deuxième lemme

On écrit $n = md + r$ avec $r \in \llbracket 0, d-1 \rrbracket$. On remarque que $m \geq 0$. Alors,

$$q^n - 1 = q^{md} q^r - 1 = (q^d - 1 + 1)^m q^r - 1.$$

Or, par le binôme de Newton,

$$(q^d - 1 + 1)^m = \sum_{k=0}^m \binom{m}{k} (q^d - 1)^k \equiv 1 [q^d - 1],$$

donc en passant aux congruences,

$$q^n - 1 \equiv q^r - 1 [q^d - 1].$$

On en déduit que $d|n$ si et seulement si $r = 0$ si et seulement si $q^d - 1 | q^n - 1$.

On se place dans le cas où $d|n$. Alors,

$$X^n - 1 = (X^d - 1) \prod_{e|n, e \nmid d} \Phi_e(X).$$

Donc, si $d \neq n$, il existe $Q \in \mathbf{Z}[X]$ tel que

$$X^n - 1 = (X^d - 1)Q\Phi(n),$$

et donc

$$\Phi_n(q) \text{ divise } \frac{q^n - 1}{q^d - 1}.$$

□

Démonstration — Preuve du théorème

- Mise en place

Soit k un corps fini non nécessairement commutatif. Notons Z son centre. Alors, Z est un sous-corps de k (contient 1, stable par somme, produit, opposé et inverse : $ax = xa \Rightarrow x = a^{-1}xa \Rightarrow a^{-1}x = xa^{-1}$) de cardinal $q \geq 2$ (il contient au moins 0 et 1). De plus, Z est commutatif par construction. Enfin, comme k est une extension de Z , c'est un Z -espace vectoriel et donc $|k| = q^n$.

Supposons par l'absurde que k est non commutatif. En particulier, cela signifie que $n > 1$, sans quoi on aurait $k = Z$ et donc k serait commutatif.

- Étude de l'action de k^* sur lui-même par automorphismes intérieurs

On fait agir k^* sur lui-même par conjugaison. On note, pour $x \in k^*$, $\omega(x)$ l'orbite de x .

Posons $k_x = \{y \in k \mid yx = xy\}$. C'est un sous-corps de k (pas forcément commutatif) de la même manière que pour Z . De plus, k_x^* est le stabilisateur de x pour l'action de groupe définie ici.

Comme Z est un sous-corps de k_x , comme au-dessus, il existe $d \in \mathbf{N}$ tel que $|k_x| = q^d$. De plus, comme k_x^* est un sous-groupe de k^* , $q^d - 1 \mid q^n - 1$ donc par le deuxième lemme, $d \mid n$, vu que $q \geq 2$. On en déduit que

$$|\omega(x)| = \frac{|k^*|}{|k_x^*|} = \frac{q^n - 1}{q^d - 1}.$$

- Polynômes cyclotomiques, équation des classes et un dessin

Par le deuxième lemme, $\Phi_n(q)$ divise $\frac{q^n - 1}{q^d - 1}$. De plus, par l'équation des classes,

$$|k^*| - |Z^*| + \sum_{x \notin Z} |\omega(x)|.$$

Or, dire que $x \notin Z$ signifie que $d \neq n$, de sorte que

$$q^n - 1 = q - 1 + \sum \frac{q^n - 1}{q^d - 1},$$

la somme portant sur un certain nombre de diviseurs stricts de n . On en déduit que $\Phi_n(q)$ divise $q - 1$, et donc

$$|\Phi_n(q)| \leq q - 1.$$

Or, $\Phi_n(q) = (q - \zeta_1) \dots (q - \zeta_l)$ avec $\zeta_1, \dots, \zeta_l$ les racines primitives n -ièmes de l'unité qui, puisque $n > 1$, sont différentes de 1 mais de norme 1.

Par un dessin, on se convainc que pour tout $i \in \llbracket 1, l \rrbracket$, $|q - \zeta_i| > q - 1$ et donc

$$q - 1 < \Phi_n(X) \leq q - 1, \text{ absurde.}$$

□

34 Indécomposabilité de la loi de Poisson

Leçons : 241, 243, 245, 266

Référence: Analyse complexe et applications, Queffélec, Queffélec

Théorème — Soient X et Y deux variables aléatoires indépendantes, à valeurs dans $\mathbf{N}$, et telles que $Z = X + Y$ suit une loi de Poisson $\mathcal{P}(\lambda)$. Alors, X et Y suivent une loi de Poisson.

• Rappels

On introduit les fonctions génératrices complexes de X , Y et Z : $G_X : z \mapsto \sum_{n \geq 0} p_n z^n$, $G_Y : z \mapsto \sum_{n \geq 0} q_n z^n$, et $G_Z : z \mapsto \sum_{n \geq 0} e^{-\lambda} \frac{\lambda^n}{n!} z^n = e^{\lambda(z-1)}$. On rappelle que les séries génératrices ont un rayon de convergence supérieur ou égal à 1 car pour toute variable aléatoire T à valeurs dans $\mathbf{N}$,

$$\sum_{n=0}^{\infty} \mathbb{P}(T = n) = 1.$$

Notons B la boule fermée de rayon 1 dans $\mathbf{C}$.

• G_X et G_Y sont des fonctions entières de produit G_Z sur $\mathbf{C}$.

Comme X et Y sont indépendantes, pour tout $z \in B$,

$$G_X(z)G_Y(z) = G_{X+Y}(z) = G_Z(z) = e^{\lambda(z-1)}.$$

En développant le produit de Cauchy à gauche, et par unicité de la décomposition en série entière,

$$p_0 q_0 = 1 \text{ et } \forall n \geq 1, e^{-\lambda} \frac{\lambda^n}{n!} = \sum_{k=0}^n p_k q_{n-k} \geq \max(p_n q_0, p_0 q_n).$$

On en déduit que pour tout $n \in \mathbf{N}^*$,

$$p_n \leq e^{-\lambda} \frac{\lambda^n}{q_0 n!} \text{ et } q_n \leq e^{-\lambda} \frac{\lambda^n}{p_0 n!},$$

donc les fonctions génératrices G_X et G_Y sont des fonctions entières (i.e ont un rayon de convergence infini). De plus, par le principe du prolongement analytique,

$$G_X(z)G_Y(z) = e^{\lambda(z-1)} \quad \forall z \in \mathbf{C}.$$

• Trouver la forme de G_X et G_Y

Soit z de module $r \geq 1$. Alors, comme $|G_X(z)| \leq G_X(|z|) = G_X(r)$ et que $q_0 G_X(r) \leq G_X(r)G_Y(r) = e^{\lambda(r-1)}$, et que le même genre de résultat se montre pour G_Y , on obtient l'existence d'une constante C positive telle que

$$|G_X(z)| \leq C e^{\lambda(|z|-1)} \text{ et } |G_Y(z)| \leq C e^{\lambda(|z|-1)}.$$

On utilise alors le

Lemme — Soit $f \in \mathcal{H}(\mathbf{C})$ une fonction entière qui ne s'annule jamais. Alors il existe une fonction $F \in \mathcal{H}(\mathbf{C})$ telle que $f = e^F$.

Démonstration — Soit $z \in \mathbf{C}$. Soit γ un chemin qui relie 0 à z , et posons $F(z) = \int_{\gamma} \frac{f'}{f}$.

F est indépendant du chemin γ . En effet, si β est un autre chemin reliant 0 à z , on a $\int_{\gamma * \beta} \frac{f'}{f} = 0$ car $\frac{f'}{f}$ est holomorphe (donc admet une primitive) et $\gamma * \beta$ est un lacet. On peut ainsi définir une fonction F .

F est holomorphe, en effet soient $z, h \in \mathbf{C}$. On a, en notant Δ la droite qui relie z à $z + h = z + r e^{i\theta}$, par théorème de continuité sous l'intégrale,

$$\frac{F(z+h) - F(z)}{h} = \frac{1}{r e^{i\theta}} \int_0^1 r e^{i\theta} \frac{f'(z + t r e^{i\theta})}{f(z + t r e^{i\theta})} dt = \int_0^1 \frac{f'(z + t r e^{i\theta})}{f(z + t r e^{i\theta})} dt \xrightarrow{r \rightarrow 0} \frac{f'(z)}{f(z)}.$$

□

En appliquant ce lemme à G_X et G_Y , il existe deux fonctions entières F et G telles que $G_X = e^F$ et $G_Y = e^G$, donc en regardant le module,

$$e^{\Re(F(z))} \leq C e^{\lambda(|z|-1)} \text{ et } e^{\Re(G(z))} \leq C e^{\lambda(|z|-1)},$$

soit

$$\Re(F(z)) \leq \ln C + \lambda(|z| - 1) \text{ et } \Re(G(z)) \leq \ln C + \lambda(|z| - 1).$$

Posons $F : z \mapsto \sum_{n \geq 0} a_n z^n$. Alors, pour tout $n \in \mathbf{N}$, et tout $r \in \mathbf{R}_+^*$,

$$a_n r^n + 0 = \frac{1}{2\pi} \int_0^{2\pi} \pi(F(r e^{i\theta}) + \overline{F(r e^{i\theta})}) e^{-in\theta} d\theta \leq \ln(C) + \lambda(r - 1).$$

On en déduit que pour tout $n \geq 2$, $a_n = 0$ (on divise par r et on le fait tendre vers 0). Avec le même raisonnement, on obtient donc l'existence de complexes a, α, b, β tels que pour tout $z \in \mathbf{C}$,

$$F(z) = \alpha z + a \text{ et } G(z) = \beta z + b.$$

Donc,

$$G_X(z) = e^{\alpha z + a} \text{ et } G_Y(z) = e^{\beta z + b}.$$

- Conclusion

Comme $1 = G_X(1) e^\alpha e^a$, donc $a = -\alpha$. De même, $b = -\beta$. On en déduit que pour tout $z \in \mathbf{C}$,

$$G_X(z) = e^{\alpha(z-1)} \text{ et } G_Y(z) = e^{\beta(z-1)}.$$

Donc, X et Y suivent des lois de Poisson de paramètres respectives α et β .

35 Théorème de Fourier-Plancherel

Leçons : 201, 207, 208, 234, 235, 250

Référence: Analyse réelle et complexe, Rudin

Théorème — Soit $f \in L^1(\mathbf{R}^n) \cap L^2(\mathbf{R}^n)$, alors $\mathcal{F}(f) \in L^2(\mathbf{R}^n)$ et $\|\mathcal{F}\|_{L^2} = (2\pi)^{\frac{n}{2}} \|f\|_{L^2}$.

On en déduit qu'il existe un unique prolongement de la transformée de Fourier en un opérateur $\mathcal{F} : L^2(\mathbf{R}^n) \rightarrow L^2(\mathbf{R}^n)$ qui vérifie

$$\forall f \in L^2(\mathbf{R}^n), \|\mathcal{F}(f)\|_{L^2} \leq (2\pi)^{\frac{n}{2}} \|f\|_{L^2}.$$

On effectue la preuve en dimension 1.

Notons $\tilde{f} : x \mapsto \overline{f(-x)}$.

- Introduction d'une fonction auxiliaire, étude de cette fonction

Posons $g = f * \tilde{f}$.

- $g \in L^1$ comme convolée de deux fonctions L^1 .
- g est bornée : en effet, on peut écrire $g(x) = \langle \tau_{-x}f, f \rangle_{L^2(\mathbf{R}, \mathbf{C})}$, donc par Cauchy-Schwarz, $|g(x)| \leq \|f\|_2^2$.
- $g(0) = \|f\|_2^2$.
- Comme $x \mapsto \tau_x f$ est continue, $g(x)$ est également continue par Cauchy-Schwarz.

- Introduction d'une approximation de l'unité et premier résultat

Posons $\rho_t : x \mapsto \frac{1}{\sqrt{4\pi t}} e^{-\frac{x^2}{4t}}$. C'est une approximation de l'unité qui vérifie $\mathcal{F}\rho_t(\xi) = e^{-t\xi^2}$. (**lemme à faire figurer dans le plan**).

Idée : On va calculer $\rho_t * g(0)$ de deux façons différentes pour obtenir ce qu'on veut.

Comme g est bornée et continue en 0, $\rho_t * g(0) \xrightarrow{t \rightarrow 0} g(0) = \|f\|_2^2$. **lemme à faire figurer dans le plan ? éventuellement à montrer, c'est pas long.**

- Inversion de Fourier et conclusion

Comme $\rho_t * g \in L^1$, par inversion de Fourier,

$$\rho_t * g(0) = \frac{1}{2\pi} \int_{\mathbf{R}} \mathcal{F}(\rho_t * g)(\xi) e^{i \cdot 0 \cdot \xi} d\xi = \frac{1}{2\pi} \int_{\mathbf{R}} e^{-t|\xi|^2} |\mathcal{F}(f)(\xi)|^2 d\xi.$$

Alors par le lemme de Fatou, on peut majorer $\|\mathcal{F}f\|_2^2$ par $(2\pi)^n \|f\|_2^2$ ce qui donne que $\mathcal{F}f \in L^2$. Par théorème de convergence dominée, on obtient donc que

$$\lim_{t \rightarrow 0} \rho_t * g(0) = \frac{1}{(2\pi)^n} \|\mathcal{F}f\|_2^2.$$

- Prolongement de la transformée de Fourier à L^2

On applique le théorème de prolongement des applications uniformément continues. On a :

- $L^1 \cap L^2$ est dense dans L^2 : si $f \in L^2$, $f_n = f \mathbb{1}_{[-n, n]} \in L^1 \cap L^2$ converge dans L^2 vers f ,
- L^2 est un espace de Banach,
- $\mathcal{F} : L^1 \rightarrow L^2$ est uniformément continue (linéaire et continue)

Ainsi peut-on prolonger la transformée de Fourier en une application linéaire continue de L^2 dans L^2 telle que pour tout $f \in L^2(\mathbf{R}^n)$,

$$\|\mathcal{F}(f)\|_{L^2} \leq (2\pi)^{\frac{n}{2}} \|f\|_{L^2}.$$

36 Théorème de Sharkowski

Leçons : 226, 228

Référence: Analyse 1, Francinou, Gianella, Nicolas

Théorème — Soit I un segment de $\mathbf{R}$ et $f : I \rightarrow I$ une fonction continue. Si f admet un point 3-périodique, alors il existe un point n -périodique pour tout $n \in \mathbf{N}^*$.

Pour commencer, on va montrer deux lemmes, dont voici le premier :

| **Lemme** — Soit K un segment inclus dans $f(I)$. Alors il existe un segment L inclus dans I tel que $K = f(L)$.

Démonstration — On note $K = [\alpha, \beta]$. Comme $K \subset f(I)$, il existe $a, b \in I$ tels que $\alpha = f(a)$ et $\beta = f(b)$.

Si $\alpha = \beta$, on a $K = \{\alpha\}$ donc $a = b$ et $L = \{a\}$ convient. Dans la suite, on suppose donc que $\alpha \neq \beta$ et donc $a \neq b$.

- Cas $a < b$

Posons $A = \{x \in [a, b] \mid f(x) = \beta\}$. C'est un fermé car image réciproque du fermé $\{\beta\}$ par l'application continue f . De plus, il est non vide car il contient b . Enfin, il est minoré par a par construction.

Posons $v = \min(A)$. On a $f(v) = \beta$ et $f(t) < \beta$ pour tout $t \in [a, v[$ (car sinon, par le théorème de la valeur intermédiaire, on aurait un élément $u < v$ d'image β par f).

De la même manière, posons $B = \{x \in [a, v] \mid f(x) = \alpha\}$. C'est un fermé non vide et majoré par v donc admet un plus grand élément u . On a alors $u < v$ et $f([u, v]) = [\alpha, \beta]$, donc le segment $L = [u, v]$ convient.

- Cas $a > b$

On procède de la même manière en prenant cette fois $u = \max\{x \in [b, a] \mid f(x) = \beta\}$ et $v = \min\{x \in [u, a] \mid f(x) = \alpha\}$.

□

Ensuite, on montre un second lemme :

| **Lemme** — Supposons qu'il existe n segments $I_0, \dots, I_{n-1}$ inclus dans I tels que

$$I_0 \subset f(I_{n-1}) \text{ et } I_{k+1} \subset f(I_k) \quad \forall k \in \llbracket 0, n-2 \rrbracket.$$

| Alors, f^n a un point fixe x_0 tel que $f^k(x_0) \in I_k$ pour tout $k \in \llbracket 0, n-1 \rrbracket$.

Démonstration —

- Cas $n = 1$

On dispose d'un segment $I_0 = [a, b]$ tel que $I_0 \subset f(I_0)$. En particulier, il existe α et β dans I_0 tels que $f(\alpha) = a$ et $f(\beta) = b$. La fonction $g = f - \text{Id}$ est alors une fonction continue sur I_0 et est négative en a et positive en b . Par le théorème de la valeur intermédiaire, g s'annule sur I_0 et f a un point fixe.

- Cas $n = 2$

On a $I_0 \subset f(I_1)$ et $I_1 \subset f(I_0)$, donc $I_0 \subset f^2(I_0)$. Par le premier cas, f^2 a un point fixe $x_0 \in I_0$. Cela dit, il n'y a pas de raison *a priori* pour que $f(x_0) \in I_1$.

Par le premier lemme, il existe un segment $J_1 \subset I_0$ tel que $f(J_1) = I_1$. On a donc $J_1 \subset I_0 \subset f(I_1) = f^2(J_1)$. Il existe donc x_0 point fixe de f^2 dans J_1 , et donc $f(x_0) \in I_1 = f(J_1)$.

- Cas général

Comme $I_1 \subset f(I_0)$, il existe un segment $J_1 \subset I_0$ tel que $f(J_1) = I_1$. On a alors

$$I_2 \subset f(I_1) = f^2(J_1).$$

On choisit alors $J_2 \subset J_1$ tel que $f^2(J_2) = I_2$.

En itérant ce procédé, on construit une suite finie de segments $J_{n-1} \subset \dots \subset J_1 \subset I_0$ telle que pour tout $k \in \llbracket 1, n-1 \rrbracket$, $f^k(J_k) = I_k$.

Enfin,

$$I_0 \subset f(I_{n-1}) = f^n(J_{n-1}),$$

donc il existe $J_n \subset J_{n-1}$ tel que $f^n(J_n) = I_0$. Alors, comme $J_n \subset I_0 = f^n(J_n)$, il existe un point fixe $x_0 \in J_n$ pour f^n , et par construction des J_k , pour tout $k \in \llbracket 0, n-1 \rrbracket$,

$$f^k(x_0) \subset I_k.$$

□

Passons à présent à la preuve du théorème.

Soit a un point 3-périodique de f . Posons $b = f(a)$ et $c = f(b)$. Quitte à permuter ces trois éléments (qui sont dans la même orbite), on suppose que $a = \min(a, b, c)$.

- Cas $a < b < c$

Posons $I_0 = [a, b]$ et $I_1 = [b, c]$. On remarque donc que $I_1 \subset f(I_0)$, $I_0 = [a, b] \subset f(I_1) = [a, c]$ et $I_1 \subset f(I_1)$. En particulier, la dernière inclusion nous donne l'existence d'un point fixe pour f .

Si on écrit $I_k \rightarrow I_j := I_k \subset f(I_j)$, on a un cycle

$$I_0 \rightarrow I_1 \rightarrow I_0,$$

donc par le deuxième lemme, il existe $x_0 \in I_0$ point fixe de f^2 tel que $f(x_0) \in I_1$. Comme $x_0 \neq b$ (sans quoi il ne serait pas point fixe de f^2), on déduit que $x_0 \notin I_1$ et donc $f(x_0) \neq x_0$, donc x_0 est un point 2-périodique.

Soit $n \geq 4$. On écrit le cycle

$$I_0 \rightarrow I_1 \rightarrow \dots \rightarrow I_1 \rightarrow I_0$$

avec $n-1$ apparitions de I_1 . Par le lemme, f^n admet un point fixe x_0 tel que $f^k(x_0) \in I_1$ pour tout $k \in \llbracket 1, n-1 \rrbracket$. Comme auparavant, on a $x_0 \neq b$ donc $x_0 \notin I_1$ donc il n'est jamais égal à $f^k(x_0)$, $k \in \llbracket 1, n-1 \rrbracket$. C'est donc un point n -périodique.

- Cas $a < c < b$

On pose $I_0 = [a, c]$ et $I_1 = [c, b]$. On a donc $I_1 \rightarrow I_0$, $I_0 \rightarrow I_0$ et $I_0 \rightarrow I_1$, donc on peut reprendre le point précédent en échangeant I_0 et I_1 .

f admet donc des points n -périodiques pour tout $n \in \mathbb{N}^*$.

37 Isométries du cube

Leçons : 101, 104, 105, 161, 191

Référence: **H2G2**, Caldero-Germoni

| **Théorème** — Les groupes d'isométrie du cube $\mathcal{C}$ sont $O(\mathcal{C}) \simeq \mathfrak{S}_4 \times \mathbf{Z}/2\mathbf{Z}$ et $SO(\mathcal{C}) \simeq \mathfrak{S}_4$.

| **Application** — Si on se donne n couleurs, le nombre de coloriage possibles du cube est

$$k = \frac{1}{24}(n^6 + 6n^3 + 8n^2 + 6n^3 + 3n^4).$$

On fait un dessin de cube en numérotant les sommets du haut A_i et ceux du bas B_i en commençant en bas à gauche puis dans le sens horaire.

- Construction d'une action

Les plus grandes distances que l'on peut trouver entre deux points du cube sont les grandes diagonales, qui sont au nombre de quatre. Les isométries du cube préservent donc les grandes diagonales (on envoie une diagonale sur une diagonale). On note $\mathcal{D} = \{D_1, D_2, D_3, D_4\}$ l'ensemble des grandes diagonales du cube, et on fait agir $SO(\mathcal{C})$ sur $\mathcal{D}$. Cela nous donne un morphisme de groupes

$$\varphi : SO(\mathcal{C}) \rightarrow \mathfrak{S}_4; g \mapsto g|_{\mathcal{D}}.$$

- Montrer que l'action est fidèle, i.e que φ est injective.

Soit g tel que $\varphi(g) = \text{Id}$. On note $D_i = A_i B_{4-i}$. Comme $g(D_i) = D_i$, soit g permute A_i et B_{4-i} soit il les laisse tels quels.

Supposons qu'il existe i tel que g laisse fixe A_i . On suppose $i = 1$ quitte à renuméroter. g laisse donc A_1 et B_3 fixes. Comme $A_1 A_2 \neq A_1 B_4$ et comme g est une isométrie, nécessairement $g(A_2) = A_2$ et $g(B_4) = B_4$. De même, A_2 et B_4 sont envoyés sur eux-mêmes. Comme (A_1, A_2, B_2, A_4) est un repère affine de l'espace, et qu'il est laissé fixe par g , on a $g = \text{Id}$.

Supposons à présent que g échange un couple de sommets selon la diagonale. Posons s_0 la symétrie centrale du cube. Alors, $s_0 \circ g$ préserve un couple de sommets donc est l'identité, ce qui est impossible car g est une isométrie positive.

En conclusion, $\text{Ker}(\varphi) = \{\text{Id}\}$ et donc $SO(\mathcal{C})$ est un sous-groupe de $\mathfrak{S}_4$.

- Montrer que φ est surjective

Il suffit de montrer que l'on réalise toute transposition de grandes diagonales.

Considérons la droite passant par le milieu de $[A_1 A_2]$ et $(B_3 B_4)$. La symétrie par rapport à cette est une isométrie positive (retournement) car elle préserve tout plan orthogonal à cette droite, donc le plan défini par les segments

$[A_3B_1]$ et $[A_4B_2]$ font partie. De plus, elle échange les diagonales (A_3B_1) et (A_4B_2) , c'est donc une transposition. On peut ainsi construire toutes les transpositions.

On a donc 24 isométries positives pour le cube, listées ci-dessous (dessins à l'appui) :

Type d'isométrie	Nombre
Identité	1
Rotations de 90° d'axe passant par les milieux de deux faces opposées	6
Rotations de 180° d'axe passant par les milieux de deux faces opposés	3
Rotations de 120° autour d'une grande diagonale	8
Rotations de 180° autour d'un axe passant par les milieux de deux arêtes opposées	6

- Cas des isométries

Le groupe $\text{SO}_3(\mathbf{R})$ est distingué dans $\text{O}_3(\mathbf{R})$ donc $\text{SO}(\mathcal{C}) = \text{O}(\mathcal{C}) \cap \text{SO}_3(\mathbf{R})$ est distingué dans $\text{O}(\mathcal{C})$ **et est d'indice 2**.

- Applications aux colorations du cube

Soit C un ensemble de n couleurs. On souhaite connaître le nombre de manières de colorier le cube avec n choix de couleurs (donc on peut faire un cube uni), sachant que si deux colorations s'obtiennent en appliquant une isométrie positive à l'autre, on considère que ce sont les mêmes. Autrement dit, on fait agir notre groupe des isométries positive sur l'ensemble des coloriages possibles des faces F :

$$\text{SO}(\mathcal{C}) \times \mathcal{F}(F, C); (g, f) \mapsto (x \mapsto f(g^{-1}x)).$$

On regarde les orbites de cette action, on souhaite en déterminer le nombre.

Par la formule de Burnside, le nombre d'orbites est

$$k = \frac{1}{|\text{SO}(\mathcal{C})|} \sum_{g \in \text{O}(\mathcal{C})} |\text{Fix}(g)|.$$

Or, un coloriage est dans le fixateur de g si et seulement si f est constante sur chaque orbite de faces pour l'action de g sur le cube. Si on note l ce nombre d'orbites, on a donc que $|\text{Fix}(g)| = |C|^l$. On détermine ce l pour chaque type d'isométrie, ce qui nous permet d'obtenir

$$k = \frac{1}{24}(n^6 + 6n^3 + 8n^2 + 6n^3 + 3n^4).$$

38 Ellipsoïde de John-Loewner

Leçons : 152, 158, 171, 219, 229, 253

Référence: Analyse pour l'agrégation, Bernis

Théorème — Soit $K \subset \mathbf{R}^N$ compact d'intérieur non vide. Alors il existe un et un seul ellipsoïde plein, centré en l'origine, de volume minimal, qui contienne K .

- Reformulation matricielle du problème

Soient q une forme quadratique définie positive et S sa matrice dans la base canonique. On note V_q le volume de l'ellipsoïde $\mathcal{E}_q$ associé à q et $\mathcal{V}$ le volume de la boule unité de $\mathbf{R}^N$ (qui est l'ellipsoïde associé à la forme quadratique $\|\cdot\|_2^2$).

Par un théorème de réduction, il existe une base orthonormée $\mathcal{B}_0$ pour le produit scalaire canonique et orthogonale pour la forme polaire associée à q . On a donc que

$$\text{Mat}_{\mathcal{B}_0}(q) = \text{diag}(\mu_1, \dots, \mu_N),$$

avec $\mu_1, \dots, \mu_N$ des réels strictement positifs. Donc, pour tout $X \in \mathbf{R}^N$,

$$q(X) = \sum_{i=1}^N \mu_i y_i^2,$$

avec y_i la i -ième coordonnée de X dans $\mathcal{B}_0$. On en déduit que

$$X \in \mathcal{E}_q \text{ si et seulement si } \sum_{i=1}^N (\sqrt{\mu_i} y_i)^2 \leq 1.$$

Posons $\Phi : \mathbf{R}^N \rightarrow \mathbf{R}^N$; $Z \mapsto P \text{diag} \left(\frac{1}{\sqrt{\mu_1}}, \dots, \frac{1}{\sqrt{\mu_N}} \right) Z$, où P est la matrice de passage de la base canonique à $\mathcal{B}_0$. $\Phi \in \text{GL}_N(\mathbf{R})$ car sa matrice est

$$\text{Mat}_{\mathcal{B}, \mathcal{B}_0}(\Phi) = P \text{diag} \left(\frac{1}{\sqrt{\mu_1}}, \dots, \frac{1}{\sqrt{\mu_N}} \right)$$

qui est inversible.

Φ est donc un $\mathcal{C}^1$ -difféomorphisme de $\mathbf{R}^N$ qui envoie la boule unité fermée sur $\mathcal{E}_q$ et avec

$$|\text{Jac}_\Phi| = \left| \det \left(P \text{diag} \left(\frac{1}{\sqrt{\mu_1}}, \dots, \frac{1}{\sqrt{\mu_N}} \right) \right) \right| = \prod_{i=1}^N \mu_i^{-\frac{1}{2}}.$$

En effet, P est une matrice de passage d'une base orthonormée à une autre donc est de déterminant ± 1 . En effectuant le changement de variables linéaire $X = \Phi(Z)$, on a

$$\begin{aligned} V_q &= \int_{\mathcal{E}_q} 1 \, dx_1 \dots dx_n, \\ &= \prod_{i=1}^N \mu_i^{-\frac{1}{2}} \int_B 1 \, dz_1 \, dz_n, \\ &= \frac{\mathcal{V}}{\sqrt{\det(S)}}. \end{aligned}$$

On se ramène donc à chercher la valeur maximale de l'application $\det$ sur l'ensemble des matrices symétriques définies positives telles que ${}^t X S X \leq 1$ pour tout élément X de K .

- Existence

Munissons $\mathcal{S}_N(\mathbf{R})$ de la norme d'opérateur subordonnée à $\|\cdot\|_2$. On travaille plutôt sur $\mathcal{S}_N^+(\mathbf{R})$ car c'est un ensemble fermé. On définit l'ensemble

$$\mathcal{C} = \{S \in \mathcal{S}_N^+(\mathbf{R}) \mid \forall X \in K, {}^t X S X \leq 1\}.$$

On va montrer que $\mathcal{C}$ est compact, c'est-à-dire fermé et borné car on travaille en dimension finie.

Soit $(S_n)_{n \in \mathbf{N}}$ une suite d'éléments de $\mathcal{C}$, qui converge vers un élément $S \in \mathcal{S}_N^+(\mathbf{R})$. Par l'inégalité de Cauchy-Schwarz, pour tout $X \in \mathbf{R}^N$ et tout $n \in \mathbf{N}$,

$$\|{}^tXS_nX - {}^tXSX\|_2 \leq \|(S - S_n)X\|_2\|X\|_2 \leq \|S - S_n\|\|X\|_2^2 \xrightarrow{n \rightarrow +\infty} 0.$$

Or, pour tout $X \in \mathbf{R}^n$ et tout $Y \in K$, ${}^tXS_nX \geq 0$ et ${}^tYS_nY \leq 1$, donc on a bien par passage à la limite que $S \in \mathcal{C}$. Donc $\mathcal{C}$ est fermé dans $\mathcal{S}_N^+(\mathbf{R})$.

Soit $S \in \mathcal{C}$ la matrice dans la base canonique d'une forme quadratique q . Comme K est d'intérieur non vide, il existe $A \in K$ et $r \in \mathbf{R}_+^*$ tel que $\overline{B(A, r)} \subset K \subset \mathcal{E}_q$. Comme $\mathcal{E}_q$ est symétrique par rapport à 0, il contient $\overline{B(-A, r)}$ et donc par convexité (c'est la boule unité pour la norme $\sqrt{q}$), il contient $\overline{B(0, r)}$. Or, cette boule est l'ellipsoïde associé à la forme quadratique $q' = \frac{\|\cdot\|_2^2}{r}$ et donc $\mathcal{E}_{q'} \subset \mathcal{E}_q$, et donc

$$q \leq q'.$$

On en déduit que

$$\|S\| = \sum_{\|X\|_2=1} q(x) \leq \sum_{\|X\|_2=1} \frac{\|X\|_2^2}{r^2} = \frac{1}{r^2}.$$

$\mathcal{C}$ est donc borné.

Reste à montrer que $\mathcal{C}$ est non vide. Par compacité de K , on dispose de $M \in \mathbf{R}_+^*$ tel que pour tout $X \in K$, $\|X\|_2 \leq M$. La matrice $\frac{1}{M^2}I_N$ est alors un élément de $\mathcal{C} \cap \mathcal{S}_N^{++}(\mathbf{R})$.

Par continuité du déterminant sur le compact $\mathcal{C}$, il existe $S_m \in \mathcal{C}$ qui maximise le déterminant. Cet élément est défini positif car

$$\det(S_m) \geq \det\left(\frac{1}{M^2}I_N\right) > 0.$$

• Unicité

Montrons tout d'abord que $\mathcal{C}$ est convexe. Soient S_1 et S_2 deux éléments de $\mathcal{C}$ et $\lambda \in]0, 1[$. On a $\lambda S_1 + (1 - \lambda)S_2 \in \mathcal{S}_N(\mathbf{R})$. De plus, pour tout $X \in \mathbf{R}^N$ et tout $Y \in K$, une simple vérification nous donne que

$${}^tX(\lambda S_1 + (1 - \lambda)S_2)X \geq 0 \text{ et } {}^tY(\lambda S_1 + (1 - \lambda)S_2)Y \leq 1,$$

donc on a bien un élément de $\mathcal{C}$.

Supposons à présent par l'absurde disposer de S_1 et S_2 distincts maximisant le déterminant. Par convexité de $\mathcal{C}$, $\frac{S_1 + S_2}{2} \in \mathcal{C}$. Par la partie précédente, S_1 et S_2 sont forcément définies positives donc il existe une base orthonormale $\mathcal{B}$ pour le produit scalaire associé à S_1 et orthogonale pour celui associé à S_2 , de telle sorte que

$$S_1 = {}^tPP \text{ et } S_2 = {}^tPDP$$

avec $D = \text{diag}(\lambda_1, \dots, \lambda_N)$. Remarquons que les λ_i sont tous strictement positifs et non tous égaux à 1. On en déduit que

$$\det(S_1)^{\frac{1}{2}} \det(S_2)^{\frac{1}{2}} = \det(P)^2 \det(D)^{\frac{1}{2}} \text{ et } \det\left(\frac{S_1 + S_2}{2}\right) = \det(P)^2 \det\left(\frac{I_N + D}{2}\right).$$

Comme $I_N \neq D$, par stricte concavité du logarithme,

$$\begin{aligned} \ln\left(\det\left(\frac{I_N + D}{2}\right)\right) &= \ln\left(\prod_{i=1}^N \frac{1 + \lambda_i}{2}\right), \\ &= \sum_{i=1}^N \ln\left(\frac{1 + \lambda_i}{2}\right), \\ &> \sum_{i=1}^N \frac{1}{2} \ln(1) + \frac{1}{2} \ln(\lambda_i). \end{aligned}$$

Donc,

$$\ln \left(\det \left(\frac{I_N + D}{2} \right) \right) > \ln \left(\prod_{i=1}^N \lambda_i^{\frac{1}{2}} \right) = \ln \left(\det(D)^{\frac{1}{2}} \right).$$

Par stricte croissance du logarithme, et en revenant à l'équation de départ, on obtient finalement que

$$\det \left(\frac{S_1 + S_2}{2} \right) > \det(D)^{\frac{1}{2}} \det(P)^2 = \det(S_1)^{\frac{1}{2}} \det(S_2)^{\frac{1}{2}} = \max_{S \in \mathcal{C}} \det(S).$$

D'où la contradiction.

39 Équation de Pell-Fermat

Leçons : 108, 126, 171, 191

Référence: Arithmétique, Marc Hindry

Théorème — Soit $d > 1$ un entier sans facteurs carrés. Alors, il existe un unique couple $(x_1, y_1) \in (\mathbf{N}^*)^2$ tel que les solutions de l'équation

$$x^2 - dy^2 = 1$$

sont exactement les $(\pm x_n, \pm y_n)$ où $x_n + \sqrt{d}y_n = (x_1 + \sqrt{d}y_1)^n$.

Remarquons que l'équation a deux solutions triviales qui sont $(\pm 1, 0)$. Dans la suite, on considérera uniquement des solutions (x, y) avec $y \neq 0$.

- Se ramener à la preuve d'un résultat d'approximation diophantienne de $\sqrt{d}$

Supposons que $x, y \in \mathbf{Z}$ vérifient $x^2 - dy^2 = 1$. Alors,

$$\begin{aligned} 0 < \frac{x}{y} - \sqrt{d} &= \frac{x - \sqrt{d}y}{y} \\ &= \frac{1}{(x + \sqrt{d}y)y} \\ &= \frac{1}{\left(\frac{x}{y} + \sqrt{d}\right)y^2} \\ &< \frac{1}{2\sqrt{d}y^2}, \end{aligned}$$

l'inégalité étant obtenue du fait que $x^2 + dy^2 > 0$, donc $\frac{x}{y} > \sqrt{d}$.

Réciproquement, si $0 < \frac{x}{y} - \sqrt{d} < \frac{1}{2\sqrt{d}y^2}$, alors

$$\begin{aligned} 0 < x^2 - dy^2 &= y^2 \left(\frac{x}{y} + \sqrt{d} \right) \left(\frac{x}{y} - \sqrt{d} \right), \\ &< \frac{1}{2\sqrt{d}} \left(2\sqrt{d} + \frac{1}{2\sqrt{d}y^2} \right), \\ &< 1 + \frac{1}{2dy^2} \end{aligned}$$

Or, $y \neq 0$ donc $y^2 \geq 1$ et $2dy^2 > 2$, donc $\frac{1}{2dy^2} < 1$. On en déduit que

$$0 < x^2 - dy^2 < 2,$$

d'où le résultat.

On cherche donc les couples (x, y) vérifiant

$$0 < \frac{x}{y} - \sqrt{d} < \frac{1}{2\sqrt{d}y^2}.$$

- Cadre de l'étude

Posons $K = \mathbf{Q}(\sqrt{d})$. Comme d n'a pas de facteurs carrés, K est une extension de $\mathbf{Q}$ de degré 2.

Notons, pour tout $a = x + \sqrt{d}y \in K$, m_a l'endomorphisme de K donné par la multiplication par a . La matrice de m_a dans la base $(1, \sqrt{d})$ est

$$\text{Mat}_{(1, \sqrt{d})}(m_a) = \begin{pmatrix} x & dy \\ y & x \end{pmatrix}.$$

Posons $N(a) = \det(m_a) = x^2 - dy^2$, $t(a) = \text{Tr}(m_a) = 2x$ et $\bar{a} = x - \sqrt{d}y$. On a :

- N est multiplicatif car $m_a \circ m_b = m_{ab}$ et le déterminant est multiplicatif.

- $N(a) = a\bar{a}$ pour tout $a \in K$, et $a \mapsto \bar{a}$ est multiplicatif.
- Si $a \in \mathbf{Z}[\sqrt{d}]$, alors $N(a)$ et $t(a)$ sont dans $\mathbf{Z}$;
- $P(a) = a^2 - t(a)a + N(a) = 0$: P est un polynôme annulateur de m_a .
- Pour tout $a \in \mathbf{Z}[\sqrt{d}]$, on a $a \in \mathbf{Z}[\sqrt{d}]^\times$ si et seulement si $N(a) = \pm 1$.

• Existence d'une solution non triviale

D'après un lemme classique d'approximation rationnelle, il existe une infinité de couples d'entiers (x, y) tels que

$$\left| \frac{x}{y} - \sqrt{d} \right| \leq \frac{1}{y^2}.$$

Un tel couple vérifie alors

$$|x^2 - dy^2| \leq |x - \sqrt{d}y| (|x + \sqrt{d}y| + |2\sqrt{d}y|) \leq 1 + 2\sqrt{d}.$$

Comme il existe une infinité de tels couples, par le principe des tiroirs, il existe $k \in \mathbf{N}^*$ tel que l'équation $x^2 - dy^2 = k$ a une infinité de solutions.

Soient (x_0, y_0) et (x_1, y_1) deux couples solutions de l'équation ci-dessus. Comme les classes de congruence modulo k sont en nombre fini et que le nombre de solutions de l'équation est infini, on peut choisir les deux couples de sorte que $x_0 \equiv x_1[k]$ et $y_0 \equiv y_1[k]$.

On pose

$$u + \sqrt{d}v = \frac{x_0 + \sqrt{d}y_0}{x_1 + \sqrt{d}y_1}.$$

On a $N(u + \sqrt{d}v) = \frac{k}{k} = 1$. De plus, $u + \sqrt{d}v \in \mathbf{Z}[\sqrt{d}]$. En effet,

$$u + \sqrt{d}v = \frac{x_0x_1 - dy_0y_1}{k} + \sqrt{d} \frac{y_0x_1 - x_0y_1}{k},$$

et comme les couples sont congrus modulo k ,

$$\begin{cases} x_0x_1 - dy_0y_1 & \equiv & x_0^2 - dy_0^2 & \equiv & 0[k] \\ x_1y_0 - x_0y_1 & \equiv & x_0y_0 - x_0y_0 & \equiv & 0[k]. \end{cases}$$

D'où l'existence d'une solution non triviale ($x_1y_0 - x_0y_1 \neq 0$ car sinon les deux solutions seraient proportionnelles).

• Description de l'ensemble des solutions

On définit le morphisme

$$L : \begin{cases} \mathbf{Z}[\sqrt{d}]^\times & \longrightarrow & \mathbf{R}^2, \\ a & \mapsto & (\log |a|, \log |\bar{a}|) \end{cases}$$

$\text{Im}(L)$ est un sous-groupe discret de $\mathbf{R}^2$. En effet, si $R > 0$, et que $a \in L^{-1}(B(0, R))$, alors $|a| \leq e^{\mathbf{R}}$ et $|\bar{a}| \leq e^{\mathbf{R}}$, donc $|t(a)| \leq 2e^{\mathbf{R}}$. Par suite, il n'existe qu'un nombre fini de $t(a)$ possibles, donc un nombre fini de polynômes annulateurs P possibles (car $N(a)$ est fixé à 1), et donc un nombre fini de racines de ces polynômes.

$\text{Ker}(L)$ est réduit à ± 1 . En effet, $-1 \in \text{Ker}(L)$ et $\text{Ker}(L)$ est un sous-groupe d'un groupe multiplicatif, donc $\{\pm 1\} \subset \text{Ker}(L)$. De plus, $\text{Ker}(L) = L^{-1}(\{0\}) \subset L^{-1}(B(0, R))$, c'est un sous-groupe fini de $\mathbf{R}^*$, donc il est inclus dans $\{\pm 1\}$.

De plus, $\text{Im}(L)$ est inclus dans la droite $x + y = 0$ car $\log |a| + \log |\bar{a}| = \log |N(a)| = 0$. Donc, $\text{Im}(L)$ est isomorphe à un sous-groupe discret de $\mathbf{R}$ et est donc monogène.

$\mathbf{Z}[\sqrt{d}]^\times / \text{Ker}(L)$ est donc isomorphe à un sous-groupe discret de $\mathbf{R}$, et est donc monogène, non réduit à $\{0\}$ grâce à l'existence d'une solution non triviale. Il existe donc $a_1 = x_1 + \sqrt{d}y_1 \in \mathbf{Z}[\sqrt{d}]^\times$ tel que $\text{Im}(L) = L(a_1)\mathbf{Z}$ et donc $\mathbf{Z}[\sqrt{d}]^\times = \pm a_1^{\mathbf{Z}}$. Comme l'inverse de a_1 est $\bar{a}_1$ et que l'ajout d'un signe plus ou moins importe peu, on peut choisir pour a_1 l'unique générateur tel que $x_1, y_1 \in \mathbf{N}^*$.

40 Décomposition polaire

Leçons : 158,160

Référence: H2G2 tome 1, Caldero-Germoni

Théorème — *La multiplication matricielle induit un homéomorphisme*

$$\mu : O_n(\mathbf{R}) \times S_n^{++}(\mathbf{R}) \longrightarrow GL_n(\mathbf{R}), (O, S) \longmapsto OS.$$

Corollaire — *Pour toute matrice inversible de $M_n(\mathbf{R})$, on a $\|A\|_2 = \sqrt{\rho({}^tAA)}$.*

Tout d'abord, μ est bien définie et continue car la multiplication est continue (à virer si besoin).

- Surjectivité

Soit $M \in GL_n(\mathbf{R})$. La matrice ${}^tMM$ est symétrique, de valeurs propres positives (${}^t x {}^tMMx = \|Mx\|_2^2 \geq 0$), et inversible, donc de valeurs propres strictement positives.

On peut donc par le théorème spectral diagonaliser ${}^tMM$ dans une base orthonormée :

$${}^tMM = P \operatorname{diag}(\lambda_1, \dots, \lambda_n) P^{-1}, P \in O_n(\mathbf{R}).$$

Posons

$$S = P \operatorname{diag}(\sqrt{\lambda_1}, \dots, \sqrt{\lambda_n}) P^{-1}.$$

S est symétrique définie positive, avec $S^2 = {}^tMM$.

Si l'on pose $O = MS^{-1}$, on obtient ${}^tOO = {}^tS^{-1} {}^tMM S^{-1} = S^{-1} S^2 S^{-1} = I_n$, i.e $O \in O_n(\mathbf{R})$. D'où la surjectivité.

- Injectivité de μ

Supposons que l'on ait $M = OS = O'S'$. Alors, $S^2 = {}^tMM = {}^tS'S' = S'^2$. Posons L le polynôme de Lagrange tel que pour tout $i \in \llbracket 1, n \rrbracket$, $Q(\lambda_i) = \sqrt{\lambda_i}$. Alors,

$$S = P \operatorname{diag}(L(\lambda_1), \dots, L(\lambda_n)) P^{-1} = L({}^tMM) = L(S^2) = L(S'^2).$$

Donc S et S' commutent, donc sont codiagonalisables. En notant μ_i les valeurs propres de S et μ'_i celles de S' , la diagonalisation simultanée permet de dire que $\mu_i = \mu'_i$ pour tout $i \in \llbracket 1, n \rrbracket$, donc $S = S'$. On en déduit immédiatement que $O = O'$.

- Continuité de l'inverse

Soit $(M_p)_{p \in \mathbf{N}}$ une suite de $GL_n(\mathbf{R})$ qui converge M . On note, pour tout $p \in \mathbf{N}$, $(O_p, S_p) = \mu^{-1}(M_p)$ et puis $(O, S) = \mu^{-1}(M)$.

Par compacité de $O_n(\mathbf{R})$, il existe une valeur d'adhérence $\bar{O}$ de la suite (O_p) . En notant $\bar{S} = \bar{O}^{-1}M$, on a une deuxième décomposition polaire, donc par unicité tout est bon.

- Preuve du corollaire

Soit $A = OS$. Comme O est une isométrie, $\|A\|_2 = \|S\|_2$. En diagonalisant S dans une base orthonormée de sorte que $|\lambda_1| \geq \dots \geq |\lambda_n|$, on voit que pour tout $x \in \mathbf{R}^n$, $\|Sx\|_2 = \sum_{i=1}^n \lambda_i^2 |P^{-1}x_i| \leq |\lambda_1| \|x\|_2$. On a égalité pour $x = e_1$. Au final,

$$\rho(S) = |\lambda_1| = \sqrt{\lambda_1^2} = \sqrt{\rho(S^2)} = \sqrt{\rho({}^tAA)}.$$

remarque : autre possibilité : tout sous-groupe compact maximal de GL_n est conjugué à un sous-groupe de O_n

41 Enveloppe convexe de $O_n(\mathbf{R})$

Leçons : 158,159,160

Référence: Algèbre, Szpirglas

| **Lemme** — Toute forme linéaire sur $M_n(\mathbf{K})$ est de la forme $M \mapsto \text{Tr}(AM)$ avec $A \in M_n(\mathbf{K})$.

| **Théorème** — L'enveloppe convexe de $O_n(\mathbf{R})$ est la boule unité de $M_n(\mathbf{R})$ pour la norme $\|\cdot\|_2$.

- Une première inclusion

La boule unité de $M_n(\mathbf{R})$ pour la norme euclidienne est convexe et contient $O_n(\mathbf{R})$ donc comme l'enveloppe convexe d'un ensemble est le plus petit convexe contenant ce dernier, on a bien que l'enveloppe convexe de $O_n(\mathbf{R})$ est incluse dans la boule unité de $M_n(\mathbf{R})$.

- Traduction de l'énoncé

Soit $M \in B(0, 1)$. Si $M \notin O_n(\mathbf{R})$, on peut par le théorème de Hahn-Banach séparer strictement le convexe compact $\{M\}$ du convexe fermé $\text{Conv}(O_n(\mathbf{R}))$ par un hyperplan. Autrement dit, il existe une forme linéaire φ telle que $\sum_{B \in O_n(\mathbf{R})} \varphi(B) < \varphi(M)$. On veut donc montrer la contraposée : pour toute forme linéaire φ ,

$$\varphi(M) \leq \sup_{B \in O_n(\mathbf{R})} \varphi(B).$$

En utilisant le lemme, on souhaite donc montrer que

$$\forall B \in M_n(\mathbf{R}), \text{Tr}(AM) \leq \sup_{B \in O_n(\mathbf{R})} \text{Tr}(AB).$$

- Décomposition polaire

On fixe $A \in M_n(\mathbf{R})$ et on lui applique le théorème de décomposition polaire : $A = OS$ avec $O \in O_n(\mathbf{R})$ et $S \in S_n^{++}(\mathbf{R})$. Comme S est symétrique, on dispose d'une base (e_i) orthonormée de vecteurs propres de S .

Par le théorème de Cauchy-Schwarz, on a alors que

$$\text{Tr}(AM) = \text{Tr}(MA) = \sum_{i=1}^n \langle MAe_i, e_i \rangle = \sum_{i=1}^n \langle Ae_i, M^*e_i \rangle \leq \sum_{i=1}^n \|Ae_i\|_2 \|M^*e_i\|_2 \leq \sum_{i=1}^n \|Ae_i\|_2^2,$$

car $\|M^*\|_2 = \|M\|_2$.

Or, $\|Ae_i\| = \|O(Se_i)\| = \|Se_i\|$ pour tout $i \in \llbracket 1, n \rrbracket$, et

$$\sup_{B \in O_n(\mathbf{R})} \text{Tr}(AB) = \text{Tr}(O^{-1}OS) = \text{Tr}(S) = \sum_{i=1}^n \|Se_i\|.$$

On a bien montré le résultat souhaité.

42 Dénombrement des polynômes irréductibles unitaires sur un corps fini

Leçons : 123, 141, 190

Référence: Mathématiques pour l'agrégation : Algèbre et géométrie, Rombaldi

Posons $P_n(X) = X^{p^n} - X \in F_p[X]$. On note $\mathcal{U}_d(p)$ l'ensemble de tous les polynômes irréductibles unitaires de degré d dans $F_p[X]$ et $I_d(p) = \text{Card}(\mathcal{U}_d(p))$.

Lemme — *Tout diviseur irréductible de P_n dans $F_p[X]$ est de degré divisant n . Réciproquement, pour tout diviseur d de n , tout polynôme $P \in \mathcal{U}_d(p)$ divise P_n .*

Théorème — *P_n est sans facteur carré dans $F_p[X]$ et on a la décomposition en facteurs irréductibles,*

$$P_n = \prod_{d|n} \prod_{P \in \mathcal{U}_d(p)} P.$$

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

$$I_n(p) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d.$$

On en déduit que pour tout n , il existe un polynôme irréductible de degré n et on a $I_n(p) \sim \frac{p^n}{n}$.

Démonstration — Preuve du lemme

- Sens direct

Soit $P \in \mathcal{U}_d(p)$ qui divise P_n dans $F_p[X]$. Alors, $\overline{P_n} = \overline{0}$ dans $F_p[X]/(P) = F_{p^d}$, i.e

$$\overline{X^{p^n}} = \overline{x}.$$

On va montrer que tout élément de F_{p^d} vérifie cela.

Comme $(\overline{X}^k)_{0 \leq k \leq d-1}$ est une base du F_p -espace vectoriel F_{p^d} , tout élément $\overline{Q} \in F_{p^d}$ s'écrit $\overline{Q} = \sum_{k=0}^{d-1} a_k \overline{X}^k$, et donc comme F_{p^d} est de caractéristique p , par le morphisme de Fröbenius et le théorème de Fermat,

$$\overline{Q}^{p^n} = \sum_{k=0}^{d-1} (a_k)^{p^n} (\overline{X}^k)^{p^n} = \sum_{k=0}^{d-1} a_k (\overline{X}^{p^n})^k = \overline{Q}.$$

On en déduit que pour tout $\overline{Q} \in F_{p^d}^\times$, $\overline{Q}^{p^n-1} = \overline{1}$.

Le groupe multiplicatif $F_{p^d}^\times$ étant cyclique d'ordre $p^d - 1$, en notant ξ un générateur du groupe, on a $\xi^{p^n-1} = 1$ et donc $p^d - 1 \mid p^n - 1$, i.e $d \mid n$.

- Réciproque

Soit $P \in \mathcal{U}_d(p)$ avec d un diviseur de n . Comme $F_{p^d} = F_p[X]/(P)$ est un corps de cardinal p^d , son groupe multiplicatif est d'ordre $p^d - 1$ et donc

$$\overline{X}^{p^d-1} = \overline{1}$$

par le théorème de Lagrange. On en déduit que $\overline{X}^{p^d} = \overline{X}$, et par itération, pour tout $k \in \mathbb{N}^*$,

$$\overline{X}^{p^{kd}} = \overline{X}.$$

En prenant $k = \frac{n}{d}$, on obtient que $\overline{X}^{p^n} - X = \overline{0}$ dans F_{p^d} , i.e $P \mid P_n$.

□

Démonstration — Preuve du théorème

Comme $P'_n(X) = p^n X^{p^n-1} - 1 = -1$ dans $F_p[X]$, on a $P_n \wedge P'_n = 1$ donc P_n est sans facteur carré dans $F_p[X]$. On déduit alors du lemme précédent que

$$X^{p^n} - X = \prod_{d|n} \prod_{P \in \mathcal{U}_d(p)} P \text{ dans } F_p[X].$$

□

Démonstration — Preuve du corollaire

- Relation vérifiée par $I_n(p)$.

En prenant les degrés, on obtient que

$$p^n = \sum_{d|n} \sum_{P \in \mathcal{U}_d(p)} \deg(P) = \sum_{d|n} d \cdot I_d(p)$$

. Par la formule d'inversion de Möbius, on obtient alors :

$$nI_n(p) = \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d = \sum_{d|n} \mu(d) p^{\frac{n}{d}}.$$

- Conclusion

Pour l'existence, cela revient à montrer que $I_n(p) \geq 1$ pour tout $n \in \mathbb{N}^*$.

Pour $n = 1$ et $n = 2$, $I_1(p) = p \geq 2$ et $I_2(p) = \frac{p(p-1)}{2} \geq 1$.

Pour $n \geq 3$, on a $nI_n(p) = p^n + \sum_{\substack{d|n \\ d \neq n}} \mu\left(\frac{n}{d}\right) p^d$. Or,

$$\left| \sum_{\substack{d|n \\ d \neq n}} \mu\left(\frac{n}{d}\right) p^d \right| \leq \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} p^k = p^{\frac{\lfloor \frac{n}{2} \rfloor - 1}{p-1}} < p^{\lfloor \frac{n}{2} \rfloor + 1} \leq p^{\frac{n}{2} + 1}. \quad (3)$$

On en déduit que

$$nI_n(p) > p^n - p^{\frac{n}{2} + 1} \geq 0,$$

donc il existe bien un polynôme irréductible unitaire de tout degré dans $F_p[X]$.

De plus, toujours par l'équation (3),

$$\left| \frac{nI_n(p)}{p^n} - 1 \right| < \frac{p^{\frac{n}{2} + 1}}{p^n} \xrightarrow{n \rightarrow +\infty} 0.$$

D'où l'équivalence.

□

43 Algorithme de descente de gradient à pas optimal

Leçons : 149, 158, 219, 226, 229, 233, 253

Référence: Analyse pour l'agrégation, Bernis

Théorème — Soit $A \in S_n^{++}(\mathbf{R})$ et soit $b \in \mathbf{R}^n$. Notons λ_{max} et λ_{min} la plus grande et la plus petite de ses valeurs propres. Notons

$$\Phi : \mathbf{R}^n \rightarrow \mathbf{R}; x \mapsto \frac{1}{2} \|x\|_A^2 - \langle b, x \rangle.$$

. Enfin, notons $\bar{x}$ l'unique solution du système linéaire $Ax = b$. Alors,

1. Φ atteint son minimum en $\bar{x}$ et seulement en ce point;
2. Soit $a \in \mathbf{R}^n$ distinct de $\bar{x}$. On définit la suite $(x_k)_{k \in \mathbf{N}}$ par

$$\begin{cases} x_0 &= a, \\ \alpha_k &= \frac{\|\nabla \Phi(x_k)\|^2}{\|\nabla \Phi(x_k)\|_A^2} \text{ si } x_k \neq \bar{x}, 0 \text{ sinon,} \\ x_{k+1} &= x_k - \alpha_k \nabla \Phi(x_k). \end{cases}$$

Alors la suite converge vers $\bar{x}$ et pour tout $k \in \mathbf{N}$,

$$\|x_{k+1} - \bar{x}\| \leq \sqrt{\frac{\lambda_{max}}{\lambda_{min}}} \left(\frac{\lambda_{max} - \lambda_{min}}{\lambda_{max} + \lambda_{min}} \right)^{k+1} \|x_0 - \bar{x}\|.$$

- Calcul du gradient de Φ et preuve du premier point

On calcule le gradient pour le produit scalaire canonique (**car le gradient dépend du produit scalaire !**).

Notons $\langle \cdot, \cdot \rangle_A = \langle \cdot, A \cdot \rangle$. C'est un produit scalaire car $A \in S_n^{++}(\mathbf{R})$. On note $\|\cdot\|_A$ la norme associée.

Soit $x \in \mathbf{R}^n$, pour tout $h \in \mathbf{R}^n$,

$$\begin{aligned} \Phi(x+h) &= \frac{1}{2} \|x+h\|_A^2 - \langle b, x+h \rangle, \\ &= \frac{1}{2} \|x\|_A^2 + \langle x, h \rangle_A + \frac{1}{2} \|h\|_A^2 - \langle b, x \rangle - \langle b, h \rangle, \\ &= \Phi(x) + \langle Ax - b, h \rangle + \frac{1}{2} \|h\|_A^2, \\ &= \Phi(x) + \langle Ax - b, h \rangle + o(\|h\|). \end{aligned}$$

On en déduit que $\nabla \Phi(x) = Ax - b = A(x - \bar{x})$, donc $\nabla \Phi$ s'annule en $\bar{x}$ et seulement en ce point. En particulier, $\nabla \Phi(\bar{x}) = 0$ et

$$\Phi(\bar{x} + h) = \Phi(\bar{x}) + \frac{1}{2} \|h\|_A^2.$$

On en déduit le premier point.

- Preuve du lemme de Kankorovitch

Le lemme suivant sera à mettre en amont dans le plan :

Lemme — (Inégalité de Kankorovitch) Pour tout élément $x \in \mathbf{R}^n$ non nul, on a

$$\frac{\|x\|^4}{\|x\|_{A^{-1}}^2 \|x\|_A^2} \geq \frac{\lambda_{max} \lambda_{min}}{(\lambda_{max} + \lambda_{min})^2}.$$

Démonstration — Soit $x \in \mathbf{R}^n$ non nul. Par le théorème spectral, la matrice A admet une base orthonormée $(e_1, \dots, e_n)$ de vecteurs propres, associés aux valeurs propres $(\lambda_1, \dots, \lambda_n)$. Remarquons également que e_i est aussi vecteur propre de A^{-1} associé à la valeur propre $\frac{1}{\lambda_i}$. En notant $x = (x_1, \dots, x_n)$ dans cette base, on a

$$\begin{aligned} \|x\|_A \|x\|_{A^{-1}} &= \sqrt{\sum_{i=1}^n \lambda_i x_i^2} \sqrt{\sum_{i=1}^n \frac{1}{\lambda_i} x_i^2}, \\ &= \sqrt{\frac{\lambda_{max}}{\lambda_{min}}} \sqrt{\sum_{i=1}^n \frac{\lambda_i}{\lambda_{max}} x_i^2} \sqrt{\sum_{i=1}^n \frac{\lambda_{min}}{\lambda_i} x_i^2}. \end{aligned}$$

Comme $2ab \leq a^2 + b^2$,

$$\|x\|_A \|x\|_{A^{-1}} = \frac{1}{2} \sqrt{\frac{\lambda_{\max}}{\lambda_{\min}}} \sum_{i=1}^n \left(\frac{\lambda_i}{\lambda_{\max}} + \frac{\lambda_{\min}}{\lambda_i} \right) x_i^2.$$

Or, l'application $g : [\lambda_{\min}, \lambda_{\max}] \rightarrow \mathbf{R}; t \mapsto \frac{t}{\lambda_{\max}} + \frac{\lambda_{\min}}{t}$ est convexe et comme $g(\lambda_{\min}) = g(\lambda_{\max}) = 1 + \frac{\lambda_{\min}}{\lambda_{\max}}$, pour tout $t \in [\lambda_{\min}, \lambda_{\max}]$,

$$g(t) \leq 1 + \frac{\lambda_{\min}}{\lambda_{\max}}.$$

Au final,

$$\|x\|_A \|x\|_{A^{-1}} = \frac{1}{2} \sqrt{\frac{\lambda_{\max}}{\lambda_{\min}}} \left(1 + \frac{\lambda_{\min}}{\lambda_{\max}} \right) \|x\|^2.$$

On obtient l'égalité souhaitée en élevant au carré.

□

- Convergence en norme $\|\cdot\|_A$.

Notons $g_k = \nabla \Phi(x_k)$. Soit $p \in \mathbf{N}$. On écrit

$$\|x_{p+1} - \bar{x}\|_A^2 = \langle A(x_{p+1} - \bar{x}), x_{p+1} - x_p \rangle + \langle A(x_{p+1} - \bar{x}), x_p - \bar{x} \rangle,$$

or $\langle A(x_{p+1} - \bar{x}), x_{p+1} - x_p \rangle = \alpha_p \langle g_{p+1}, g_p \rangle = 0$ (explication qualitative du bouquin à lire). Par symétrie de A , on obtient alors que

$$\begin{aligned} \|x_{p+1} - \bar{x}\|_A^2 &= \langle A(x_{p+1} - x_p), x_p - \bar{x} \rangle + \langle A(x_p - \bar{x}), x_p - \bar{x} \rangle, \\ &= \langle x_{p+1} - x_p, A(x_p - \bar{x}) \rangle + \|x_p - \bar{x}\|_A^2, \\ &= -\alpha_p \langle g_p, g_p \rangle + \|x_p - \bar{x}\|_A^2, \\ &= -\frac{\|g_p\|^4}{\|g_p\|_A^2} + \|x_p - \bar{x}\|_A^2. \end{aligned}$$

Par ailleurs,

$$\|x_p - \bar{x}\|_A^2 = \langle A(x_p - \bar{x}), x_p - \bar{x} \rangle = \langle A(x_p - \bar{x}), A^{-1}A(x_p - \bar{x}) \rangle = \|g_p\|_{A^{-1}}^2,$$

donc

$$\|x_{p+1} - \bar{x}\|_A^2 = \left(1 - \frac{\|g_p\|^4}{\|g_p\|_A^2 \|g_p\|_{A^{-1}}^2} \right) \|x_p - \bar{x}\|_A^2.$$

Par l'inégalité de Kankorovitch, on obtient alors que

$$\|x_{p+1} - \bar{x}\|_A \leq \left(\frac{\lambda_{\max} - \lambda_{\min}}{\lambda_{\max} + \lambda_{\min}} \right) \|x_p - \bar{x}\|_A.$$

- Convergence en norme euclidienne

On a $\sqrt{\lambda_{\min}} \|\cdot\| \leq \|\cdot\|_A \leq \sqrt{\lambda_{\max}} \|\cdot\|$, donc par récurrence immédiate du paragraphe précédent, pour tout $k \in \mathbf{N}$,

$$\|x_{k+1} - \bar{x}\| \leq \sqrt{\frac{\lambda_{\max}}{\lambda_{\min}}} \left(\frac{\lambda_{\max} - \lambda_{\min}}{\lambda_{\max} + \lambda_{\min}} \right)^{k+1} \|x_0 - \bar{x}\|.$$

On a donc convergence en vitesse géométrique.

44 Nombres de Bell

Leçons : 190,241, 243

Référence: Analyse pour l'agrégation, Bernis

Théorème — Pour tout $n \in \mathbf{N}^*$, on note B_n le nombre de relations d'équivalence sur un ensemble à n éléments. Par convention, $B_0 = 1$. Alors,

1. Pour tout $n \in \mathbf{N}$,

$$B_{n+1} = \sum_{k=0}^n \binom{n}{k} B_{n-k}.$$

2. La série entière de la variable réelle t , $\sum_{n \geq 0} \frac{B_n}{n!} t^n$, a un rayon de convergence non nul et sa somme S vérifie :

$$\forall t \in]-R, R[, S'(t) = \exp(t)S(t).$$

3. Pour tout entier naturel $n \in \mathbf{N}$,

$$B_n = \frac{1}{e} \sum_{p=0}^{\infty} \frac{p^n}{p!} \text{ (formule de Doblinski).}$$

- Compter les relations d'équivalence revient exactement à compter les partitions de $\llbracket 1, n \rrbracket$.

En effet, l'ensemble des classes d'équivalence pour une relation d'équivalence est une partition de l'ensemble.

Réciproquement, en posant $x \sim y$ si x et y sont dans le même ensemble de la partition, on a construit une relation d'équivalence.

- Preuve du premier point

Soient $n \in \mathbf{N}$ et $\mathcal{P}_{n+1}$ l'ensemble des partitions de $\llbracket 1, n+1 \rrbracket$. Pour dénombrer $\mathcal{P}_{n+1}$, on va classer les partitions en fonction du cardinal de l'ensemble contenant $n+1$.

On note $\mathcal{P}_{n+1,k}$ l'ensemble des partitions telles que l'ensemble contenant $n+1$ est à $k+1$ éléments. On a $\mathcal{P}_{n+1} = \bigsqcup_{k=0}^n \mathcal{P}_{n+1,k}$.

Soit $k \in \llbracket 0, n \rrbracket$. Soit $P \in \mathcal{P}_{n+1,k}$ une partition. On note A l'ensemble de P contenant $n+1$, qui est de cardinal $k+1$. Alors, P est la réunion de $\{A\}$ et d'une partition du complémentaire de A , qui est de déterminant $n-k$.

On a $\binom{n}{k}$ choix pour A (on choisit les éléments qu'on met avec $n+1$), donc

$$|\mathcal{P}_{n+1,k}| = \binom{n}{k} B_{n-k}.$$

On en déduit que

$$|\mathcal{P}_{n+1}| = \sum_{k=0}^n \binom{n}{k} B_{n-k}.$$

- Preuve du deuxième point

Il suffit de montrer que $B_n \leq n!$.

On va pour cela montrer que l'ensemble $\mathcal{P}_n$ s'injecte dans $\mathfrak{S}_n$.

Soit $n \in \mathbf{N}^*$. Notons, pour $A \subset \llbracket 1, n \rrbracket$, c_A le cycle de support $(a_1, \dots, a_d)$ où les a_i sont les éléments de A énumérés dans l'ordre croissant. Alors, la fonction qui à une partition $P = \{A_1, \dots, A_k\}$ associe la permutation $\sigma = c_{A_1} \dots c_{A_p}$ est une injection comme conséquence de l'unicité de la décomposition d'une permutation en produit de cycles à supports disjoints.

On en déduit que $B_n \leq n!$. On en déduit que $\frac{B_n}{n!} = O(1)$, donc le rayon de convergence de la série entière est supérieur ou égal à celui de $\sum_n t^n$ qui vaut 1.

Par dérivation terme à terme de X dans l'intervalle ouvert de convergence,

$$S'(t) = \sum_{n=0}^{\infty} \frac{(n+1)B_{n+1}}{(n+1)!} t^n = \sum_{n=0}^{\infty} \frac{1}{n!} \sum_{k=0}^n \binom{n}{k} B_{n-k} t^n = \sum_{n=0}^{\infty} \sum_{k=0}^n \frac{1}{k!} \frac{B_{n-k}}{(n-k)!} t^n.$$

Ainsi S' apparaît-elle comme le produit de Cauchy des séries entières S et $\exp$.

- Preuve du troisième point.

D'après le deuxième point, S est la solution sur $] - R, R[$ du problème de Cauchy linéaire

$$\begin{cases} y'(t) &= \exp(t)y; \\ y(0) &= 1 \end{cases}$$

Donc, S coïncide sur $] - R, R[$ avec $\frac{1}{e} \exp \circ \exp$.

Or, pour tout réel $t \in \mathbf{R}$,

$$\exp(\exp(t)) = \sum_{p=0}^{\infty} \sum_{n=0}^{\infty} \frac{p^n t^n}{n! p!} t^n,$$

donc par unicité du développement en série entière, $R = +\infty$, $S = \frac{1}{e} \exp \circ \exp$ et pour tout $n \in \mathbf{N}$,

$$B_n = \frac{1}{e} \sum_{p=0}^{\infty} \frac{p^n}{p!},$$

ce qui achève la preuve.

Remarque : B_n est le moment d'ordre n d'une loi de poisson e paramètre 1.

45 Système de congruences

Leçons : 120, 126, 142

Référence: Carnet de voyage en algèbre, Caldero, Perroni

Théorème — Soient m et n deux entiers quelconques. On note $\mu = \text{ppcm}(m, n)$ et $\delta = \text{pgcd}(m, n)$. On a une suite exacte courte (d'anneaux)

$$1 \rightarrow \mathbf{Z}/\mu\mathbf{Z} \xrightarrow{\varphi} \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z} \xrightarrow{\psi} \mathbf{Z}/\delta\mathbf{Z} \rightarrow 1.$$

Corollaire — Si $a \equiv b[\delta]$, alors le système

$$\begin{cases} x \equiv a & [m], \\ x \equiv b & [n] \end{cases}$$

a des solutions

Application — Le système $\begin{cases} x \equiv 2 & [21], \\ x \equiv 11 & [35] \end{cases}$ n'a pas de solution.

En revanche, le système $\begin{cases} x \equiv 3 & [21], \\ x \equiv 10 & [35] \end{cases}$ est résoluble dans $\mathbf{Z}$.

Démonstration — Preuve du théorème

- Construire le morphisme φ

On considère le morphisme d'anneaux $\tilde{\varphi} : \mathbf{Z} \rightarrow \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}; x \mapsto (\bar{x}^m, \bar{x}^n)$.

Soit $n \in \text{Ker}(\tilde{\varphi})$. Alors, $m \mid x$ et $n \mid x$, donc $\mu \mid x$. Donc, $\mu\mathbf{Z} \subset \text{Ker}(\tilde{\varphi})$. Réciproquement, si $x \in \mu\mathbf{Z}$, on a nécessairement que $x \in \text{Ker}(\tilde{\varphi})$. Par passage au quotient, on construit donc un morphisme d'anneaux

$$\varphi : \mathbf{Z}/\mu\mathbf{Z} \rightarrow \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$$

injectif.

- Construire le morphisme ψ

Posons

$$\psi : \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z} \rightarrow \mathbf{Z}/\delta\mathbf{Z}; (\bar{x}^m, \bar{y}^n) \mapsto \bar{x}^\delta - \bar{y}^\delta.$$

ψ est bien défini, en effet si a et b sont deux représentants distincts de $\bar{x}^m$, on a $a = x + km$ et $b = x + qm$ et comme $\delta \mid m$, $\bar{a}^\delta = \bar{b}^\delta$. Il en va de même pour y car $\delta = \text{pgcd}(m, n)$.

ψ est un morphisme car $\bar{x}^m \mapsto \bar{x}^\delta$ en est un et pareil pour n .

Montrons à présent que ψ est surjectif. Soit $\bar{z}^\delta \in \mathbf{Z}/\delta\mathbf{Z}$. Soit z un représentant de la classe. Alors $\psi(\bar{z}^m, 0)$ fonctionne.

- Montrer que $\text{Im}(\varphi) = \text{Ker}(\psi)$

On voit que $\text{Im}(\varphi) = \{(\bar{x}^m, \bar{x}^n)\} \subset \text{Ker}(\psi)$. Par injectivité de φ , $\text{Im}(\varphi) = |\mathbf{Z}/\mu\mathbf{Z}| = \mu$. On en déduit que

$$|\text{Im}(\varphi)| = \mu = \frac{mn}{\delta} = \frac{|\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}|}{|\mathbf{Z}/\delta\mathbf{Z}|} = \frac{|\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}|}{|\text{Im}(\psi)|} = |\text{Ker}(\psi)|.$$

On a l'égalité des ensembles par égalité des cardinaux.

□

Démonstration — Preuve du corollaire

Soient u, v deux entiers tels que $um + vn = \delta$.

- Trouver une solution particulière

Écrivons $a = b + k\delta$ et considérons $x_0 = \frac{avn + xbum}{\delta}$. Alors,

$$x_0 = \frac{(b + k\delta)vn + bum}{\delta} = b \frac{vn + um}{\delta} + kvn \equiv b[n].$$

De la même façon, en écrivant $b = a - k\delta$, on trouve $x_0 \equiv a[m]$.

- Détermination de l'ensemble des solutions

Soit x une solution du système. Alors, $x - x_0 \in \text{Ker}(\tilde{\varphi}) = \mu\mathbf{Z}$, d'où $\text{Sol} \subset x_0 + \mu\mathbf{Z}$. La réciproque étant triviale, on a le résultat.

□

Passons à l'application.

- Premier système

Supposons par l'absurde qu'il existe une solution x au système. Alors,

$$\tilde{\varphi}(x) = (\bar{x}^{21}, \bar{x}^{35}) = (\bar{2}^{21}, \bar{11}^{35}) \in \text{Im}(\varphi) = \text{Ker}(\psi).$$

Or, $\bar{2}^7 - \bar{11}^7 = \bar{5}^7 \neq \bar{0}^7$. D'où la contradiction.

- Second système

Cette fois-ci, on a bien $\bar{3}^7 = \bar{10}^7$. En appliquant le raisonnement du corollaire, on a

$$x_0 = \frac{-3 \cdot 35 + 10 \cdot 2 \cdot 21}{7} = 45$$

et donc $S = 45 + 105\mathbf{Z}$.

46 Conditions de cyclicité de $(\mathbf{Z}/n\mathbf{Z})^\times$

Leçons : 104, 108, 120, 121

Référence: Cours de cryptographie, Zemor

Théorème — *Le groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^\times$ est cyclique si et seulement si $n = 2, 4, p^k, 2p^k$ avec p premier impair.*

- Si n n'est pas de cette forme, on n'a pas de cyclicité.

Tout d'abord, supposons $n = 2^k$ avec $k = 3$. On a $\varphi(2^k) = 2^{k-1}$.

Par récurrence, on montre que pour tout a impair, $a^{2^{k-2}} \equiv 1[2^k]$. En effet, si $a^{2^{k-2}} = 1 + m2^k$,

$$a^{2^{k-1}} = (1 + m2^k)^2 = 1 + m2^{k+1} + m^2 2^{2k} \equiv 1[2^{k+1}].$$

De cela, on déduit que $(\mathbf{Z}/n\mathbf{Z})^\times$ n'admet pas d'élément d'ordre $\varphi(n)$, car si $a \in (\mathbf{Z}/n\mathbf{Z})^\times$ (on le prend impair car s'il est pair il n'est de toute façon pas viable), a est d'ordre au plus $\varphi(n)/2$. Donc $(\mathbf{Z}/n\mathbf{Z})^\times$ n'est pas cyclique.

Dans les autres cas où n n'est pas de la forme indiquée, on a $n = n_1 n_2$ avec $n_1 \wedge n_2 = 1$ et $\varphi(n_1) \geq 2$ et $\varphi(n_2) \geq 2$. D'après le théorème chinois,

$$(\mathbf{Z}/n\mathbf{Z})^\times \simeq (\mathbf{Z}/n_1\mathbf{Z})^\times \times (\mathbf{Z}/n_2\mathbf{Z})^\times,$$

donc tout élément de $(\mathbf{Z}/n\mathbf{Z})^\times$ a pour ordre un diviseur de $\text{ppcm}(\varphi(n_1), \varphi(n_2))$. Or, ces deux indicatrices sont paires, donc ce ppcm est plus petit que $\varphi(n_1)\varphi(n_2) = \varphi(n)$.

- Montrer qu'il existe un élément g premier avec p tel que pour tout $k > 1$, $g^{\varphi(p^{k-1})} \not\equiv 1[p^k]$.

Soit g premier à p . On a

$$(g + p)^{p-1} \equiv g^{p-1} + (p-1)pg^{p-2} \equiv g^{p-1} - pg^{p-2}[p^2].$$

Comme p n'est pas premier à p^2 , on en déduit que soit g soit $g + p$, que l'on notera g_1 , vérifie $g_1^{p-1} \not\equiv 1[p^2]$.

On montre ensuite par récurrence que g_1 est le candidat recherché. On a initialisé, cherchons donc à prouver l'hérédité. Par le petit théorème de Fermat, $g_1^{\varphi(p^{k-1})} \equiv 1[p]$, donc

$$g_1^{\varphi(p^k)} \equiv (1 + mp^{k-1})^p \equiv \dots \not\equiv 1[p^{k+1}].$$

- Preuve du cas $n = p^k$.

C'est vrai pour $k = 1$. Soit g premier à p qui vérifie le point précédent. On montre que g est premier à p^k .

Soit e l'ordre de g modulo p^k . On a forcément $g^e \equiv 1[p]$ donc $(p-1) \mid e$. De plus, $e \mid \varphi(p^k) = p^{k-1}(p-1)$. On en déduit que e est de la forme $e = (p-1)p^i$ et d'après le choix de g , on a nécessairement que $i = k-1$. L'ordre de g est donc bien égal à $\varphi(p^k)$.

- Preuve du cas $n = 2p^k$

Soit g premier à p^k . On note g_1 celui de g ou $g + p$ qui est impair, de sorte que $g_1 \in (\mathbf{Z}/n\mathbf{Z})^\times$. On constate que g_1 est premier à $2p^k$ puisque son ordre modulo $2p^k$ est au moins égal à $\varphi(p^k)$ et que $\varphi(2p^k) = \varphi(p^k)$.

Les cas $n = 2$ et $n = 4$ étant triviaux, on a le résultat.

47 Théorèmes de point fixe compact

Leçons : 203, 223, 226

Référence: Analyse pour l'agrégation, Bernis

Théorème — Soient $(E, \|\cdot\|)$ un espace vectoriel normé, K un compact de E et $f : K \rightarrow K$ une application continue.

1. On suppose que pour tout $x, y \in K$ distincts, $\|f(x) - f(y)\| < \|x - y\|$. Alors, f admet un et un seul point fixe $\alpha \in K$. De plus, pour tout $x \in K$, la suite $(f^n(x))_{n \in \mathbf{N}}$ converge vers α .
2. On suppose de plus K étoilé et pour tout $x, y \in K$, $\|f(x) - f(y)\| \leq \|x - y\|$. Alors f admet un point fixe.

Démonstration — Preuve du premier point

- Existence d'un point fixe

Posons $g : K \rightarrow \mathbf{R}_+$; $x \mapsto \|f(x) - x\|$.

Cette application est 2-lipschitzienne par inégalité triangulaire et compte tenu de l'hypothèse. Elle est donc continue sur le compact K , donc atteint son minimum en un point $\alpha \in K$.

Supposons par l'absurde que α n'est pas un point fixe de f . Alors, par hypothèse, on obtient que $g(f(\alpha)) < g(\alpha)$, ce qui est absurde par définition de α . Donc α est un point fixe de f .

- Unicité du point fixe

Si α_1, α_2 sont deux points fixes distincts de f , par hypothèse, $\|\alpha_2 - \alpha_1\| < \|\alpha_2 - \alpha_1\|$, ce qui est absurde. D'où l'unicité du point fixe.

- Convergence de la suite des itérées

Soit $x_0 \in K$. On définit la suite $x_n = f^n(x_0)$ par récurrence.

Notons A l'ensemble des valeurs d'adhérence de la suite. On écrit $A = \bigcap_{n \in \mathbf{N}} \overline{\{x_k \mid k \geq n\}}$. On montre par double inclusion que $f(A) = A$.

Soit $y \in A$. On dispose d'une sous-suite $(x_{\varphi(n)})$ qui converge vers y . Quitte à ré-extraire, on suppose $\varphi(0) \geq 1$. Dans ce cas, pour tout $n \in \mathbf{N}$, par continuité de f ,

$$x_{\varphi(n)+1} = f(x_{\varphi(n)}) \xrightarrow{n \rightarrow +\infty} f(y).$$

Ainsi, $f(y) \in A$ et $f(A) \subset A$.

Réciproquement, on pose $\psi = \varphi - 1$ une extractrice. La suite $(x_{\psi(n)})$ étant à valeurs dans le compact K , elle a une valeur d'adhérence x limite de la sous-suite $(x_{\psi \circ \chi(n)})$, et donc $x \in A$. Par continuité de f ,

$$f(x_{\psi \circ \chi(n)}) \xrightarrow{n \rightarrow +\infty} f(x).$$

Or, par construction de ψ , $f(x_{\psi(n)}) = x_{\varphi(n)}$, et donc

$$f(x_{\psi \circ \chi(n)}) = x_{\varphi \circ \chi(n)} \xrightarrow{n \rightarrow +\infty} y.$$

Donc $y = f(x)$ et donc $y \in f(A)$. Donc $A \subset f(A)$.

Supposons par l'absurde que A n'est pas réduit à un singleton. L'ensemble A étant fermé par définition, et inclus dans le compact K , il est compact et on dispose donc d'un couple $(y_1, y_2) \in A^2$ tel que $\|y_1 - y_2\| = \text{diam}(A)$.

Comme $f(A) = A$, on dispose de deux éléments $x_1, x_2 \in A$ tels que $f(x_1) = y_1$ et $f(x_2) = y_2$. Alors,

$$\|y_2 - y_1\| = \|f(x_2) - f(x_1)\| < \|x_2 - x_1\| \leq \text{diam}(A) = \|y_2 - y_1\|,$$

ce qui est absurde. Donc A est un singleton. La suite (x_n) ayant une unique valeur d'adhérence, elle converge forcément vers celle-ci. Par continuité de f , cette valeur d'adhérence est forcément α .

□

Démonstration — Preuve du second point

Soit $z \in K$ tel que K soit étoilé par rapport à z . Pour tout $n \in \mathbf{N}^*$, on définit

$$h_n : \begin{cases} K & \longrightarrow K; \\ x & \longmapsto z + \left(1 - \frac{1}{n}\right)(x - z) \end{cases}$$

la restriction à K de l'homothétie (affine) de centre z et de rapport $1 - \frac{1}{n}$. Posons également $f_n = h_n \circ f$. Pour tout n , f_n vérifie le premier point donc a un unique point fixe $\alpha_n \in K$. On extrait une sous-suite de cette suite de points fixes qui converge vers $\alpha \in K$. Par inégalité triangulaire, on obtient bien que $f(\alpha) = \alpha$:

$$\begin{aligned} \|f(\alpha) - \alpha\| &\leq \|f(\alpha) - f_{\varphi(n)}(\alpha)\| + \|f_{\varphi(n)}(\alpha) - f_{\varphi(n)}(\alpha_{\varphi(n)})\| + \|f_{\varphi(n)}(\alpha_{\varphi(n)}) - \alpha_{\varphi(n)}\| + \|\alpha_{\varphi(n)} - \alpha\|, \\ &\leq \frac{1}{\varphi(n)} \|f(\alpha) - z\| + \left(1 - \frac{1}{\varphi(n)}\right) \|\alpha - \alpha_{\varphi(n)}\| + 0 + \|\alpha_{\varphi(n)} - \alpha\|, \\ &\leq \frac{1}{\varphi(n)} \|f(\alpha) - z\| + 2\|\alpha_{\varphi(n)} - \alpha\|, \\ &\xrightarrow{n \rightarrow +\infty} 0. \end{aligned}$$

□

Remarque — La convergence, contrairement au cas de Picard, peut être très lente !

Posons par exemple,

$$f : \begin{cases} [0, 1] & \longrightarrow [0, 1]; \\ x & \longmapsto x - x^2 \exp\left(-\frac{1}{x}\right) \text{ si } x \neq 0; 0 \text{ sinon.} \end{cases}$$

Soit $x \in]0, 1[$, notons (u_n) la suite des itérées. Alors, le théorème montre que (u_n) tend vers 0 (IAF).

Pour avoir un équivalent de u_n , on regarde $u_n - u_{n+1} = u_n^2 \exp\left(-\frac{1}{u_n}\right)$. Heuristiquement,

$$1 = \frac{u_n - u_{n+1}}{u_n^2 \exp\left(-\frac{1}{u_n}\right)} \stackrel{?}{\sim} \int_{u_{n+1}}^{u_n} \frac{1}{t^2} \exp\left(\frac{1}{t}\right) dt = \exp\left(\frac{1}{u_{n+1}}\right) - \exp\left(\frac{1}{u_n}\right).$$

On vérifie donc que

$$\begin{aligned} \exp\left(\frac{1}{u_{n+1}}\right) - \exp\left(\frac{1}{u_n}\right) &= \exp\left(\frac{1}{u_n - u_n^2 \exp\left(-\frac{1}{u_n}\right)}\right) - \exp\left(\frac{1}{u_n}\right), \\ &= \exp\left(\frac{1}{u_n} \frac{1}{1 - u_n \exp\left(-\frac{1}{u_n}\right)}\right) - \exp\left(\frac{1}{u_n}\right), \\ &= \exp\left[\frac{1}{u_n} \left(1 + u_n \exp\left(-\frac{1}{u_n}\right) + O\left(u_n^2 \exp\left(-\frac{2}{u_n}\right)\right)\right)\right] - \exp\left(\frac{1}{u_n}\right), \\ &= \exp\left(\frac{1}{u_n}\right) \left[\exp\left(\exp\left(-\frac{1}{u_n}\right) + O\left(u_n \exp\left(-\frac{2}{u_n}\right)\right)\right) - 1\right], \\ &= \exp\left(\frac{1}{u_n}\right) \left[\exp\left(-\frac{1}{u_n}\right) + O\left(u_n \exp\left(-\frac{2}{u_n}\right)\right)\right], \\ &\sim 1. \end{aligned}$$

Par équivalence de sommes partielles de séries divergentes à termes positifs, et par télescopage,

$$\exp\left(\frac{1}{u_n}\right) - \exp\left(\frac{1}{u_0}\right) = \sum_{k=0}^n -1 \exp\left(\frac{1}{u_{k+1}}\right) - \exp\left(\frac{1}{u_k}\right) \sim \sum_{k=0}^{n-1} 1 = n.$$

Donc, comme $\exp\left(\frac{1}{u_0}\right)$ est négligeable devant $\exp\left(\frac{1}{u_n}\right)$, par passage au log dans l'équivalence,

$$u_n \sim \frac{1}{\ln(n)}.$$

48 Théorème de Weierstrass par les probabilités

Leçons : 209

Référence: Probabilités 1, Ouvrard

Théorème — (Weierstrass) Soit $f \in \mathcal{C}^0([0, 1], \mathbf{R})$. Il existe une suite de polynômes qui converge uniformément sur $[0, 1]$ vers f .

Soit $f \in \mathcal{C}([0, 1], \mathbf{R})$.

- Introduction du module de continuité

On définit $\omega : \mathbf{R}_+ \rightarrow \mathbf{R}_+$; $\delta \mapsto \sup\{|f(u) - f(v)| \mid u, v \in [0, 1], |v - u| \leq \delta\}$. Comme f est continue sur un segment, le théorème de Heine nous dit que f est uniformément continue et ω est donc bien définie. De plus, on voit directement que

1. ω est croissante,
2. $\omega(0) = 0$ et ω est continue en 0
3. Pour $\lambda \in \mathbf{R}_+$ et $\delta \in \mathbf{R}_+$, on a $\omega(\lambda\delta) \leq (\lambda + 1)\omega(\delta)$.

En effet, pour tout $\varepsilon \in \mathbf{R}_+^*$, il existe η tel que $\omega(\eta) < \varepsilon$ par uniforme continuité de f . Donc $\omega \leq \varepsilon$ sur $]0, \eta]$ donc ω est continue en 0.

Pour le point 3, on prend $u < v$ tels que $|v - u| \leq \lambda\delta$.

On considère la subdivision $x_i = u + i\delta$ si $u + i\delta < v$ puis $x_m = v$ dès que $u + m\delta > v$. Alors, $m \leq \lambda + 1$ et $|f(u) - f(v)| \leq m\omega(\delta)$.

- Introduction des polynômes de Bernstein

On se place dans un espace probabilisé $(\Omega, \mathcal{A}, \mathbb{P})$. Soit $x \in [0, 1]$. On se donne une suite de variables i.i.d $(X_n)_{n \in \mathbf{N}}$ avec $X_n \sim \mathcal{B}(x)$. On pose $S_n = \sum_{k=1}^n X_k$.

Alors, $S_n \sim \mathcal{B}(n, x)$, donc par le théorème de transfert,

$$E \left[f \left(\frac{S_n}{n} \right) \right] = \sum_{k=0}^n f \left(\frac{k}{n} \right) \binom{n}{k} x^k (1-x)^{n-k}.$$

On pose, pour tout $n \in \mathbf{N}^*$, $B_n(x) = \sum_{k=0}^n f \left(\frac{k}{n} \right) \binom{n}{k} x^k (1-x)^{n-k}$.

- Convergence uniforme vers f

Par inégalité triangulaire et définition du module de continuité,

$$|f - B_n(f)|(x) = \left| E \left[f(x) - f \left(\frac{S_n}{n} \right) \right] \right| \leq E \left[\left| f(x) - f \left(\frac{S_n}{n} \right) \right| \right] \leq E \left[\omega \left(\left| x - \frac{S_n}{n} \right| \right) \right].$$

Par le troisième point vérifié par ω ,

$$|f - B_n(f)|(x) \leq E \left[\left(1 + \sqrt{n} \left| x - \frac{S_n}{n} \right| \right) \omega \left(\frac{1}{\sqrt{n}} \right) \right] \leq \left(1 + \sqrt{n} E \left[\left| x - \frac{S_n}{n} \right| \right] \right) \omega \left(\frac{1}{\sqrt{n}} \right).$$

Par l'inégalité de Cauchy-Schwarz, on obtient alors :

$$E \left[\left| x - \frac{S_n}{n} \right| \right] \leq E[1^2]^{\frac{1}{2}} E \left[\left(x - \frac{S_n}{n} \right)^2 \right]^{\frac{1}{2}} = \sqrt{E \left[\left(x - \frac{S_n}{n} \right)^2 \right]}.$$

$x - \frac{S_n}{n}$ étant centrée,

$$E \left[\left(x - \frac{S_n}{n} \right)^2 \right] = \text{Var} \left(\frac{S_n}{n} \right) = \frac{1}{n^2} \sum_{i=1}^n \text{Var}(X_i) = \frac{x(1-x)}{n} \leq \frac{1}{4n}.$$

Donc, $\|f - B_n(f)\|_\infty \leq \frac{3}{2} \omega \left(\frac{1}{\sqrt{n}} \right)$ et on obtient le résultat en utilisant le point 2, avec un contrôle de la vitesse de convergence par le module de continuité.

- Vitesse de convergence

Si f est k -lipschitzienne, on a $\omega(\delta) \leq k\delta$ donc la vitesse de convergence est au pire en $\frac{1}{\sqrt{n}}$.

Montrons que la vitesse est optimale. Considérons $f : x \mapsto \left|x - \frac{1}{2}\right|$, 1-lipschitzienne et vérifiant $\omega(\delta) = \delta$. On a

$$\|f - B_n(f)\|_\infty \geq \left|f\left(\frac{1}{2}\right) - B_n(f)\left(\frac{1}{2}\right)\right| = \left|B_n(f)\left(\frac{1}{2}\right)\right| = E\left[\left|\frac{S_n}{n} - \frac{1}{2}\right|\right] = \frac{1}{2n}E[|2S_n - n|].$$

Or, $2S_n - n = \sum_{i=1}^n 2X_i - 1 = \sum_{i=1}^n \varepsilon_i$ où $\varepsilon_i \sim \mathcal{R}(1/2)$ et posons $Y = \prod_{j=1}^n \left(1 + i\frac{\varepsilon_j}{n}\right)$.

D'une part, $\sqrt{e}E[|2S_n - n|] \geq E[|2S_n - n||Y|]$. En effet,

$$|Y| = \prod_{j=1}^n \sqrt{1 + \frac{\varepsilon_j^2}{n}} = \prod_{j=1}^n \sqrt{1 + \frac{1}{n}} \leq \prod_{j=1}^n \sqrt{e^{\frac{1}{n}}} \leq \sqrt{e}.$$

D'autre part, on a

$$E[(2S_n - n)Y] = nE\left[\varepsilon_1 \left(1 + i\frac{\varepsilon_1}{\sqrt{n}}\right) \prod_{j>1} \left(1 + i\frac{\varepsilon_j}{\sqrt{n}}\right)\right] = n\left(E[\varepsilon_1] + \frac{i}{\sqrt{n}}E[\varepsilon_1^2]\right) \prod_{j>1} \left(1 + i\frac{E[\varepsilon_j]}{\sqrt{n}}\right) = i\sqrt{n}.$$

Finalement,

$$\|f - B_n(f)\|_\infty \geq \frac{1}{2n}\sqrt{\frac{n}{e}} = \frac{1}{2\sqrt{e}}\omega\left(\frac{1}{\sqrt{n}}\right).$$

49 Système de Lotka-Volterra

Leçons : 222

Référence: Analyse 4, FGN Soient a, b, c, d, x_0, y_0 des réels strictement positifs. On considère le système différentiel (proie-prédateur) :

$$\begin{cases} x' &= ax - bxy, \\ y' &= -cy + dxy \end{cases} \quad \text{avec } (x(0), y(0)) = (x_0, y_0).$$

Proposition —

1. Ce système admet une solution maximale qui est globale.
2. x et y sont périodiques.

• Interprétation physique

x augmente avec x et décroît avec y : c'est la proie. y décroît avec y et croît avec x : c'est le prédateur.

• Les solutions sont à valeurs dans $\mathbf{R}_+^*$

Tout d'abord, le système admet bien une solution maximale car $f : (x, y) \mapsto (ax - bxy, -cy + dxy)$ est de classe C^1 donc localement lipschitzienne (et Cauchy-Lipschitz).

Supposons qu'il existe t_1 tel que $x(t_1) = 0$. Alors par le théorème de Cauchy-Lipschitz, on a à tout temps $x(t) = 0$ et $y(t) = y(t_1)e^{c(t-t_1)}$, ce qui est absurde car $x_0 > 0$. Il en va de même pour y , donc on reste forcément dans $(\mathbf{R}_+^*)^2$.

• La solution est globale

Posons $H(x, y) = dx + by - c \ln(x) - a \ln(y)$. Par dérivation,

$$\frac{d}{dt}H(x(t), y(t)) = d(ax - bxy) + b(dxy - cy) - c \frac{ax - bxy}{x} - a \frac{-cy + dxy}{y} = 0,$$

donc H est constante sur une trajectoire.

Notons I l'intervalle ouvert de définition de X . On note $g_1(x) = dx - c \ln(x)$ et $g_2(y) = by - a \ln(y)$. Ces deux fonctions possèdent des minimum respectivement en $\frac{c}{d}$ et en $\frac{a}{b}$, et $H(x, y) = g_1(x) + g_2(y)$.

D'après ce qui précède, il existe $\gamma \in \mathbf{R}$ tel que $H(x(t), y(t)) = \gamma$ à tout temps. On en déduit que pour tout $t \in I$,

$$\begin{cases} g_1(x(t)) &\leq \gamma - m_2, \\ g_2(y(t)) &\leq \gamma - m_1 \end{cases}$$

Or, $g_1(x) \xrightarrow{x \rightarrow 0} \infty$ et $g_1(x) \xrightarrow{x \rightarrow \infty} \infty$, donc nécessairement x est borné par des réels $\alpha, \beta \in \mathbf{R}_+^*$. Pareil pour y , donc X est bornée sur I dont $I = \mathbf{R}$ par le lemme de sortie de tout compact.

• Montrer que x et y sont périodiques

On a deux points d'équilibre pour le système : l'origine et $\left(\frac{c}{d}, \frac{a}{b}\right)$. On exclut ces cas où on est constant.

On coupe $(\mathbf{R}_+^*)^2$ en quatre parties suivant le signe de x' et y' . On numérote les zones de 1 à 4 dans le sens trigonométrique, on suppose que $(x_0, y_0) \in Z_1 = \{x' \geq 0, y' \leq 0\}$. On suppose que la trajectoire reste dans cette zone. Alors x est croissante majorée, donc admet une limite en l'infini. De même y est décroissante et minorée par 0 dont admet une limite en l'infini. Alors, x' et y' admettent une limite en l'infini, limites qui sont forcément nulles sans quoi x et y ne seraient pas bornées. On en déduit que $y \xrightarrow[t \rightarrow +\infty]{} \frac{a}{b}$: en effet x ne peut tendre vers 0, or $y_0 < \frac{a}{b}$ et y décroît, c'est absurde. Donc la trajectoire quitte Z_1 .

On note $t_1 = \inf\{t > 0, X(t) \notin Z_1\}$. Par continuité, on a forcément $x(t) = \frac{c}{d}$ et $y(t_1) < \frac{a}{b}$, donc $x'(t_1) > 0$ et $y'(t_1) = 0$. Il existe donc $\eta \in \mathbf{R}_+^*$ tel que pour tout $t \in]t_1, t_1 + \eta[$, $X(t) \in Z_2$. On peut donc faire comme

précédemment pour trouver t_2 tel qu'on entre dans Z_3 , et t_3 tel qu'on entre dans Z_4 , enfin t_4 pour revenir dans Z_1 .

Reste à expliquer pourquoi c'est périodique. Pour cela, remarquons que $y \mapsto H\left(\frac{c}{d}, y\right) = m_1 + g_2(y)$ est décroissante strictement sur $\left[\frac{a}{b}, +\infty\right[$. Comme H est constante sur une trajectoire, celle-ci ne peut passer que par un unique point de la demi-droite $\left\{\frac{c}{d}\right\} \times \left[\frac{a}{b}, +\infty\right[$. Or, à chaque passage de Z_1 à Z_2 , on passe par cette demi-droite, on passe donc une infinité de fois par ce point. Si on note t_1 et t_2 deux passages consécutifs par ce point, le théorème de Cauchy-Lipschitz montre que x et y sont $T = t_2 - t_1$ périodiques.

- Conclusion

La valeur moyenne de x est $\frac{c}{d}$ et celle de y est $\frac{a}{b}$ par un simple calcul.

Si on note ε le taux de perte de chaque espèce par la chasse, on voit que les nouvelles moyennes sont respectivement $\frac{c + \varepsilon}{d}$ et $\frac{a - \varepsilon}{b}$. La chasse profite donc aux proies.

50 Théorème de structure des polynômes symétriques

Leçons : 105,144

Référence: Algèbre, Tauvel

Lemme — Soit $P \in A[X_1, \dots, X_n]$ symétrique tel que $P(x_1, \dots, X_{n-1}, 0) = 0$. Alors Σ_n divise le polynôme P .

On définit le poids d'un monôme X^ν où $\nu = (\nu_1, \dots, \nu_n) \in \mathbf{N}^n$ par $\pi(X^\nu) = \nu_1 + \dots + n\nu_n$. Le poids d'un polynôme est alors le maximum des poids de ses monômes. On pose $\pi(P) = +\infty$ si $P = 0$.

Théorème — Soit $P \in A[X_1, \dots, X_n]$ symétrique de degré d . Il existe $Q \in A[Y_1, \dots, Y_n]$ tel que $\pi(Q) \leq d$ tel que $P(x_1, \dots, X_n) = Q(\Sigma_n, \dots, \Sigma_n)$.
De plus, ce polynôme est unique (dans le sens où les Σ_i sont algébriquement indépendants dans A).

• Preuve du lemme

On raisonne par récurrence sur n , le cas $n = 1$ étant clair.

On note τ la transposition $(n-1, n)$. Écrivons $P = P_0 + P_1 X_n + \dots + P_k X_n^k$, où $P_0, \dots, P_k \in A[X_1, \dots, X_{n-1}]$. Par hypothèse, $P_0 = 0$.

Comme $\tau \cdot P = P$, on déduit que $P(X_1, \dots, X_{n-2}, 0, X_n) = 0$. Il en résulte que pour tout $j \in \llbracket 1, k \rrbracket$, on a $P_j(X_1, \dots, X_{n-2}, 0) = 0$. Par hypothèse de récurrence, P_j est divisible par Σ_{n-1} . Donc $\Sigma_n = X_n \Sigma_{n-1}$ divise P . D'où la preuve du lemme par théorème de récurrence.

• Preuve de l'existence du théorème

On peut supposer $n \geq 2$ et $d \geq 1$. Notons $\sigma_1, \dots, \sigma_{n-1}$ les polynômes symétriques élémentaires en $X_1, \dots, X_{n-1}$. Posons $B = A[X_1, \dots, X_{n-1}]$, et pour $j \in \llbracket 1, n-1 \rrbracket$,

$$\Sigma_j^0 = \Sigma_j(X_1, \dots, X_{n-1}, 0).$$

Remarquons que $\sigma_j = \Sigma_j^0$. On raisonne par récurrence sur n et d .

Si $R(X_1, \dots, X_{n-1}) = P(X_1, \dots, X_{n-1}, 0)$, alors $R \in B$ et R est symétrique. D'après l'hypothèse de récurrence, il existe $Q_1 \in B$ tel que

$$\begin{cases} \pi(Q_1) \leq d, \\ P(X_1, \dots, X_n) = Q_1(\sigma_1, \dots, \sigma_{n-1}) = Q_1(\Sigma_1^0, \dots, \Sigma_{n-1}^0). \end{cases}$$

Le polynôme Q_1 est de degré au plus d . Posons $P_1(X_1, \dots, X_n) = P(X_1, \dots, X_n) - Q_1(\Sigma_1, \dots, \Sigma_{n-1})$. On a $\deg(P_1) \leq d$ et $P_1(X_1, \dots, X_{n-1}, 0) = 0$, donc par le lemme, il existe $P_2 \in A[X_1, \dots, X_n]$ tel que $P_1 = \Sigma_n P_2$. Le polynôme P_2 est symétrique, de degré inférieur ou égal à $d - n$.

D'après l'hypothèse de récurrence sur d , il existe $Q_2 \in A[X_1, \dots, X_n]$ tel que

$$\begin{cases} \pi(Q_2) \leq d - n, \\ P(X_1, \dots, X_n) = Q_1(\Sigma_1, \dots, \Sigma_{n-1}) + Q_2(\Sigma_1, \dots, \Sigma_{n-1})\Sigma_n. \end{cases}$$

Enfin, ce polynôme dans le terme de droite est de poids au plus d . D'où l'existence.

• Indépendance algébrique des polynômes symétriques élémentaires

On raisonne par récurrence sur n . Le cas $n = 1$ est clair.

Supposons $n \geq 2$ et $\Sigma_1, \dots, \Sigma_n$ algébriquement liés sur A . Soit $P \in A[X_1, \dots, X_n]$, non nul et de degré minimal vérifiant $P(\Sigma_1, \dots, \Sigma_n) = 0$. Il existe $P_0, \dots, P_k \in A[X_1, \dots, X_{n-1}]$ tels que :

$$P = P_0 + P_1 X_n + \dots + P_k X_n^k.$$

Si $P_0 = 0$, alors $P = X_n Q$ avec $\deg(Q) < \deg(P)$ et $Q(\Sigma_1, \dots, \Sigma_n) = 0$, ce qui est absurde car P est de degré minimal. Dans l'autre cas,

$$P(\Sigma_1^0, \dots, \Sigma_{n-1}^0, 0) = P_0(\sigma_1, \dots, \sigma_{n-1}) = 0.$$

Comme P_0 est non nul, c'est absurde par l'hypothèse de récurrence.

51 Action de Steinitz

Leçons : 150

Référence: H2G2, tome 1, Caldero-Germoni

Proposition — On considère l'action suivante

$$(GL_m(\mathbf{K}) \times GL_n(\mathbf{K})) \times M_{m,n}(\mathbf{K}) \longrightarrow M_{m,n}(\mathbf{K}); ((P, Q), A) \longmapsto (P, Q) \cdot A = PAQ^{-1}.$$

1. A et B sont dans la même orbite si et seulement si elles ont même rang.
2. On note O_r l'ensemble des matrices de rang $r \in \llbracket 0, n \rrbracket$. Alors, $\overline{O_r} = \bigcup_{k=0^r} O_k$.

- Si A et B sont dans la même orbite, alors elles ont même rang

Il existe $P, Q \in GL_n(\mathbf{K})$ telles que $A = PBQ^{-1}$. On peut les voir comme des matrices de changement de base, donc A et B sont les matrices du même endomorphisme dans une base différente. Le rang d'un endomorphisme étant défini de façon intrinsèque, par le théorème du rang, $\text{rg}(A) = \text{rg}(B)$.

- Si A et B ont même rang, alors elles sont dans la même orbite

On montre par récurrence sur $p = \min(m, n)$ l'équivalence à J_r .

Si $p = 1$, on a une ligne ou bien une colonne donc par des transvections on obtient le résultat.

Si c'est vrai pour (m, n) , alors c'est vrai pour $(m+1, n+1)$.

Par des opérations élémentaires, on peut se ramener à $a_{1,1} = 1$, le reste de la ligne / colonne nulle et on applique l'hypothèse de récurrence.

- Montrer que la réunion des O_k est un fermé de $M_{m,n}(\mathbf{K})$

Notons R cette réunion. Comme A est de rang au plus r ssi tous ses mineurs d'ordre supérieur ou égal à $r+1$ sont nuls, on peut écrire

$$R = \bigcap_{|I|=|J| \geq r+1} \Delta_{I,J}^{-1}(\{0\}).$$

Comme les fonctions $\Delta_{I,J}$ sont continues, R est fermé comme intersection de fermés.

On en déduit que $\overline{O_r} \subset R$.

- Inclusion réciproque

Soit $M \in R$ de rang $k \leq r$. Il existe donc P, Q tels que $M = PJ_rQ^{-1}$. On pose $M(\varepsilon) = P \begin{pmatrix} I_k & 0 & 0 \\ 0 & \varepsilon I_{r-k} & 0 \\ 0 & 0 & 0 \end{pmatrix} Q^{-1}$.

La suite $M_n = M \begin{pmatrix} 1 \\ \frac{1}{n} \end{pmatrix}$ converge vers M et est de rang r , donc $M \in \overline{O_r}$. D'où le résultat.

52 Théorème de Cauchy-Lipschitz linéaire

Leçons : 221

Référence: Analyse pour l'agrégation, Bernis

Théorème — Soit $n \in \mathbf{N}^*$. Soient $A : \mathbf{R} \longrightarrow M_n(\mathbf{R})$ et $b : \mathbf{R} \longmapsto \mathbf{R}^n$ deux applications continues. Soit $y_0 \in \mathbf{R}^n$. Alors le problème de Cauchy

$$\begin{cases} y' &= A(t)y + b(t), \\ y(0) &= y_0 \end{cases} \quad (4)$$

admet une unique solution définie sur $\mathbf{R}$ tout entier ;

On munit $\mathbf{R}^n$ d'une norme $\|\cdot\|$ et $M_n(\mathbf{R})$ de la norme subordonnée associée $\|\cdot\|_M$.

- Localisation du problème, vérification de l'hypothèse de lipschitzité

Soit $[a, b]$ un segment d'intérieur non vide contenant 0. On cherche une solution de (4) définie sur $[a, b]$. Posons

$$f : \mathbf{R} \times \mathbf{R}^n \longrightarrow \mathbf{R}^n; (t, x) \longmapsto A(t)x + b(t).$$

Par composition des applications continues A et $\|\cdot\|_M$, la fonction $t \mapsto \|A(t)\|_M$ est continue sur le segment $[a, b]$. Elle y est donc bornée et on dispose de $M \in \mathbf{R}_+^*$ telle que pour tout $t \in [a, b]$,

$$\|A(t)\|_M \leq M.$$

On en déduit que pour tout couple $(x_1, x_2) \in (\mathbf{R}^n)^2$ et tout $t \in [a, b]$, on a

$$\|f(t, x_1) - f(t, x_2)\| \leq M\|x_1 - x_2\|.$$

Ainsi f est-elle globalement lipschitzienne selon sa deuxième variable, uniformément en la première variable sur $[a, b]$.

- Reformulation du problème

Notons $E = \mathcal{C}^0([a, b], \mathbf{R}^n)$ et $F = \mathcal{C}^1([a, b], \mathbf{R}^n)$. On les munit de la norme infinie $\|\cdot\|_\infty$. Soit L l'application (linéaire par linéarité de f et de l'intégrale)

$$L : E \longrightarrow E; \varphi \longmapsto (L(\varphi) : t \mapsto y_0 + \int_0^t f(s, \varphi(s)) \, ds).$$

Par le théorème fondamental de l'analyse, l'opérateur L est à valeurs dans F . De plus, pour tout $\varphi \in E$, et tout $t \in [a, b]$,

$$L(\varphi)'(t) = f(t, \varphi(t)) = A(t)\varphi(t) + b(t) \text{ et } L(\varphi)(0) = y_0.$$

On en déduit que si φ est un point fixe de l'opérateur L , alors c'est une solution sur $[a, b]$ de classe $\mathcal{C}^1$ du problème de Cauchy (4). Réciproquement, si φ vérifie le problème de Cauchy sur $[a, b]$, alors c'est un point fixe de l'opérateur L .

- Application du théorème de Picard

On montre par récurrence sur $p \in \mathbf{N}^*$ que pour tout $(\varphi_1, \varphi_2) \in E^2$ et tout $t \in [a, b]$, on a

$$\|L^p(\varphi_1)(t) - L^p(\varphi_2)(t)\| \leq \frac{M^p |t|^p}{p!} \|\varphi_1 - \varphi_2\|_\infty.$$

- Initialisation :

$$\|L(\varphi_1)(t) - L(\varphi_2)(t)\| \leq \left| \int_0^t \|f(s, \varphi_1(s)) - f(s, \varphi_2(s))\| \, ds \right| \leq M|t| \|\varphi_1 - \varphi_2\|_\infty.$$

- **Hérédité :** On suppose la propriété vérifiée pour un certain rang $p \in \mathbf{N}^*$. Pour tout $t \in [a, b]$,

$$\begin{aligned}
& \|L^{p+1}(\varphi_1)(t) - L^{p+1}(\varphi_2)(t)\| \\
& \leq \left| \int_0^t \|f(s, L^p(\varphi_1)(s)) - f(s, L^p(\varphi_2)(s))\| \, ds \right|, \\
& \leq \frac{M^{p+1}}{p!} \left| \int_0^t |s|^p \|\varphi_1 - \varphi_2\|_\infty \, ds \right|, \\
& = \frac{M^{p+1}|t|^{p+1}}{(p+1)!} \|\varphi_1 - \varphi_2\|_\infty.
\end{aligned}$$

D'où l'hérédité.

Comme $\frac{M^p(b-a)^p}{p!} \xrightarrow{p \rightarrow +\infty} 0$, il existe $P \in \mathbf{N}^*$ pour lequel c'est plus petit que 1. Donc L^P est contractante sur le Banach $(E, \|\cdot\|_\infty)$.

D'après le théorème du point fixe de Picard, il existe un unique élément φ_0 de E tel que $L^P(\varphi_0) = \varphi_0$. En composant par L , $L(\varphi_0)$ est également un point fixe de L^P , donc φ_0 est un point fixe de L . Il est unique car tout point fixe de L est aussi point fixe de L^P . Finalement, φ_0 est l'unique solution sur $[a, b]$ du problème de Cauchy (4).

- Construction d'une solution globale

Pour tout $p \in \mathbf{N}^*$, on pose $K_p = [-p, p]$ et on note $\varphi_p \in \mathcal{C}^1(K_p, \mathbf{R}^n)$ l'unique solution du problème de Cauchy sur K_p . Tout réel t est élément d'un des K_p et on peut poser $p(t) = \min\{p \in \mathbf{N}^* \mid t \in K_p\}$. Posons

$$\varphi : \mathbf{R} \longrightarrow \mathbf{R}^n; \quad t \longmapsto \varphi_{p(t)}(t).$$

Soit $t_0 \in \mathbf{R}$. Il est à l'intérieur de $K_{p(t_0)+1}$ et donc par unicité de la solution de ce problème de Cauchy sur ce compact, pour tout entier $p \in \llbracket 1, p(t_0) \rrbracket$, φ_p coïncide avec $\varphi_{p(t_0)+1}$ sur K_p de sorte que sur $K_{p(t_0)+1}$ qui est un voisinage de t_0 , φ coïncide avec $\varphi_{p(t_0)+1}$. Donc φ est dérivable en t_0 et $\varphi'(t_0) = A(t_0)\varphi(t_0) + b(t_0)$. Comme t_0 est quelconque et comme $\varphi(0) = \varphi_1(0) = y_0$, φ est solution sur $\mathbf{R}$ de (4).

Soit ψ une solution sur $\mathbf{R}$ de (4). Par unicité de la solution sur $K_{p(t_0)+1}$, ψ coïncide avec φ sur $] -p(t_0)+1, p(t_0)+1[$ et donc $\psi(t_0) = \varphi(t_0)$ pour t_0 quelconque. D'où l'unicité de φ .

53 Prolongement méromorphe de la fonction Gamma d'Euler

Leçons : 207

Référence: Nom, Auteur

Proposition —

1. Γ est holomorphe sur $\Omega_0 = \{\Re(z) > 0\}$
2. Γ admet un unique prolongement méromorphe sur $\mathbf{C}$, holomorphe sur $\mathbf{C} \setminus \mathbf{Z}_-$.
3. Pour tout $z \in \Omega_0$, $\Gamma(z) = \lim_{n \rightarrow +\infty} \frac{n! n^z}{x(x+1) \dots (x+n)}$.

- Preuve du premier point

On applique le théorème d'holomorphicité sous l'intégrale à la fonction

$$\begin{aligned} f : \Omega_0 \times \mathbf{R}_+ &\longrightarrow \mathbf{C}; \\ (z, t) &\longmapsto e^{(z-1)\ln(t)} e^{-t}. \end{aligned}$$

- Pour tout $z \in \Omega_0$, $f(z, \cdot)$ est mesurable sur $\mathbf{R}_+$ car continue.
- Pour tout $t \in \mathbf{R}_+$, $f(\cdot, t) \in \mathcal{H}(\Omega_0)$.
- Pour tout $z \in \Omega_0$ de partie réelle contenue dans $]\varepsilon, M[$ avec $0 < \varepsilon < M < +\infty$, on a pour tout $t \in \mathbf{R}_+$:

$$|f(z, t)| = e^{(\Re(z)-1)\ln(t)} e^{-t} \leq \begin{cases} 1 & \text{si } t \leq 1, \\ t^{1-\varepsilon} & \text{si } t > 1. \end{cases}$$

Ainsi Γ est-elle holomorphe sur Ω_0 .

- Prolongement de Γ à $\mathbf{C} \setminus \mathbf{Z}_-$.

Soit $z \in \Omega_0$. Par une intégration par parties (attention aux bornes),

$$\Gamma(z+1) = \int_0^\infty t^z e^{-t} dt = [-t^z e^{-t}]_0^\infty + \int_0^\infty z t^{z-1} e^{-t} dt = z \int_0^\infty t^{z-1} e^{-t} dt = z \Gamma(z).$$

On en déduit par récurrence immédiate que pour tout $n \in \mathbf{N}$,

$$\Gamma(z+n) = (z+n-1)\Gamma(z+n-1) = \dots = \left(\prod_{j=0}^{n-1} (z+j) \right) \Gamma(z).$$

Posons alors $\Gamma_n : z \mapsto \frac{\Gamma(z+n)}{\prod_{j=0}^{n-1} (z+j)}$. Cette fonction est bien définie et holomorphe sur $\Omega_n = \{\Re(z) > -n\} \setminus \llbracket -(n-1), 0 \rrbracket$, et elle coïncide avec Γ sur Ω_0 . C'est donc un prolongement holomorphe de Γ .

Pour tout $n, m \in \mathbf{N}$, Γ_n et Γ_m coïncident sur $\Omega_m \cap \Omega_n$ par le théorème de prolongement analytique. Ainsi peut-on définir un unique prolongement analytique de Γ sur $\mathbf{C} \setminus \mathbf{Z}_-$ en posant $\Gamma(z) = \Gamma_n(z)$ où n est tel que $z \in \Omega_n$. Il vient alors que pour $n \in \mathbf{N}$ et $z \in \Omega_{n+1}$,

$$(z+n)\Gamma(z) = \frac{\Gamma(z+n+1)}{\prod_{j=0}^{n-1} (z+j)} \xrightarrow{z \rightarrow -n} \frac{\Gamma(1)}{(-1)^n n!} = \frac{(-1)^n}{n!}.$$

Donc Γ est méromorphe sur $\mathbf{C}$, de pôles les entiers $-\mathbf{N}$, tous simples de résidus $\frac{(-1)^n}{n!}$.

- Preuve de la formule de Gauss

Fixons $z_0 \in \Omega_0$. Par le théorème de convergence dominée, il vient

$$\Gamma(z) = \lim_{n \rightarrow +\infty} \int_0^n t^{z-1} \left(1 - \frac{t}{n}\right)^n dt = \lim_{n \rightarrow +\infty} I_n.$$

Soit $n \in \mathbf{N}$. En intégrant n fois par parties,

$$\begin{aligned}
 I_n &= \left[\frac{t^z}{z} \left(1 - \frac{t}{n} \right)^n \right]_0^n + \frac{n}{nz} \int_0^n t^z \left(1 - \frac{t}{n} \right)^{n-1} dt, \\
 &= \frac{n}{nz} \frac{n-1}{n(z+1)} \int_0^n t^{z+1} \left(1 - \frac{t}{n} \right)^{n-2} dt, \\
 &= \frac{n}{nz} \frac{n-1}{n(z+1)} \cdots \frac{1}{n(z+n-1)} \int_0^n t^{z+n-1} dt, \\
 &= \frac{n!n^z}{z(z+1) \cdots (z+n)}.
 \end{aligned}$$

54 Autres résultats rédigés toujours utiles

Hahn-Banach géométrique

Leçons : 181, 253

Référence: Demander à, Alan Pinoy

Théorème — (Hahn-Banach analytique) Soient E un espace vectoriel de dimension finie, G un sous-espace vectoriel de E , $g \in G^*$ et $p : E \rightarrow \mathbf{R}$ positivement homogène qui vérifie l'inégalité triangulaire, telle que

$$\forall x \in G, g(x) \leq p(x).$$

Alors il existe $\tilde{g} \in E^*$ qui prolonge g et telle que pour tout $x \in E$, $\tilde{g}(x) \leq p(x)$.

Théorème — (Hahn-Banach géométrique) Soient A et B des parties convexes non vides et disjointes de $\mathcal{E}$. Si A est ouvert, alors il existe un hyperplan H qui sépare A et B .

Preuve de Hahn-Banach analytique

On raisonne par récurrence sur $\text{codim}(G)$.

- Initialisation

Si $\text{codim}(G) = 0$ alors $G = E$ et $\tilde{g} = g$ convient.

- Hérédité

On va montrer que l'on peut prolonger g à tout espace de la forme $G \oplus \mathbf{R}u$, $u \in E \setminus G$.

En effet, si c'est le cas, en notant $\bar{g}$ ce prolongement et $\beta = \bar{g}(u)$, on a que pour tout $x \in G$ et tout $t \in \mathbf{R}$ que

$$\bar{g}(x + tu) = g(x) + t\beta \leq p(x + tu),$$

soit pour tout $x \in G$ et tout $t > 0$,

$$\begin{cases} g(x) + t\beta & \leq p(x + tu), \\ g(x) - t\beta & \leq p(x - tu). \end{cases}$$

En posant $y = \frac{x}{t}$, pour tout $y \in G$,

$$\begin{cases} g(y) + \beta & \leq p(y + u), \\ g(y) - \beta & \leq p(y - u). \end{cases}$$

On en déduit que pour tout $y, z \in G$,

$$g(z) - p(z - u) \leq \beta \leq p(y + u) - g(y),$$

soit finalement

$$\sup_{z \in G} \{g(z) - p(z - u)\} \leq \inf_{y \in G} \{p(y + u) - g(y)\}.$$

Si on récapitule, on a montré que le fait de prolonger g à $G \oplus \mathbf{R}u$ pour un $u \in E \setminus G$ quelconque est équivalent à montrer que $\sup_{z \in G} \{g(z) - p(z - u)\} \leq \inf_{y \in G} \{p(y + u) - g(y)\}$.

Montrons la propriété équivalente. Soient $y, z \in G$. Il suffit de remarquer que

$$g(y) + g(z) = g(z + y) \leq p(y, z) = p(y + u - u + z) \leq p(y + u) + p(z - u).$$

En réarrangeant cette inégalité et en passant respectivement aux bornes supérieure à gauche et inférieure à droite, on a montré que l'on peut prolonger g à $G \oplus \mathbf{R}u = \bar{G}$. Comme $\text{codim}(\bar{G}) = \text{codim}(G) - 1$, on peut appliquer l'hypothèse de récurrence à $\bar{g}$ pour obtenir le résultat. D'où l'hérédité.

Le théorème de Hahn-Banach analytique est donc vrai par principe de récurrence.

Preuve du théorème de Hahn-Banach géométrique

Commençons par démontrer un lemme :

| **Lemme** — Soit $\mathcal{C} \subset E$ convexe, ouvert, $x_0 \in E \setminus \mathcal{C}$. Alors on peut séparer $\mathcal{C}$ et $\{x_0\}$ par un hyperplan.

• Preuve du lemme.

Quitte à translater notre convexe, on a $0 \in \overset{\circ}{\mathcal{C}} = \mathcal{C}$. On pose $g(tx_0) = t$ et $\rho = J_{\mathcal{C}}$ la jauge du convexe. Alors,

$$\begin{cases} \forall t \in \mathbf{R}_+, & g(tx_0) = t \leq t\rho(x_0) = \rho(tx_0), \\ \forall t \in \mathbf{R}_-, & g(tx_0) = t < 0 \leq \rho(tx_0). \end{cases}$$

Si l'on prend α le prolongement de g donné par le théorème de Hahn-Banach analytique, alors $H = \text{Ker}(\alpha)$ convient.

• Preuve du théorème.

Soit $\mathcal{C} = A - B = \{a - b, a \in A, b \in B\}$. $\mathcal{C}$ est convexe, ouvert et disjoint de $\{0\}$ car A et B sont disjoints. Par le lemme, il existe une forme linéaire $\alpha \in E^*$ telle que pour tout $x \in \mathcal{C}$,

$$\alpha(x) \leq \alpha(0) = 0.$$

Cela revient à dire que pour tout $a \in A, b \in B$,

$$\alpha(a) \leq \alpha(b).$$

D'où la séparation des ensembles.

Dual de $M_n(\mathbf{K})$

Leçons : 159

Référence: Oraux X-ENS Algèbre ??, Francinou, Gianella, Nicolas

Proposition —

1. $f : M_n(\mathbf{K}) \rightarrow M_n(\mathbf{K})^*$; $A \mapsto \text{Tr}(A \cdot)$ est un isomorphisme.
2. Tr est la seule forme linéaire commutative à proportionnalité près : $\forall A, B \in M_n(\mathbf{K}), f \in M_n(\mathbf{K})^*$ et $f(AB) = f(BA) \Rightarrow f = \lambda \text{Tr}, \lambda \in \mathbf{K}$.
3. Tout hyperplan de $M_n(\mathbf{K})$ rencontre $GL_n(\mathbf{K})$.

1) La fonction f est bien évidemment linéaire (bilinéarité du produit matriciel et linéarité de la trace). De plus, $M_n(\mathbf{K})$ et son dual ont même dimension. Il suffit donc de montrer que f est injective. Soit donc $A \in M_n(\mathbf{K})$ qui annule f . On note, pour $i, j \in \llbracket 1, n \rrbracket^2$, $E_{i,j} = (\delta_{i,k} \delta_{j,l})_{1 \leq k, l \leq n}$ les matrices constituant la base canonique de $M_n(\mathbf{K})$. On rappelle que pour $i, j, k, l \in \llbracket 1, n \rrbracket$, $E_{i,j} E_{k,l} = \delta_{j,k} E_{i,l}$.

Alors, en écrivant $A = \sum_{1 \leq i, j \leq n} a_{i,j} E_{i,j}$, par linéarité de la trace,

$$\begin{aligned} 0 &= \text{Tr}(A E_{k,l}) = \sum_{1 \leq i, j \leq n} a_{i,j} \text{Tr}(E_{i,j} E_{k,l}), \\ &= \sum_{1 \leq i, j \leq n} a_{i,j} \text{Tr}(\delta_{j,k} E_{i,l}), \\ &= \sum_{i=1}^n a_{i,k} \text{Tr}(E_{i,l}), \\ &= a_{l,k}. \end{aligned}$$

Donc $A = 0$ et f est injective. On a montré que f est un isomorphisme.

2) Soit $A \in M_n(\mathbf{K})$ telle que $f_A = f(A)$ soit une forme linéaire vérifiant $f_A(MN) = f_A(NM)$ pour toutes matrices M et N . Par les propriétés de la trace, on voit que pour tout $(M, N) \in M_n(\mathbf{K})^2$,

$$(f_A(MN) = f_A(NM)) \Leftrightarrow \text{Tr}((AM - MA)N) = 0.$$

Fixons $M \in M_n(\mathbf{K})$. L'application $N, L \mapsto \text{Tr}({}^t N L)$ étant un produit scalaire, on voit que $AM - MA \in M_n(\mathbf{K})^\perp$ pour ce produit scalaire, donc $AM - MA = 0$. M étant quelconque, A commute avec toutes les matrices, donc en particulier avec les $M = E_{i,i}$. En regardant cela, on voit que les lignes et colonnes de A sont nulles à l'exception des coefficients diagonaux. A est donc diagonale. Cela revient à dire que $f_A = \lambda \text{Tr}$ où $A = \lambda I_n$.

3) Soit H un hyperplan de $M_n(\mathbf{R})$. On l'écrit comme le noyau d'une forme linéaire non nulle : par 1., $H = \text{Ker}(f_A)$ avec $A \in M_n(\mathbf{K})$. On note $r = \text{rg}(A)$. Alors A est équivalente à $J_r = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$: il existe $P, Q \in GL_n(\mathbf{K})$ telles que $A = P J_r Q$.

Soit $X \in M_n(\mathbf{R})$. On a $\text{Tr}(AX) = \text{Tr}(J_r(QXP))$ par propriétés de la trace. Comme Q et P sont inversibles, il suffit de trouver $Y \in GL_n(\mathbf{K})$ telle que $\text{Tr}(J_r Y) = 0$. On vérifie que

$$Y = \begin{pmatrix} 0 & \dots & \dots & 0 & 1 \\ 1 & 0 & \dots & \dots & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & 0 \end{pmatrix}$$

convient. Alors $X = Q^{-1} Y P^{-1}$ est un élément de $H \cap GL_n(\mathbf{K})$. D'où le résultat.

Théorème de Sylow

Leçons : 101, 103, 104

Référence: Cours d'algèbre, Perrin

Théorème — Soit G un groupe de cardinal $p^\alpha m$ avec p premier qui ne divise pas m .

1. G admet un p -Sylow. De plus, si H est un sous-groupe de G qui est un p -groupe, il existe un p -Sylow S qui contient H .
2. Les p -Sylow sont tous conjugués
3. Si on note k le nombre de p -Sylow, alors $k \equiv [p]$, et donc $k|m$.

On admet (on l'indiquera dans le plan de leçon) que $P = \{A = (a_{i,j}) \mid a_{i,j} = 0 \text{ si } i > j \text{ et } a_{i,i} = 1\}$ est un p -Sylow de $GL_n(\mathbf{F}_p)$.

On commence par montrer le lemme suivant :

Lemme — Soit H un sous-groupe de G et soit S un p -Sylow de G . Alors, il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p -Sylow de H .

Démonstration —

On fait opérer G sur G/S par translation à gauche. Alors, le stabilisateur de aS est aSa^{-1} . En effet, pour tout $s, t \in S$,

$$(ata^{-1})as = ats \in aS.$$

Or, H opère lui aussi sur G/S par restriction, et le stabilisateur de aS est alors $T_a = aSa^{-1}H$.

Pour tout $a \in G$, T_a est un p -groupe et en notant $\omega(aS)$ l'orbite de aS pour l'action, par la formule des classes,

$$\text{Card}(H/T_a) = \text{Card}(\omega(aS)).$$

Si tous ces nombres sont divisibles par p , il en est de même de $\text{Card}(G/S)$ qui est réunion disjointe des orbites, ce qui est absurde car S est un p -Sylow de G . Il en existe donc un qui n'est pas divisible par p et qui est donc un p -Sylow de H .

□

• Preuve du premier point

Par le théorème de Cayley, on injecte G dans $\mathfrak{S}_n$ qui lui-même se plonge dans $GL_n(\mathbf{F}_p)$ par les matrices de permutation. Or, P est un p -Sylow de $GL_n(\mathbf{F}_p)$, donc par le lemme, il existe un p -Sylow pour G .

Toujours grâce au lemme, si H est un p -sous-groupe de G et S est un p -Sylow de G , il existe $a \in G$ tel que T_a est un p -Sylow de H . Or, comme H est un p -groupe, $T_a = H$ par égalité des cardinaux. Donc $H \subset aSa^{-1}$ qui est un Sylow (en effet, tout groupe conjugué à un Sylow est un Sylow).

• Preuve du deuxième point

Si H est un Sylow, par le même raisonnement que précédemment, comme c'est un p -groupe, il est inclus dans un aSa^{-1} , et on a même égalité par égalité des cardinaux.

• Preuve du dernier point

On fait opérer G par conjugaison sur l'ensemble X de ses p -Sylow. Soit S un p -Sylow, il opère aussi sur X par restriction et on a (par une propriété générale sur les actions de groupe) :

$$\text{Card}(X) \equiv \text{Card}(X^S)[p].$$

Il faut donc montrer que $\text{Card}(X^S) = 1$. Comme $\{S\} \subset X^S$, on doit montrer qu'il n'y a pas d'autre élément.

Soit T un p -Sylow. On suppose que T est fixé par S , autrement dit pour tout $s \in S$, $sTs^{-1} = T$. Posons $N = \langle S, T \rangle$ le sous-groupe de G engendré par S et T . Alors, T et S sont des p -Sylow de N (car le cardinal de N divise celui de G et est divisible par p^α), mais comme T est distingué dans N , c'est en réalité le seul p -Sylow de N , donc $T = S$. Le dernier point est donc prouvé.