Développements d'agrégation

Benjamin Havret
École normale supérieure[1]

1. Préparation à l'agrégation effectuée à l'École normale supérieure de Cachan

Table des matières

Introduction

Ce fichier rassemble les développements que j'ai préparés lors de ma préparation à l'agrégation en 2016.

Mon but en les tapant était de me forcer à les écrire complètement, sans raccourci, afin de traquer les subtiles erreurs que je commettais en les rédigeant au brouillon. Ils ont ensuite été relus plusieurs fois donc ne devraient pas contenir de trop grosse faute. Malgré ça, ils contiennent encore probablement des erreurs. Si vous repérez une erreur, ou si vous avez des questions sur un développement, n'hésitez pas à me contacter par courriel (Prenom.Nom@normalesup.org).

En revanche, très peu de ces développements ont été testés en temps limité. Je ne pense pas qu'il y en ait qui soient vraiment trop longs, mais en tout état de cause tout dépend de votre façon de les exposer. Les suivants ont fait leurs preuves en oraux blancs : Théorème de Prokhorov ; Sous-groupes compacts de $\mathrm{GL}(E)$; Décomposition effective de Dunford ; Lemme d'Artin, $\int_0^1 \log\Gamma$ et formules de multiplication. ; Un théorème de Kronecker ; Algorithme de Berlekamp ; Équation de la chaleur sur le cercle ; Construction du pré-mouvement brownien ; Principe de localisation.

Concernant l'inclusion dans les leçons, elle n'est qu'indicative, et dépend évidemment des plans et des angles que vous choisissez. En tout état de cause il faut que le développement occupe une place logique dans le plan et ne soit pas introduit sans contexte. A posteriori, certains développements me paraissent un peu hors sujet par rapport aux leçons dans lesquelles je les incluais.

Pour mes oraux je suis tombé sur les leçons 108, pour laquelle j'ai démontré le Théorème de la base de Burnside, et 246, pour laquelle j'ai démontré le Principe de localisation.

Beaucoup de ces développements sont dus aux préparateurs et aux étudiants de la préparation à l'agrégation de l'ens de Cachan. Je me suis aussi beaucoup servi dans le polycopié de Loïc Devilliers (disponible sur sa page web) qui a fait un grand travail de réécriture pour un grand nombre de développements. Certains développements n'ont aucune référence bibliographique, soit parce que je n'en connaissais pas, soit parce que la méthode présentée dans les livres ne me plaisait pas. Pour ceux-là (et pour les autres aussi en fait), il m'était nécessaire de les connaitre parfaitement. Pour les autres, même si j'indique une référence, la présentation que je choisis diffère parfois de celle de la référence.

Développements communs aux leçons d'algèbre et d'analyse

1. Théorème de Cauchy–Kowalevski

Référence Aucune ! (d'après un document de Maxime Breden)

Leçons

- 124. Anneau des séries formelles. applications
- 220. Équations différentielles $X' = f(t, X)$. Exemples d'étude des solutions en dimension 1 et 2
- 243. Convergence des séries entières, propriétés de la somme. Exemples et applications
- 244. Fonctions développables en série entière, fonctions analytiques. Exemples

Théorème 1. *Soit I un intervalle de $\mathbf{R}$, y_0 un point de I et $F : I \to \mathbf{R}$ une fonction développable en série entière au voisinage de y_0. Pour tout $t_0 \in \mathbf{R}$, le problème de Cauchy*

$$\begin{cases} y' = F(y) \\ y(t_0) = y_0 \end{cases} \tag{1}$$

admet une unique solution développable en série entière au voisinage de t_0. En particulier si F est analytique sur I, alors l'équation $y' = F(y)$ admet une solution analytique sur tout son intervalle de définition.

Remarque 2. Pour la leçon 124. Anneau des séries formelles. applications, on préférera la formulation suivante : pour toute série formelle F, il existe une unique série formelle S telle que $S(0) = 0$ et satisfaisant $S' = F \circ S$. La démonstration est la même, à ce changement de formulation près.

Démonstration. Sans perte de généralité on peut supposer $t_0 = 0$, $y_0 = 0$.

Lemme 3. *Il existe une suite de polynômes P_k à coefficients entiers positifs, de degré k telle que pour toute fonction F développable en série entière en 0,*

1. *Si y est solution de (1) alors pour tout $k \geqslant 1$, $y^{(k)}(0) = P_k(F(0), \dots, F^{(k-1)}(0))$;*
2. *Si la série entière*

$$\sum_{k \geqslant 1} \frac{P_k(F(0), \dots, F^{(k-1)}(0))}{k!} t^k \tag{2}$$

a un rayon de convergence non nul alors sa somme est solution de (1).

Démonstration du lemme. La formule de Faa di Bruno fournit, pour $k \geqslant 1$, un polynôme Q_k à $2k$ variables et à coefficients entiers positifs tel que

$$(g \circ h)^{(k)} = Q_k \left(g' \circ h, \dots, g^{(k)} \circ h, h', \dots, h^{(k)} \right)$$

En particulier, si $y' = F(y)$, il existe P_k à k variables et à coefficients entiers positifs tel que

$$y^{(k)} = (F \circ y)^{(k-1)} = P_k(F(y), \dots, F^{(k-1)}(y)) :$$

il est défini par récurrence comme suit. $P_1(X_0) = X_0$ et

$$P_k(X_0, \dots, X_{k-1}) = Q_{k-1}(X_1, \dots, X_{k-1}, P_1(X_0), \dots, P_{k-1}(X_0, \dots, X_{k-2})).$$

En particulier si y est une solution de (1) on a

$$y^{(k)}(0) = P_k(F(0), \dots, F^{(k-1)}(0)).$$

D'autre part si la série entière (2) a un rayon de convergence non nul, notons ϕ sa somme. Les fonctions ϕ' et $F \circ \phi$ sont développables en série entière au voisinage de 0 (comme dérivée/composée de fonctions analytiques). Vérifions que leurs dérivées successives en 0 sont les mêmes, ce qui garantira l'égalité des deux fonctions et conclura la démonstration. Si $k \geqslant 1$, la formule de Faa-di Bruno puis la définition de P_{k+1} fournissent successivement les égalités

$$\begin{aligned}
(F \circ \phi)^{(k)}(0) &= Q_k \left(F' \circ \phi(0), \dots, F^{(k)} \circ \phi(0), \phi'(0), \dots, \phi^{(k)}(0) \right) \\
&= Q_k \left(F'(0), \dots, F^{(k)}(0), P_1(F(0)), \dots, P_k \left(F(0), \dots, F^{(k-1)}(0) \right) \right) \\
&= P_{k+1}(F(0), \dots, F^{(k)}(0)) \\
&= \phi^{(k+1)}(0).
\end{aligned}$$

Le lemme est démontré. □

Il reste à montrer que si F est développable en série entière autour de 0, disons avec un rayon de convergence R, alors la série entière (2) a un rayon de convergence non nul. Soit $r \in]0, R[$, puis $C > 0$ tel que pour tout $k \geqslant 0$,

$$\frac{|F^{(k)}(0)|}{k!} \leqslant \frac{C}{r^k}.$$

Puisque P_k est à coefficients positifs on a

$$\begin{aligned}
\left| P_k(F(0), \dots, F^{(k-1)}(0)) \right| &\leqslant P_k(|F(0)|, \dots, |F^{(k-1)}(0)|) \\
&\leqslant P_k \left(\frac{C0!}{r^0}, \dots, \frac{C(k-1)!}{r^{k-1}} \right) \\
&= P_k(g(0), \dots, g^{(k-1)}(0)),
\end{aligned}$$

où $g(y) = \frac{C}{r-y}$.

La fonction $\psi : y \mapsto r - \sqrt{r - 2Cy}$ est une solution de

$$\begin{cases} y' = g(y) \\ y(0) = 0 \end{cases},$$

qui est développable en série entière au voisinage de 0 (rayon de convergence $r/2C$). Ainsi sa série de Taylor, qui est grâce au lemme,

$$\sum_{k \geqslant 0} \frac{\psi^{(k)}(0)}{k!} t^k = \sum_{k \geqslant 0} \frac{P_k(g(0), \dots, g^{(k-1)}(0))}{k!} t^k$$

admet un rayon de convergence strictement positif, puis par comparaison, la série entière

$$\sum_{k\geqslant 1} \frac{P_k(F(0),\dots,F^{(k-1)}(0))}{k!} t^k$$

aussi. □

2. Extrema liés, billard convexe.

Référence

Leçons

- 159. Formes linéaires et hyperplans en dimension finie. Exemples et applications
- 214. Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications
- 215. Applications différentiables définies sur un ouvert de $\mathbf{R}^n$. Exemples et applications
- 217. Sous-variétés de $\mathbf{R}^n$. Exemples
- 219. Extremums : existence, caractérisation, recherche. Exemples et applications

Théorème 1. *Soient des fonctions réelles $f, g_1, \dots, g_r$ de classe C^1 définies sur un ouvert $U \subset \mathbf{R}^d$, et $\Gamma = \{x \in U \,:\, \forall i\, g_i(x) = 0\}$. Si $f|_\Gamma$ admet un extremum local en $a \in \Gamma$ et si les formes linéaires $\mathrm{d}g_i(a)$ forment une famille libre alors il existe des réels $\lambda_1, \dots, \lambda_r$, uniques, tels que*

$$\mathrm{d}f(a) = \sum_{i=1}^{r} \lambda_i \,\mathrm{d}g_i(a).$$

Démonstration. L'hypothèse assure que la matrice $\left(\frac{\partial g_i}{\partial x_j}\right)_{\substack{i\leqslant r\\ j\leqslant d}}$ est de rang r. Quitte à renuméroter la base de $\mathbf{R}^d$, on peut supposer que la matrice $\left(\frac{\partial g_i}{\partial x_j}\right)_{\substack{i\leqslant r\\ j\leqslant r}}$ est inversible. Écrivons $a = (\alpha, \beta) \in \mathbf{R}^{d-r} \times \mathbf{R}^r$, et plus généralement écrivons $x = (u, v)$. Le théorème des fonctions implicites garantit qu'il existe un voisinage $W \subset U$ de β, un voisinage $V \subset \mathbf{R}^{d-r}$ de α et une fonction $\phi : V \to W$ de classe C^1 tels que $\phi(\alpha) = \beta$ et

$$\Gamma \cap (V \times W) = \{(u, \phi(u)) \,:\, u \in V\}.$$

Ainsi $h : u \mapsto f(u, \phi(u))$, qui est de classe C^1 sur W, admet un extremum local en α, donc $\mathrm{d}h(\alpha) = 0$, c'est-à-dire

$$\partial_u f(a) + \partial_v f(a) \circ \mathrm{d}\phi(\alpha) = 0 \qquad \text{(forme linéaire sur } \mathbf{R}^{d-r}\text{)}. \tag{3}$$

Puisque pour tout u, on a $g_i(u, \phi(u)) = 0$, la même relation vaut aussi pour les g_i. On a donc pour tout $1 \leqslant i \leqslant r$

$$\partial_u g_i(a) + \partial_v g_i(a) \circ \mathrm{d}\phi(\alpha) = 0.$$

Ainsi le sous-espace de $\mathbf{R}^d$

$$E = \{(u, v) \,:\, v = \mathrm{d}\phi(\alpha) \cdot u\},$$

qui est de dimension $d - r$, est contenu dans chacun des hyperplans $\ker \mathrm{d}g_i(a)$. Par un argument de dimension on a en fait l'égalité

$$E = \bigcap_{i=1}^{r} \ker \mathrm{d}g_i(a).$$

Mais la relation (3) assure que $E \subset \ker \mathrm{d}f(a)$. Finalement on a

$$\bigcap_{i=1}^{r} \ker \mathrm{d}g_i(a) \subset \ker \mathrm{d}f(a),$$

ce qui fournit l'existence des multiplicateurs de Lagrange. □

Démonstration pour la leçon 217. L'hypothèse assure que $(g_1, \dots, g_r)$ est une submersion de $\mathbf{R}^d$ dans $\mathbf{R}^r$ et donc que Γ est (au voisinage de a) une sous-variété de $\mathbf{R}^d$ de dimension $d-r$ et d'espace vectoriel tangent en a $T_a\Gamma = \bigcap_{i=1}^r \ker \mathrm{d}g_i(a)$. Si $v \in T_a\Gamma$, il existe un chemin γ tracé sur Γ tel que $\gamma(0) = a$ et $\gamma'(0) = v$. Puisque $f \circ \gamma$ admet un extremum local en 0 on a $\mathrm{d}f(a) \cdot v = 0$. Ainsi on a

$$\bigcap_{i=1}^r \ker \mathrm{d}g_i(a) \subset \ker \mathrm{d}f(a),$$

ce qui fournit l'existence des multiplicateurs de Lagrange. □

Théorème 2. *Soit Ω un ouvert convexe non vide de $\mathbf{R}^2$ tel que $\partial\Omega$ soit une sous-variété C^1 de $\mathbf{R}^2$: c'est-à-dire que $\partial\Omega = \{g = 0\}$ pour une certaine submersion $g : \mathbf{R}^2 \to \mathbf{R}$. Il existe trois points A, B, C de $\partial\Omega$ telle que la droite normale à $\partial\Omega$ en A soit la bissectrice de l'angle $\widehat{BAC}$, de même pour les points B et C.*

Démonstration. L'idée est de trouver un triangle inscrit dans Ω de périmètre maximal et de vérifier qu'il satisfait à ces conditions. L'application

$$f : \left| \begin{array}{ccc} (\mathbf{R}^2)^3 & \longrightarrow & \mathbf{R} \\ (A,B,C) & \longmapsto & AB + AC + BC \end{array} \right.$$

est continue sur le compact $(\partial\Omega)^3$, donc y atteint un maximum, en (au moins) un triplet (A_0, B_0, C_0). Par ailleurs f est de classe C^1 sur l'ouvert U des triplets des points deux-à-deux distincts.

Montrons que $(A_0, B_0, C_0) \in U$. Sinon, disons que $A_0 = B_0$. Soit B_1 un autre point de $\partial\Omega$. L'inégalité triangulaire donne alors $f(A_0, B_1, C_0) > f(A_0, B_0, C_0)$, contredisant la maximalité de $f(A_0, B_0, C_0)$.

L'application

$$\phi : \left| \begin{array}{ccc} \mathbf{R}^2 \backslash \{B_0, C_0\} & \longrightarrow & \mathbf{R} \\ A & \longmapsto & f(A, B_0, C_0) \end{array} \right.$$

est de classe C^1. Le théorème des extrema liés garantit que

$$\nabla\phi(A_0) \in \mathrm{Vect}\, \nabla g(A_0),$$

c'est donc un vecteur normal à $\partial\Omega$. Or

$$\nabla\phi(A_0) = \frac{\overrightarrow{A_0B_0}}{A_0B_0} + \frac{\overrightarrow{A_0C_0}}{A_0C_0},$$

qui est un vecteur directeur de la bissectrice de l'angle $\widehat{B_0A_0C_0}$. □

Compléments : conditions suffisantes de minimum local

Théorème 3. *Soient des fonctions réelles $f, g_1, \dots, g_r$ de classe C^1 définies sur un ouvert $U \subset \mathbf{R}^d$, $\Gamma = \{x \in U \,:\, \forall i\, g_i(x) = 0\}$, et $a \in \Gamma$. Supposons que les formes linéaires $\mathrm{d}g_i(a)$ forment une famille libre et qu'il existe des réels $\lambda_1, \dots, \lambda_r$ tels que*

$$\mathrm{d}f(a) = \sum_{i=1}^r \lambda_i\, \mathrm{d}g_i(a).$$

Si de plus la fonction $f - \sum \lambda_i g_i$ est convexe sur $\mathbf{R}^d$ ou si la restriction de sa différentielle seconde à

$$T_a\Gamma = a + \bigcap_{i=1}^r \ker \mathrm{d}g_i(a)$$

est définie positive alors $f|_\Gamma$ admet un minimum local en a.

3. Méthode de Newton pour les polynômes

Référence A. Chambert-Loir, D. Firmigier Maillot *tome 2*

Leçons

- 144. Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications
- 218. Applications des formules de Taylor
- 223. Suites numériques. Convergence, valeurs d'adhérence. Exemples et applications
- 224. Exemples de développements asymptotiques de suites et de fonctions
- 232. Méthodes d'approximation des solutions d'une équation $F(X) = 0$. Exemples

Théorème 1. *Soit P un polynôme unitaire scindé sur $\mathbf{R}$. Soit $\xi_1 < \ldots < \xi_r$ ses racines, et m_j leur multiplicité. Considérons la méthode de Newton*

$$x_{n+1} = x_n - \frac{P(x_n)}{P'(x_n)}$$

pour $x_0 > \xi_r$. La suite est bien définie, décroît strictement vers ξ_r. Si $m_r = 1$ alors pour tout $c > 0$

$$|x_n - \xi_r| = o(c^n).$$

Si $m_r > 1$, il existe une constante $\lambda > 0$ tel que

$$|x_n - \xi_r| \sim \lambda \left(1 - \frac{1}{m_r}\right)^n.$$

Démonstration. Introduisons la fonction

$$f : \left| \begin{array}{ccc}]\xi_r, +\infty[& \longrightarrow & \mathbf{R} \\ x & \longmapsto & x - \frac{P(x)}{P'(x)} \end{array} \right. .$$

1. Étude de la fonction f. Le théorème de Gauss-Lucas garantit que P et toutes ses dérivées sont strictement positifs sur $]\xi_r, +\infty[$. Ainsi f est bien définie et pour tout $x > \xi_r$, $f(x) < x$. Comme

$$\frac{P'}{P} = \sum_{i=1}^{r} \frac{m_i}{X - \xi_i},$$

$P'(x)/P(x)$ tend vers $+\infty$ lorsque x tend vers ξ_r^+. La fonction f se prolonge par continuité en posant $f(\xi_r) = \xi_r$.
Enfin constatons que $f' = \frac{PP''}{P'^2} > 0$ sur $]\xi_r, +\infty[$. Finalement f est strictement croissante $[\xi_r, +\infty[\to [\xi_r, +\infty[$. La bonne définition de la suite (x_n) s'ensuit, et sa décroissance, vers un point fixe de f dans $[\xi_r, +\infty[$, qui ne peut être que ξ_r (pour tout $x > \xi_r$, $f(x) < x$).

2. Montrons que $f'(\xi_r^+) = 1 - \frac{1}{m_r}$. Dérivant P'/P on obtient

$$\frac{P''P}{P^2} - \frac{P'^2}{P^2} = -\sum_{i=1}^{r} \frac{m_i}{(X - \xi_i)^2},$$

donc

$$f'(x) = \frac{P''P}{P'^2}(x) = 1 + \frac{\frac{P''P}{P^2} - \frac{P'^2}{P^2}}{\left(\frac{P'}{P}\right)^2} = 1 - \frac{\sum_{i=1}^{r} \frac{m_i}{(X-\xi_i)^2}}{\left(\sum_{i=1}^{r} \frac{m_i}{X-\xi_i}\right)^2} \underset{x \to \xi_r^+}{\longrightarrow} 1 - \frac{1}{m_r}.$$

3. Si $m_r = 1$. On a donc $f'(\xi_r) = 0$. Soit $c > 0$ puis $\epsilon > 0$ tel que si $|x - \xi_r| \leqslant \epsilon$, $|f'(x)| \leqslant c$, et enfin N tel que si $n \geqslant N$, $|x_n - \xi_r| \leqslant \epsilon$. L'inégalité de Taylor-Lagrange donne

$$\left|\frac{f(x_n) - \xi_r}{x_n - \xi_r}\right| \leqslant \sup_{[\xi_r, x_n]} |f'| \leqslant c.$$

Ainsi pour tout $n \geqslant N$,

$$|x_n - \xi_r| \leqslant c^{n-N}|x_N - \xi_r|.$$

4. Si $m_r > 1$. Pour les mêmes raisons

$$\left|\frac{f(x_n) - \xi_r}{x_n - \xi_r}\right| \leqslant \sup_{[\xi_r, x_n]} |f'| \leqslant C < 1$$

pour n assez grand (prendre $C \in]1 - \frac{1}{m_r}, 1[$). Ainsi $|x_n - \xi_r| = O(C^n)$. Puis une formule de Taylor-Lagrange à l'ordre 2 donne

$$\frac{f(x_n) - \xi_r}{x_n - \xi_r} = 1 - \frac{1}{m_r} + O(x_n - \xi_r),$$

puis

$$\frac{f(x_n) - \xi_r}{(x_n - \xi_r)\left(1 - \frac{1}{m_r}\right)} = 1 + O(C^n).$$

En prenant le logarithme,

$$\log(x_{n+1} - \xi_r) - \log(x_n - \xi_r) = \log\left(1 - \frac{1}{m_r}\right) + O(C^n),$$

puis par sommation des relations de comparaison, il existe une constante μ telle que

$$\log(x_n - \xi_r) = n \log\left(1 - \frac{1}{m_r}\right) + \mu + o(1).$$

□

4. Simplicité du groupe spécial orthogonal $\mathrm{SO}_n(\mathbf{R})$

Référence S. Gonnord et N. Tosel

Leçons

- 103. Exemples et applications des notions de sous-groupes distingués et de groupes quotients. Applications
- 160. Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie)
- 161. Isométries d'un espace affine euclidien de dimension finie. Applications en dimension 2 et 3
- 204. Connexité. Exemples et applications
- 217. Sous-variétés de $\mathbf{R}^n$. Exemples

Théorème 1. *Pour tout entier impair n supérieur à 3, le groupe spécial orthogonal $\mathrm{SO}_n(\mathbf{R})$ est simple.*

On notera $\mathfrak{so}_n(\mathbf{R})$ l'ensemble des matrices antisymétriques réelles.

Démonstration. Soit G un sous-groupe distingué de $\mathrm{SO}_n(\mathbf{R})$, et non réduit à $\{I_n\}$. Il s'agit de démontrer que $G = \mathrm{SO}_n(\mathbf{R})$. Pour cela, travaillant avec la topologie usuelle induite sur $\mathrm{SO}_n(\mathbf{R})$, constatons que si G contient un voisinage de l'identité, c'est-à-dire $I_n \in \overset{\circ}{G}$, on a les égalités

$$G = \bigcup_{g\in G} g\overset{\circ}{G}, \qquad \text{et} \qquad \mathrm{SO}_n(\mathbf{R})\backslash G = \bigcup_{g\in \mathrm{SO}_n(\mathbf{R})\backslash G} g\overset{\circ}{G},$$

qui font de G une partie ouverte et fermée du connexe $\mathrm{SO}_n(\mathbf{R})$. Ainsi, G n'étant pas vide, il s'ensuit $G = \mathrm{SO}_n(\mathbf{R})$. Il est donc suffisant d'établir que G contient un voisinage de l'identité. On va pour cela construire un C^1 difféomorphisme local autour de I_n, de $\mathrm{SO}_n(\mathbf{R})$ sur G. Il va prendre la forme suivante.

Version 1 : avec le langage des sous-variétés : Si $w_1, \dots, w_n \in G$, on considère l'application

$$\psi : \left| \begin{array}{ccc} \mathrm{SO}_n(\mathbf{R}) & \longrightarrow & G \subset \mathrm{SO}_n(\mathbf{R}) \\ u & \longmapsto & [uw_1u^{-1}w_1^{-1}]\dots[uw_ru^{-1}w_r^{-1}] \end{array} \right. .$$

Sa différentielle en I_n est l'application

$$\ell = \mathrm{d}\psi_{I_n} : \left| \begin{array}{ccc} \mathfrak{so}_n(\mathbf{R}) & \longrightarrow & \mathfrak{so}_n(\mathbf{R}) \\ u & \longmapsto & \sum_{j=1}^r u - w_juw_j^{-1} \end{array} \right. .$$

Version 2 : sans sous-variétés : Si $w_1, \dots, w_n \in G$, on considère l'application

$$\psi : \left| \begin{array}{ccc} \mathbf{M}_n(\mathbf{R}) & \longrightarrow & \mathbf{M}_n(\mathbf{R}) \\ u & \longmapsto & [uw_1u^{-1}w_1^{-1}]\dots[uw_ru^{-1}w_r^{-1}] \end{array} \right. .$$

Sa différentielle en I_n est l'application

$$\ell = \mathrm{d}\psi_{I_n} : \left| \begin{array}{ccc} \mathbf{M}_n(\mathbf{R}) & \longrightarrow & \mathbf{M}_n(\mathbf{R}) \\ u & \longmapsto & \sum_{j=1}^r u - w_juw_j^{-1} \end{array} \right. .$$

On utilise la paramétrisation suivante de $\mathrm{SO}_n(\mathbf{R})$:

$$\chi : \left| \begin{array}{ccc} \mathbf{M}_n(\mathbf{R}) & \longrightarrow & \mathbf{M}_n(\mathbf{R}) \\ h & \longmapsto & \exp(h) \\ \big(\mathfrak{so}_n(\mathbf{R}) & \longrightarrow & \mathrm{SO}_n(\mathbf{R})\big) \end{array} \right. .$$

Sa différentielle en 0 est Id, qui est inversible. Par conséquent χ est un C^1 difféomorphisme local de $0 \in U$ dans $I_n \in V$. Considérons

$$\tilde{\psi} = \chi^{-1} \circ \psi \circ \chi : U \to V.$$

Comme $\chi(\mathfrak{so}_n(\mathbf{R})) = \mathrm{SO}_n(\mathbf{R})$, on peut restreindre $\tilde{\psi}$:

$$\tilde{\psi} : U \cap \mathfrak{so}_n(\mathbf{R}) \to V \cap \mathfrak{so}_n(\mathbf{R}).$$

Sa différentielle en 0 est $\mathrm{d}\psi_{I_n}|_{\mathfrak{so}_n(\mathbf{R})}$. Si elle est inversible, alors $\tilde{\psi}$ est un C^1 difféomorphisme local. En particulier $\chi^{-1} \circ \psi \circ \chi(\mathfrak{so}_n(\mathbf{R}))$ est un voisinage de 0, donc

$$\psi \circ \chi(\mathfrak{so}_n(\mathbf{R})) = (\chi^{-1})^{-1} \left(\chi^{-1} \circ \psi \circ \chi(\mathfrak{so}_n(\mathbf{R}))\right)$$

est un voisinage de I_n dans $\mathrm{SO}_n(\mathbf{R})$. Or c'est une partie de G, qui se trouve par conséquent être un voisinage de I_n dans $\mathrm{SO}_n(\mathbf{R})$.

Retour au programme commun : On souhaite que $\mathrm{d}\psi_{I_n}$ soit une application linéaire injective. Nous allons exploiter la stricte convexité de la norme euclidienne $\|M\| = \mathrm{Tr}(MM^{\mathbf{T}})$ sur $\mathbf{M}_n(\mathbf{R})$. Soit $u \in \mathfrak{so}_n(\mathbf{R})$ satisfait $\ell(u) = 0$, c'est-à-dire

$$u = \frac{1}{r} \sum_{j=1}^{r} w_j u w_j^{-1}.$$

D'autre part comme pour tout $w \in O_n(\mathbf{R})$, $\|u\| = \|wuw^{-1}\|$, on a

$$\|u\| = \frac{1}{r} \sum_{j=1}^{r} \|w_j u w_j^{-1}\|.$$

Il s'ensuit

$$\left\| \frac{1}{r} \sum_{j=1}^{r} w_j u w_j^{-1} \right\| = \frac{1}{r} \sum_{j=1}^{r} \|w_j u w_j^{-1}\|,$$

ce qui par stricte convexité de la norme euclidienne sur la sphère impose que pour tout j, $w_j u w_j^{-1} = u$, c'est-à-dire que u commute avec chacun des w_j. Attachons-nous donc à trouver des éléments $w_1, \ldots, w_r \in G$ tels que la seule matrice antisymétrique commutant avec chacun d'eux soit la matrice nulle. S'ensuivra l'injectivité de la différentielle $\mathrm{d}\psi_{I_n}$, puis, grâce au théorème d'inversion locale (version sous-variétés), le fait que $G \supset \psi(\mathrm{SO}_n(\mathbf{R}))$ contient un voisinage de I_n (au sens de la topologie induite sur $\mathrm{SO}_n(\mathbf{R})$), concluant la démonstration.

Donnons-nous un élément $w \in G$ distinct de I_n. Puisqu'en outre n est impair, on a

$$\{0\} \neq \ker(w - I_n) \neq \mathbf{R}^n.$$

Notons V ce sous-espace, et d sa dimension. Constatons que si $g \in \mathrm{SO}_n(\mathbf{R})$, $\ker(gwg^{-1} - I_n) = g(V)$, et, comme $G \lhd \mathrm{SO}_n(\mathbf{R})$, gwg^{-1} est encore un élément de G. Choisissons une famille (g_J) d'éléments de $\mathrm{SO}_n(\mathbf{R})$ paramétrée par $J \in \mathcal{J} = \mathfrak{P}_d(\{1, \ldots, n\})$ (parties à d éléments), telle que $g_J(V) = \mathrm{Vect}_{j \in J}\, e_j$. Puis posons $w_J = g_J w g_J^{-1}$. Si une matrice antisymétrique commute avec chacun des w_J, alors elle laisse stable chacun des $g_J(V)$, donc chacune des droites $\mathbf{R}e_j$: autrement dit c'est une matrice antisymétrique et diagonale, elle est donc nulle. □

5. Sous-groupes compacts de $\mathrm{GL}(E)$

Référence Szpirglas, *Algèbre L3.*

Leçons

- 106. Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $\mathrm{GL}(E)$. Applications
- 150. Exemples d'actions de groupes sur les espaces de matrices
- 160. Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie)
- 181. Barycentres dans un espace affine réel de dimension finie, convexité. Applications
- 203. Utilisation de la notion de compacité
- 206. Théorèmes de point fixe. Exemples et applications
- 208. Espaces vectoriels normés, applications linéaires continues. Exemples
- 253. Utilisation de la notion de convexité en analyse

Commençons par un théorème de point fixe.

Théorème 1. *Soit K une partie convexe et compacte d'un espace euclidien E, et H un sous-groupe compact de $\mathrm{GL}(E)$ dont tous les éléments laissent stable K. Il existe, dans K, un point fixe commun à tous les éléments de H.*

Démonstration. Introduisons ce que nous allons établir être une norme

$$N(x) = \max_{h\in H} \|h(x)\|.$$

Pour tout $x \in E$, il existe, par compacité, $h \in H$ tel que $N(x) = \|h(x)\|$. Ainsi $N(x)$ n'est nul que si x l'est. L'inégalité triangulaire et l'homogénéité ne posent pas de problème.
La norme N est strictement convexe : si $N(x+y) = N(x) + N(y)$ alors x et y sont positivement liés. En effet soit $h \in H$ tel que $N(x+y) = \|h(x+y)\|$. On a

$$\|h(x)\| + \|h(y)\| \leqslant N(x) + N(y) = N(x+y) = \|h(x+y)\| \leqslant \|h(x)\| + \|h(y)\|,$$

qui implique par stricte convexité de la norme euclidienne que $h(x)$ et $h(y)$ sont positivement liés, donc x et y aussi.
Considérons enfin un point $y \in K$ minimisant la norme N. Nous allons établir que c'est un point fixe commun aux éléments de H. Si h est un élément de H, $g \mapsto gh$ étant une bijection de H sur lui-même, il vient

$$N(h(y)) = N(y).$$

Le vecteur $h(y) \in K$ réalise donc également un minimum de N sur K. Comme K est convexe $\frac{1}{2}(y + h(y)) \in K$, donc

$$N\left(\frac{1}{2}(y+h(y))\right) \geqslant \min_{x\in K} N(x) = N(y) = N(h(y)) = \frac{1}{2}(N(y) + N(h(y))).$$

Utilisant d'autre part l'inégalité triangulaire et l'homogénéité de la norme N, il vient

$$N(y + h(y)) = N(y) + N(h(y)).$$

La stricte convexité de N assure que y et $h(y)$ sont positivement liés, et, ayant la même norme, sont égaux. Le vecteur $y \in K$ est donc un point fixe commun aux éléments de H. □

Théorème 2. *Soit G est un sous-groupe compact du groupe linéaire* $\mathrm{GL}(E)$ *d'un espace euclidien E. Il existe $u \in \mathrm{GL}(E)$ tel que uGu^{-1} soit un sous-groupe de $O(E)$.*

Démonstration. Introduisons l'endomorphisme

$$\Psi : \begin{array}{ccc} G & \longrightarrow & \mathrm{GL}(\mathrm{S}(E)) \\ g & \longmapsto & (s \mapsto gsg^*) \end{array}.$$

Soit $H = \Psi(G)$: c'est un sous-groupe compact de $\mathrm{GL}(\mathrm{S}(E))$. Puis considérons

$$\kappa = \{gg^* \,:\, g \in G\},$$

et K son enveloppe convexe. Le théorème de Carathéodory garantit que K est un compact. Comme G est compact, c'est en fait une partie compacte de $\mathrm{S}^{++}(E)$. Et, G étant un groupe, κ est stable par les éléments de H, K aussi par linéarité. Le théorème de point fixe précédemment établi fournit l'existence d'un point fixe $s \in K$ commun aux éléments de H : pour tout $g \in G$, $s = gsg^*$. Si r est la racine carrée de s, on a finalement pour tout $g \in G$,

$$r^2 = gr^2g^*.$$

C'est-à-dire

$$(r^{-1}gr)(r^{-1}gr)^* = I_n.$$

Aussi $r^{-1}Gr$ est-il un sous-groupe de $O(E)$. □

6. Convergence des méthodes de Jacobi et de Gauss-Seidel

Référence G. Allaire et S.-M. Kaber, *Algèbre linéaire numérique* (p.155).

Leçons

- 158. Matrices symétriques réelles, matrices hermitiennes
- 162. Systèmes d'équations linéaires ; opérations, aspects algorithmiques et conséquences théoriques
- 233. Analyse numérique matricielle : résolution approchée de systèmes linéaires, recherche de vecteurs propres, exemples

Développements d'algèbre

7. Automorphismes de $k(X)$

Référence Szpirglas, *Algèbre L3*

Leçons

- 122. Anneaux principaux. Applications
- 140. Corps des fractions rationnelles à une indéterminée sur un corps commutatif. Applications
- 141. Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications

Soit A un anneau principal (intègre en particulier), et K son corps des fractions.

Définition 1 (Contenu d'un polynôme)**.** Le contenu d'un polynôme $P \in A[X]$, noté $c(P)$ est le pgcd de ses coefficients (il est défini à un inversible près en fait).

Lemme 2 (Lemme de Gauss)**.** *Soit $P, Q \in A[X]$. On a $c(PQ) = c(P)c(Q)$.*

Démonstration. Quitte à factoriser P et Q par leur contenu, on peut supposer qu'ils sont de contenu 1. Supposons par l'absurde que le contenu de PQ soit distinct de 1, c'est-à-dire que les coefficients de PQ ont un diviseur irréductible commun d. Puisque A est principal, l'idéal (d) est maximal donc $L = A/(d)$ est un corps. Projetée dans $L[X]$, l'identité $PQ = PQ$ devient $\bar{P}\bar{Q} = \overline{PQ} = 0$. Mais, $L[X]$ étant intègre ceci impose $\bar{P} = 0$ et $\bar{Q} = 0$ et entre en contradiction avec le fait que P et Q ont un contenu égal à 1 □

Lemme 3. *Tout polynôme $P \in A[X]$, irréductible sur $A[X]$ l'est sur $K[X]$.*

Démonstration. Supposons que $P = QR$, avec Q et R de degré au moins 1. L'hypothèse assure qu'ils ne peuvent pas être tous deux dans $A[X]$. Disons que $Q \in K[X]\backslash A[X]$. Soit $a \in A$ non nul tel que $aQ \in A[X]$ et soit de contenu 1. Alors $P = aQ(R/a)$. L'hypothèse nous dit que $S = R/a \notin A[X]$. Soit $b \in A$ non nul, (et nécessairement non inversible) tel que $bS \in A[X]$ et soit de contenu 1. On a alors

$$bP = (aQ)(bS).$$

Mais le membre de gauche a un contenu divisible par b tandis que le membre de droite a pour contenu 1. C'est absurde. □

Théorème 4. *Soit k un corps.*

$$\mathrm{Aut}(k(X)) = \left\{ F \mapsto F\left(\frac{aX+b}{cX+d}\right) \ : \ a,b,c,d \in k,\ ad - bc \neq 0 \right\}.$$

Démonstration. Pour l'inclusion de droite à gauche, il suffit de voir que

$$F \mapsto F\left(\frac{dX-b}{-cX+a}\right)$$

est la bijection réciproque.

Pour l'inclusion directe : soit $\sigma \in \mathrm{Aut}(k(X))$. Notons $F = \sigma(X)$. Puisque σ est un automorphisme on a

$$k(F) = k(\sigma(X)) = \sigma(k(X)) = k(X).$$

En particulier $X \in k(F)$. Écrivons F sous forme irréductible : $F = P/Q$. Considérons le polynôme suivant dans $k[F][T]$:

$$W(F)(T) = P(T) - FQ(T).$$

En l'évaluant en $X \in k(F)$, on obtient $W(X) = 0$. Ainsi le polynôme $T - X \in k(F)[T]$ divise W. On peut écrire

$$W(F)(T) = (T-X)S(F)(T) \qquad \text{avec } S(F)(T) \in k(F)[T]. \tag{4}$$

La suite de la démonstration a pour but d'établir que $S \in k(F)$.

Vérifions déjà que W est irréductible dans $k[F][T]$. Si $W = AB$, où $A, B \in k[F][T]$, cette décomposition vaut aussi dans $k[T][F]$. Puisque le degré partiel en F de W est 1, celui de A ou B est nul : écrivons donc sans perte de généralité $A = A(T) \in k[T]$ et $B = C(T) + FD(T)$. Le fait que $AB = W$ impose

$$A(T)C(T) = P(T) \qquad \text{et} \qquad A(T)D(T) = Q(T).$$

En particulier $A(T)$ divise $P(T)$ et $Q(T)$, donc, puisque $P(T)$ et $Q(T)$ sont irréductibles, A est constant. Ceci prouve que W est irréductible dans $k[F][T]$.

Le lemme qui précède assure, puisque $k[F]$ est un anneau principal, que W est irréductible dans $k(F)[T]$. Or $T - X$ le divise, donc il est de degré 1 en T. Ceci impose que P et Q sont de degré 1, concluant la démonstration (la condition $ad - bc \neq 0$ étant clairement nécessaire).

<u>Une autre méthode</u> Écrivons $X \in k(F)$ sous forme irréductible : $X = \alpha(F)/\beta(F)$. Par conséquent

$$W(F)(T) = (\alpha(F)T - \beta(F))\frac{S(F)(T)}{\beta(F)}.$$

Puisque W est irréductible dans $k[F][T]$, soit $\frac{S(F)(T)}{\beta(F)} \in k$, soit ce est un élément de $k(F)[T] \backslash k[F][T]$. Dans ce cas, en le factorisant par le ppcm $\delta(F)$ des dénominateurs de ses coefficients dans leur écriture en fraction irréductible, on peut écrire

$$\delta(F)W(F)(T) = (\alpha(F)T - \beta(F))U(F)(T).$$

En prenant le contenu, on obtient $\delta(F) \in k$, ce qui est absurde. On a donc établi que $W(F)(T)$ est de degré 1 en T, et on conclut comme précédemment □

8. Algorithme de Berlekamp

Référence M. Demazure, *Cours d'algèbre*

Leçons

— 123. Corps finis. Applications

— 141. Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications

Soit q une puissance d'un nombre premier p, et $P \in \mathbf{F}_q[X]$.

Proposition 1. *Si $P' = 0$, alors il existe $Q \in \mathbf{F}_q[X]$ tel que $P = Q(X)^p$. Sinon, soit $\operatorname{pgcd}(P, P') = 1$, et P est sans facteur carré, soit $\operatorname{pgcd}(P, P')$ est diviseur non trivial de P.*

Démonstration. Si $P' = 0$, il existe $R \in \mathbf{F}_q[X]$ tel que $P = R(X^p)$. Notant a_i les coefficients de R, et posant $b_i = a_i^{q/p}$, puis $Q = \sum b_i X^i$, on a $P = Q(X)^p$. □

Théorème 2 (Algorithme de Berlekamp)**.** *Supposons $P = P_1 \dots P_r$ sans facteur carré. Introduisons l'application*

$$\psi_P : \left| \begin{array}{ccc} \mathbf{F}_q[X]/(P) & \longrightarrow & \mathbf{F}_q[X]/(P) =: K_P \\ Q & \longmapsto & Q^q \end{array} \right. .$$

C'est une application linéaire et $\dim \ker(\psi_P - I) = r$.

Démonstration. L'application est $\mathbf{F}_q-$linéaire par propriété du morphisme de Frobenius. Notons $V = \ker(\psi_P - I)$. On a $Q \in V$ si et seulement si $P \mid Q^q - Q$, ce qui équivaut à $P_j \mid Q^q - Q$ pour tout $j \leqslant r$. Le lemme chinois fournit un isomorphisme d'anneaux

$$\begin{array}{ccc} K_P & \longrightarrow & K_{P_1} \times \cdots \times K_{P_r} \\ Q & \longmapsto & (Q \mod P_1, \dots, Q \mod P_r) \end{array} .$$

Puisque chaque P_i est irréductible, les anneaux K_{P_i} sont des corps, extensions de $\mathbf{F}_q$ donc dans lesquels le polynôme $Y^q - Y$ a q racines. Vu l'isomorphisme, l'équation $Q^q - Q = 0$ a donc q^r solutions dans K_P. Ainsi $\dim \ker(\psi_P - I) = r$. Ce qui conclut la démonstration du théorème. En fait si $r \geqslant 2$, on peut trouver explicitement un diviseur de P. Soit en effet $Q \in \mathbf{F}_q[X]$ de degré $\geqslant 1$ et $< \deg P$ tel que $P \mid Q^q - Q$, ce que l'on récrit $\operatorname{pgcd}(P, Q^q - Q) = P$. Or

$$Q^q - Q = \prod_{\alpha \in \mathbf{F}_q} (Q - \alpha).$$

et, grâce au théorème de Bezout, ces facteurs sont deux-à-deux premiers entre eux. Conséquemment,

$$P = \prod_{\alpha \in \mathbf{F}_q} \operatorname{pgcd}(P, Q - \alpha).$$

Comme $1 \leqslant \deg Q < \deg P$, on a, pour tout $\alpha \in \mathbf{F}_q$, $1 \leqslant \deg(Q - \alpha) < \deg P$, et par suite $\deg(\operatorname{pgcd}(P, Q - \alpha)) < \deg P$. Par conséquent l'un des facteurs $\operatorname{pgcd}(P, Q - \alpha)$ est de degré au moins 1 : c'est un diviseur non trivial de P. □

Si le temps le permet : un mot sur la complexité. Notons $\delta = \deg P$ Le calcul de la matrice de ψ_P demande

9. Théorème de la base de Burnside

Référence M. Zavidovique, *Un max de maths.*

Leçons

- 101. Groupe opérant sur un ensemble. Exemples et applications
- 103. Exemples et applications des notions de sous-groupes distingués et de groupes quotients. Applications
- 104. Groupes finis. Exemples et applications
- 108. Exemples de parties génératrices d'un groupe. Applications
- 151. Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications

Soit G un p-groupe.

Définition 1. Un sous-groupe maximal de G est un sous-groupe strict de G maximal pour l'inclusion. On note $\mathcal{M}$ leur ensemble.

Lemme 2. *Tout sous-groupe maximal de G est distingué, et son quotient est isomorphe à $\mathbf{Z}/p\mathbf{Z}$.*

Démonstration. Considérons un sous-groupe maximal H de G, et son normalisateur N. La formule des classes (pour l'action de H sur G/H par translation à gauche) pour les p-groupes assure que p divise $|N/H| = |(G/H)^H|$, cardinal au moins égal à p donc. Ainsi, $|N| > |H|$, et par maximalité, $N = G$, c'est-à-dire que $H \lhd G$. Puisque H est maximal, le p-groupe G/H n'a pas de sous-groupe propre, il est donc cyclique, puis isomorphe à $\mathbf{Z}/p\mathbf{Z}$ (cyclique d'ordre premier). □

Théorème 3. *Les parties génératrices de G minimales (pour l'inclusion) ont toutes le même cardinal.*

Démonstration. Considérons le sous-groupe $\Phi(G) = \bigcap_{H\in\mathcal{M}} H$ de G. Le lemme précédent garantit que c'est un sous-groupe distingué de G. Montrons déjà le théorème pour le groupe $G/\Phi(G)$. Pour cela on va munir $G/\Phi(G)$ d'une structure de $\mathbf{F}_p$-espace vectoriel. Déjà, puisque pour tout $H \in \mathcal{M}$, le groupe G/H est abélien (lemme 2), le groupe dérivé $D(G)$ est contenu dans chacun des éléments de $\mathcal{M}$ donc dans $\Phi(G)$; aussi $G/\Phi(G)$ est-il abélien. Par ailleurs pour tout $x \in G$, et tout $H \in \mathcal{M}$, le lemme assure que $x^p \in H$. Ainsi pour tout $x \in G$, $x^p \in \Phi(G)$. Ceci permet de munir $G/\Phi(G)$ d'une structure de $\mathbf{F}_p$-espace vectoriel (ici on utilise une notation multiplicative pour l'opération interne d'espace vectoriel !). Les parties génératrices de $G/\Phi(G)$ de minimales pour l'inclusion sont des $\mathbf{F}_p$-familles génératrices de $G/\Phi(G)$ minimales (pour l'inclusion). La théorie de la dimension affirment qu'elles ont toutes le même cardinal.

Enfin pour conclure, notant π la projection $G \to G/\Phi(G)$, montrons qu'une famille (g_i) engendre G si et seulement si la famille $(\pi(g_i))$ engendre $G/\Phi(G)$. L'implication directe est immédiate : elle découle de la surjectivité de π. Pour l'implication réciproque, procédons par contraposée. Si (g_i) n'engendre pas G, considérons un sous-groupe maximal H de G contenant (le sous-groupe engendré par) la famille (g_i). Alors $\Phi(G) \subset H \subsetneq G$, donc $\pi(H) \subsetneq G/\Phi(G)$, et $(\pi(g_i))$ n'engendre pas $G/\Phi(G)$. □

Remarque 4. J'ai présenté ce développement lors de mon oral d'algèbre (leçon 108). Aucune question sur le développement n'a été posée. Note : 19/20.

10. Théorèmes de Chevalley-Warning et de Erdös-Ginzburg-Ziv

Référence M. Zavidovique, *Un max de maths.*

Leçons

- 120. Anneaux $\mathbf{Z}/n\mathbf{Z}$. Applications
- 121. Nombres premiers. Applications
- 123. Corps finis. Applications
- 126. Exemples d'équations diophantiennes
- 142. Algèbre des polynômes à plusieurs indéterminées. Applications

Théorème 1. *Soit q une puissance d'un nombre premier p. On se donne un entier $n \geqslant 1$ et des polynômes $P_1, \dots, P_r \in \mathbf{F}_q[X_1, \dots, X_n]$ tels que $\sum degP_i \leqslant n$. Alors, notant V l'ensemble des zéros (éléments de $\mathbf{F}_q^n$) communs à ces polynômes, on a*

$$|V| = 0 \mod p.$$

Démonstration. Considérons le polynôme

$$S = \prod_{i=1}^{r} (1 - P_i^{q-1}).$$

Sa fonction associée est l'indicatrice de V. Il s'agit donc d'établir que

$$\sum_{x \in \mathbf{F}_q^n} S(x) = 0.$$

Si $S = 0$, on a le résultat. Sinon soit $S_\alpha = c_\alpha X_1^{\alpha_1} \dots X_n^{\alpha_n}$ un de ses monômes. Vue la condition sur les degrés des polynômes P_i, le degré de S n'excède pas $(q-1)n$, et donc l'un des α_i n'excède pas $q-1$. Si $\alpha_i = 0$,

$$\sum_{x \in \mathbf{F}_q} x^{\alpha_i} = 0.$$

Sinon, soit g un générateur du groupe cyclique $\mathbf{F}_q^\times$: en particulier $g^{\alpha_i} \neq 1$. On a

$$\sum_{h \in \mathbf{F}_q^\times} h^{\alpha_i} = \sum_{h \in \mathbf{F}_q^\times} h^{\alpha_i} g^{\alpha_i} = g^{\alpha_i} \sum_{h \in \mathbf{F}_q^\times} h^{\alpha_i}.$$

Ainsi

$$\sum_{x \in \mathbf{F}_q} x^{\alpha_i} = \sum_{h \in \mathbf{F}_q^\times} h^{\alpha_i} = 0.$$

A fortiori $\sum_{x \in \mathbf{F}_q^n} S_\alpha(x) = 0$. Le théorème est démontré. □

Théorème 2. *Soit n un entier naturel non nul et $a_1, \dots, a_{2n-1}$ des entiers relatifs. Il existe une partie $I \subset [2n-1]$ à exactement n éléments telle que*

$$\sum_{i \in I} a_i = 0 \mod n.$$

Démonstration. Elle comporte deux étapes. D'abord on prouve le résultat pour les nombres premiers, puis on démontre qu'il est stable par produit. Soit p un nombre premier, et $a_1, \ldots, a_{2p-1}$ des entiers relatifs. Considérons les polynômes à $2n-1$ variables, et à coefficients dans $\mathbf{F}_p$ suivants

$$P = \sum_{i=1}^{2p-1} X_i^{p-1}, \qquad Q = \sum_{i=1}^{2p-1} a_i X_i^{p-1}.$$

Le théorème de Chevalley–Warning garantit que le nombre de zéros communs à ces deux polynômes est divisible par p. Comme $(0, \ldots, 0)$ en est un, on sait donc qu'il existe un zéro commun non trivial $x = (x_1, \ldots, x_{2p-1})$. Or grâce au petit théorème de Fermat,

$$P(x) = |\{i \,:\, x_i \neq 0\}|, \qquad Q(x) = \sum_{i=1}^{2p-1} a_i \mathbf{1}_{x_i \neq 0},$$

de sorte que $I = \{i \,:\, x_i \neq 0\}$ est de cardinal p et que

$$\sum_{i \in I} a_i = 0 \mod p.$$

Montrons maintenant que si n et m vérifient la propriété souhaitée, alors il en va de même de mn. Considérons des entiers relatifs $a_1, \ldots, a_{2mn-1}$. Le fait que la propriété soit vraie pour n garantit qu'il existe $I_1 \subset [2n-1] \subset [2nm-1]$ à exactement n éléments telle que $\sum_{i \in I_1} a_i = 0 \mod n$: disons

$$\sum_{i \in I_1} a_i = n b_1.$$

Puis il existe $I_2 \subset [2nm-1] \backslash I_1$ ayant aussi n éléments et telle que l'on puisse écrire

$$\sum_{i \in I_2} a_i = n b_2.$$

Ainsi de suite jusqu'à l'obtention d'une partie $I_{2m-1} \subset [2nm-1] \backslash (I_1 \cup \ldots \cup I_{2m-2})$. Soit alors un $J \subset [2m-1]$ ayant m éléments et telle que

$$\sum_{j \in J} b_j = 0 \mod m.$$

Finalement $K = \bigcup_{j \in J} I_j$ est une partie de $[2nm-1]$ à mn éléments et telle que

$$\sum_{i \in K} a_i = \sum_{j \in J} n b_j = 0 \mod nm.$$

□

11. Décomposition effective de Dunford

Référence J. Risler, P. Boyer, *Algèbre pour la licence 3 : groupes, anneaux, corps.*

Leçons

- 153. Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications
- 155. Endomorphismes diagonalisables en dimension finie
- 157. Endomorphismes trigonalisables. Endomorphismes nilpotents

Soit k un corps commutatif et E un $k-$ espace vectoriel de dimension $d \geqslant 1$.

Théorème 1. *Soit $u \in \mathcal{L}(E)$ dont le polynôme minimal est scindé. Il existe un unique couple $(d, \nu) \in \mathcal{L}(E)^2$, commutant entre eux, avec d diagonalisable et ν nilpotent. Ce sont des polynômes en u. Si Q est un polynôme scindé à racines simples tel que $Q(u)$ soit nilpotente alors la suite définie par $u_0 = u$, $u_{n+1} = u_n - Q(u_n)Q'(u_n)^{-1}$ est bien définie et stationne sur d.*

Remarque 2. SI k est de caractéristique nulle on peut prendre $Q = \frac{\chi_u}{\text{pgcd}(\chi_u, \chi_u')}$.

Lemme 3. *Pour tout n,*

- *u_n est bien définie ;*
- *c'est un polynôme en u ;*
- *$Q(u_n) \in \left(Q(u)^{2^n}\right)$;*
- *et $Q'(u_n)$ est inversible.*

Démonstration du lemme. Pour $n = 0$, $u_0 = u \in k[u]$, et $Q(u) \in \left(Q(u)^{2^0}\right)$. Et, puisque $\text{pgcd}(Q, Q') = 1$, une relation de Bezout donne

$$\text{Id} = AQ(u) + BQ'(u),$$

donc

$$BQ'(u) = \text{Id} - \underbrace{AQ(u)}_{\text{nilpotent}} \qquad \text{est inversible.}$$

Supposons la chose vraie au rang n. On a donc $Q'(u_n)^{-1} \in k[Q'(u_n)] \subset k[u]$. Aussi $u_{n+1} \in k[u]$ et est bien défini.
Par ailleurs une formule de Taylor donne

$$Q(u_{n+1}) = \underbrace{Q(u_n) + (u_{n+1} - u_n)Q'(u_n)}_{=0} + \underbrace{(u_{n+1} - u_n)}_{\in (Q(u)^{2^n})}{}^2 T(u_n, u_{n+1}) \in \left(Q(u)^{2^{n+1}}\right).$$

Enfin une autre formule de Taylor donne

$$Q'(u_{n+1}) - Q'(u_n) = (u_{n+1} - u_n)S(u_{n+1}, u_n) = \underbrace{Q(u_n)}_{\text{nilpotent}} Q'(u_n)^{-1} S(u_{n+1}, u_n) \qquad \text{nilpotent.}$$

Donc

$$Q'(u_{n+1}) = \underbrace{Q'(u_n)}_{\text{inversible}} + \underbrace{Q'(u_{n+1}) - Q'(u_n)}_{\text{nilpotent}}$$

est inversible. □

Démonstration du théorème. Soit (par hypothèse) n_0 tel que $Q(u)^{2^{n_0}} = 0$. Alors $Q(u_{n_0}) = 0$. Puisque Q est scindé à racines simples, $d = u_{n_0}$ est diagonalisable. Par ailleurs

$$\nu = u_0 - u_{n_0} = \sum_{j=0}^{n_0-1} u_{j+1} - u_j.$$

Les endomorphismes $u_{j+1} - u_j = Q(u_j)Q'(u_j)^{-1}$ sont nilpotents et commutent deux-à-deux donc ν est nilpotent.

Il reste à établir l'unicité de la décomposition. Soit $u = d' + \nu'$ une autre décomposition. Alors, puisque d', et ν' commutent, ils commutent avec u et avec ν et d qui sont des polynômes en u. Ainsi $\nu - \nu'$ est nilpotent et $d - d'$ diagonalisable. Comme $\nu - \nu' = -(d - d')$, c'est qu'ils sont nuls. □

12. Théorème de structure des groupes abéliens par la théorie des caractères

Référence G. Peyré et P. Colmez.

Leçons

- 102. Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications
- 104. Groupes finis. Exemples et applications
- 107. Représentations et caractères d'un groupe fini sur un $\mathbf{C}$-espace vectoriel
- 109. Représentations de groupes finis de petit cardinal
- 110. Caractères d'un groupe abélien fini et transformée de Fourier discrète. Applications
- 120. Anneaux $\mathbf{Z}/n\mathbf{Z}$. Applications

Soit G un groupe abélien fini, et n son ordre.

Théorème 1 (Lemme de prolongement)**.** *Si H est un sous-groupe de G, et χ un caractère de H, il existe un caractère de G prolongeant χ. En d'autres termes le morphisme de restriction*

$$\begin{array}{ccc} \hat{G} & \longrightarrow & \hat{H} \\ \chi & \longmapsto & \chi_{|H} \end{array}$$

est surjectif.

Démonstration. Procédons par récurrence forte sur l'indice $r = [G : H]$. Si $r = 1$, il n'y a rien à établir. Si $r > 1$. Soit χ un caractère de H, et $g \in G\backslash H$. On va prolonger χ sur $K = \langle H, g\rangle$. Comme $[G : K] < [G : H]$, on pourra conclure par récurrence. G/H est un groupe d'ordre r. Soit k l'ordre de gH dans ce groupe : k divise r d'après le théorème de Lagrange. En particulier $\chi(g^k)$ est bien défini. Considérons-en un racine k^e ω : $\chi(g^k) = \omega^k$. Posons, si $l \in \mathbf{Z}$, et $h \in H$, $\tilde{\chi}(g^l h) = \omega^l \chi(h)$, et vérifions que $\tilde{\chi} \in \hat{K}$.
$\tilde{\chi}$ est-il bien défini : si $g^l h = g^m t$, alors k divise $l - m$, et $g^{l-m} h = t$. Ainsi $\chi(g^{l-m})\chi(h) = \chi(t)$, donc $(\omega^k)^{(l-m)/k}\chi(h) = \chi(t)$, c'est-à-dire, $\omega^l \chi(h) = \omega^m \chi(t)$.
C'est un caractère :

$$\tilde{\chi}(g^l h g^m t) = \tilde{\chi}(g^{l+m} h t) = \omega^{l+m}\chi(h)\chi(t) = \omega^l \chi(h)\omega^m \chi(t) = \tilde{\chi}(g^l h)\tilde{\chi}(g^m t).$$

Ainsi $\tilde{\chi} \in \hat{K}$, et par hypothèse de récurrence, $\tilde{\chi}$ se prolonge en un caractère de G. □

Théorème 2 (Théorème de structure des groupes abéliens finis : existence)**.** *Il existe une suite $d_1 \mid \ldots \mid d_k$ tels que*

$$G \simeq \mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_k\mathbf{Z}.$$

Démonstration. Procédons par récurrence sur l'ordre de G. Soit x un élément de G d'ordre maximal d_k. On va établir que

$$G \simeq \langle x\rangle \times G/\langle x\rangle.$$

Puisque $\langle x\rangle$ est cyclique, son groupe dual lui est isomorphe, donc isomorphe à $\mathbf{U}_{d_k}$: soit χ un générateur de $\widehat{\langle x\rangle}$ et η sa réciproque, qui est un isomorphisme $\mathbf{U}_{d_k} \to \langle x\rangle$. Le lemme de prolongement qui précède fournit un caractère $\tilde{\chi}$ de G prolongeant χ. Puisque d_n est l'ordre maximal des éléments du groupe, l'ordre de tout autre élément divise d_n, et par conséquent $\tilde{\chi}$ prend ses valeurs dans $\mathbf{U}_{d_k}$. Montrons que

$$\begin{array}{ccc} G & \longrightarrow & \langle x\rangle \times G/\langle x\rangle \\ g & \longmapsto & (\eta \circ \tilde{\chi}(g), g\langle x\rangle) \end{array}$$

est un isomorphisme. Déjà il s'agit d'un morphisme de groupes de même cardinal. Vérifions qu'il est injectif : si $(\eta \circ \chi(g), g\langle x\rangle) = (1, \langle x\rangle)$, alors $g \in \langle x\rangle$, et $1 = \eta \circ \tilde{\chi}(g) = \eta \circ \chi(g) = g$, donc, puisque $\eta \circ \chi = Id_{\langle x\rangle}$, $g = 1$.

L'hypothèse de récurrence fournit $d_1 \mid \ldots \mid d_{k-1}$ et un isomorphisme

$$G/\langle x\rangle \simeq \mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_{k-1}\mathbf{Z}.$$

Par suite

$$G \simeq \mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_k\mathbf{Z}.$$

Mais ce dernier groupe a un élément d'ordre d_{k-1}. Comme d_k est l'ordre maximal des éléments de G, $d_{k-1} \mid d_k$. □

On a utilisé le lemme suivant

Lemme 3. *Soit G un groupe abélien, et d l'ordre maximal de ses éléments. L'ordre de tout élément divise d.*

Démonstration. On commence par montrer que si deux éléments sont d'ordre premiers entre eux, leur produit est d'ordre leur produit. Ensuite, si $x \in G$ est d'ordre d et si y est un élément d'ordre n ne divisant pas d, soit p premier tel que $v_p(n) > v_p(d)$. Alors $x^{p^{v_p(d)}}$ et $y^{n/p^{v_p(n)}}$ sont d'ordres respectifs $d/p^{v_p(d)}$ et $p^{v_p(n)}$. et leur produit d'ordre $dp^{v_p(n)-v_p(d)}$. L'ordre d de x n'est pas maximal. □

Démonstration de l'unicité. Supposons que

$$G_1 = \mathbf{Z}/\alpha_1\mathbf{Z} \times \cdots \times \mathbf{Z}/\alpha_k\mathbf{Z} \simeq \mathbf{Z}/\beta_1\mathbf{Z} \times \cdots \times \mathbf{Z}/\beta_l\mathbf{Z} = G_2.$$

Montrons par récurrence sur $k + l$ que $k = l$ et que $\alpha_i = \beta_i$. Supposons $k \geqslant l$. Pour tout entier q, l'équation $qx = 0$ admet $\operatorname{pgcd}(q, n_1) \times \ldots \times \operatorname{pgcd}(q, n_r)$ dans $\mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_r\mathbf{Z}$.
L'équation $\alpha_1 x$ a α_1^k solutions dans G_1 et, dans G_2, il y en a $\prod \operatorname{pgcd}(\alpha_1, \beta_j) \leqslant \alpha_1^l \leqslant \alpha_1^k$.
Nécessairement $k = l$ et pour tout j, on a $\operatorname{pgcd}(\alpha_1, \beta_j) = \alpha_1$ qui se récrit $\alpha_1 \mid \beta_j$. Et par symétrie (maintenant que $k = l$), $\beta_1 \mid \alpha_j$. En particulier $\beta_1 = \alpha_1$. Pour formaliser proprement la récurrence on écrit en supposant $\alpha_j = \beta_j$ pour $j < j_0$, que l'équation $\alpha_{j_0} x = 0$ a autant de solutions dans G_1 et dans G_2, et on conclut que $\alpha_{j_0} = \beta_{j_0}$. □

13. Un théorème de Kronecker

Référence A. Szpirglas *Algèbre L3*

Leçons

- 102. Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications
- 143. Résultant. Applications
- 144. Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications
- 190. Méthodes combinatoires, problèmes de dénombrement

Théorème 1. *Tout polynôme $P \in \mathbf{Z}[X]$ unitaire et dont les racines complexes sont toutes de module inférieur à 1 est produit d'une puissance de X et de polynômes cyclotomiques.*

Lemme 2. *L'ensemble $A_n = \{P \in Z[X] \text{de degré } n, \text{ unitaire : } V(P) \subset \bar{D}(0,1)\}$ est fini.*

Démonstration. Utilisons l'hypothèse sur les racines et les relations coefficients-racines pour borner les coefficients de ces polynômes. Si $P = \prod_{i=1}^{n}(X - \zeta_i) = X^n + p_1 X^{n-1} + \dots p_n \in A_n$,

$$p_k = (-1)^k \Sigma_k(\zeta_1, \dots, \zeta_n) = (-1)^k \sum_{i_1 < \dots < i_k} \zeta_{i_1} \dots \zeta_{i_k},$$

donc

$$|p_k| \leqslant \sum_{i_1 < \dots < i_k} 1 = \binom{n}{k}.$$

Ainsi les coefficients de P (qui sont en outre entiers) ne peuvent prendre qu'un nombre fini de valeurs. □

Lemme 3. *Si $P = \prod_{i=1}^{n}(X - \zeta_i) \in A_n$ alors pour tout $k \geqslant 0$, $P_k = \prod_{i=1}^{n}(X - \zeta_i^k) \in A_n$.*

Démonstration. P_k est unitaire, de degré n, et de racines dans $\bar{D}(0,1)$. La difficulté est de démontrer qu'il est à coefficients entiers. Développons-le :

$$P_k = X^n + \sum_{j=1}^{n} (-1)^j \Sigma_j(\zeta_1^k, \dots, \zeta_n^k) X^{n-j}.$$

Soit $S_j = \Sigma_j(X_1^k, \dots, X_n^k) \in \mathbf{Z}[X_1, \dots, X_n]^{\mathfrak{S}_n}$. Le théorème de structure des polynômes symétriques fournit un polynôme $Q_j \in \mathbf{Z}[Z_1, \dots, Z_n]$ tel que $S_j = Q_j(\Sigma_1, \dots, \Sigma_n)$. Ainsi

$$\Sigma_j(\zeta_1^k, \dots, \zeta_n^k) = S_j(\zeta_1, \dots, \zeta_n) = Q_j(\underbrace{\Sigma_1(\zeta_1, \dots, \zeta_n)}_{=-p_1 \in \mathbf{Z}}, \dots, \underbrace{\Sigma_n(\zeta_1, \dots, \zeta_n)}_{=(-1)^n p_n \in \mathbf{Z}}) \in \mathbf{Z}.$$

Pour la leçon 143, on utilisera la démonstration alternative suivante : Soit $Q(Y) = Y^k - X$.

$$\mathrm{Res}_Y(Q(Y), P(Y)) = \prod\prod (\lambda_i^k - X) \in \mathbf{Z}[X].$$

□

Démonstration du théorème de Kronecker. Les deux précédents lemmes assurent que

$$\{P_k \,:\, k \geqslant 0\} \text{ est fini.}$$

Aussi l'ensemble de leur racines

$$\{\zeta_j^k \,:\, k \geqslant 0,\, j \in \{1, \dots n\}\} \text{ est fini.}$$

Donc pour tout $j \in \{1, \dots n\}$,

$$\{\zeta_j^k \,:\, k \geqslant 0, \} \text{ est fini,}$$

c'est-à-dire que ζ_j est soit nul soit une racine de l'unité. Écrivons donc

$$P = X^{n-r} \prod_{j=1}^{r} (X - \zeta_j),$$

où ζ_j une racine primitive $n(j)^e$ de l'unité. Ainsi P divise $X^{n-r} \prod_{j=1}^{r} \phi_{n_j}$, a priori dans $\mathbf{C}[X]$, mais puisque ce sont tous des polynômes de $\mathbf{Z}[X]$ dans $\mathbf{Q}[X]$, et puisque les ϕ_{n_j} (et X) sont irréductibles sur $\mathbf{Q}[X]$, qui est principal (a fortiori factoriel), on a le résultat. □

Corollaire 4. *Soit $B \in \mathbf{M}_n(\mathbf{Z})$, et $k \in \mathbf{N}\backslash\{0, 1\}$ tel que $I_n + kB$ soit d'ordre fini m. Si $k \geqslant 3$, alors B est nulle. Si $k = 2$, soit $B = 0$, soit $m = 2$.*

Démonstration. La matrice $I_n + kB$ est diagonalisable, et ses valeurs propres sont dans $\mathbf{U}_m$, donc $B = \frac{1}{k}((I_n + kB) - I_n$ est diagonalisable de valeurs propres

$$\left\{ \frac{\zeta - 1}{k} \,:\, \zeta \in \mathrm{Sp}(I_n + kB) \subset \mathbf{U}_m \right\}.$$

Elles sont donc toutes de modules inférieur à 1. Et ce sont les racines de $\chi_B \in \mathbf{M}_n(\mathbf{Z})$. Le théorème de Kronecker affirme qu'elles sont soit nulles, soit sont des racines de l'unité.
Si $k \geqslant 3$, alors $|\frac{\zeta-1}{k}| < 1$, donc les valeurs propres de B sont nulles, et puisque B est diagonalisable, B est nulle.
Si $k = 2$, alors pour toute valeur propre ζ de $(I_n + kB)$ d'une part $|\frac{\zeta-1}{2}| \in \{0, 1\}$, et d'autre part $\zeta \in \mathbf{U}_m$. Nécessairement $\zeta \in \{-1, 1\}$. Ainsi $(I_n + kB)$ est d'ordre 1 (et $B = 0$) ou d'ordre 2. □

14. Exponentielle d'une somme et application

Référence Aucune.

Leçons

— 156. Exponentielle de matrices. Applications

— 157. Endomorphismes trigonalisables. Endomorphismes nilpotents

Proposition 1. *Si $A, B \in \mathbf{M}_n(\mathbf{C})$ et si $[A,[A,B]] = 0$ alors*

$$e^A B e^{-A} = B + [A,B]$$

Démonstration. Si $t \in \mathbf{R}$,

$$\begin{aligned}\frac{\mathrm{d}}{\mathrm{d}t}\left[e^{tA}Be^{-tA}\right] &= e^{tA}(AB-BA)e^{-tA} \\ &= [A,B]e^{tA}e^{-tA} \qquad \text{car } A \text{ commute avec } [A,B].\end{aligned}$$

En intégrant on a donc pour tout $t \in \mathbf{R}$,

$$e^{tA}Be^{-tA} = B + t[A,B].$$

□

Proposition 2. *Si A et B sont des éléments de $\mathbf{M}_n(\mathbf{C})$ commutant toutes deux avec $N = [A,B]$, alors pour tout $t \in \mathbf{C}$,*

$$e^{t(A+B)} = e^{tA}e^{-t^2N/2}e^{tB}.$$

Démonstration. Si $t \in \mathbf{R}$ (ou $\mathbf{C}$),

$$\begin{aligned}\frac{\mathrm{d}}{\mathrm{d}t}\left[e^{tA}e^{-t^2N/2}e^{tB}\right] &= e^{tA}Ae^{-t^2N/2}e^{tB} + e^{tA}e^{-t^2N/2}(-tN)e^{tB} + e^{tA}e^{-t^2N/2}Be^{tB} \\ &= e^{tA}e^{-t^2N/2}(A+B-tN)e^{tB} \qquad \text{vues les hypothèses de commutativité.}\end{aligned}$$

Le lemme 5 donne

$$e^{tA}B = (B+tN)e^{tA}.$$

Donc l'égalité précédente devient

$$\begin{aligned}\frac{\mathrm{d}}{\mathrm{d}t}\left[e^{tA}e^{-t^2N/2}e^{tB}\right] &= (A - tN + B + tN)e^{tA}e^{-t^2N/2}e^{tB} \\ &= (A+B)\left[e^{tA}e^{-t^2N/2}e^{tB}\right],\end{aligned}$$

soit une relation du type

$$\frac{\mathrm{d}}{\mathrm{d}t}\phi(t) = (A+B)\phi(t).$$

Finalement

$$\phi(t) = e^{tA}e^{-t^2N/2}e^{tB} = e^{t(A+B)}.$$

□

Proposition 3. *Soient A, B des éléments de $\mathbf{M}_n(\mathbf{C})$ tels que $N = [A,B]$ commute avec A et B. La matrice N est nilpotente et A et B sont cotriangulables.*

Démonstration. Le lemme 6 se récrit : pour tout $t \in \mathbf{C}$

$$e^{t^2 N/2} = e^{tA} e^{-t(A+B)} e^{tB}$$

Si λ est une valeur propre (complexe) non nulle de N, et v un vecteur propre associé. Soit μ une racine carré de $1/\lambda$ et $t(x) = \sqrt{2}\mu x$ ($x \in \mathbf{R}$). On a

$$e^{t(x)^2 N/2} v = e^{t(x)^2 \lambda/2} = e^{x^2},$$

tandis que

$$e^{t(x)A} e^{-t(x)(A+B)} e^{t(x)B} v = O_{x\to\infty}\left(e^{x(\|A\|+\|B\|+\|A+B\|)}\right).$$

C'est une contradiction. On a montré que N est nilpotente.
Établissons maintenant par récurrence (forte) sur n que A et B sont cotriangulables. Si $N = 0$, A et B commutent donc sont cotriangulables. Sinon, considérons $F = \ker N$ qui est un sous-espce de dimension comprise entre 1 et $n-1$, et stable par A et B car elles commutent à N. Dans une base adaptée à l'inclusion $\ker N \subset \mathbf{R}^n$, les matrices A, B et N s'écrivent respectivement

$$A = \begin{pmatrix} A' & * \\ 0 & A'' \end{pmatrix}, \qquad B = \begin{pmatrix} B' & * \\ 0 & B'' \end{pmatrix}, \qquad N = \begin{pmatrix} N' & * \\ 0 & N'' \end{pmatrix}.$$

Le fait que A et B commutent avec N entraîne (par un simple calcul des produits par blocs) que A' et B' commutent avec N' d'une part (en fait $N' = 0$), A'' et B'' commutent avec N'' d'autre part. L'hypothèse de récurrence assure donc que A' et B' sont cotriangulables ; A'' et B'' aussi. □

Remarque 4. Il convient de savoir que l'on peut établir plus simplement ce dernier résultat : en particulier sans utiliser les deux premiers. On commence par constater que N ne peut être inversible : sinon on aurait $N^{-1}AB - N^{-1}BA = I_n$, soit $N^{-1}AB - BN^{-1}A = I_n$ vu que N et B commutent. En prenant la trace, on obtiendrait une contradiction. Considérant alors le sous-espace $V = \ker N$ stable par A et B et sur lequel les endomorphismes induits par A et B commutent, on obtient l'existence d'un vecteur propre commun à A, B et N. On conclut par récurrence.

15. Théorème de Gauss–Wantzel

Référence J.-C. Carrega, *Théorie des corps : la règle et le compas.*

Leçons

- 102. Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications
- 125. Extensions de corps. Exemples et applications
- 141. Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications
- 182. Applications des nombres complexes à la géométrie
- 183. Utilisation des groupes en géométrie

Théorème 1 (Gauss-Wantzel)**.** *Le nombre $e^{2\,\mathrm{i}\,\pi/n}$ est constructible à la règle et au compas si et seulement si n est le produit d'une puissance de deux et de nombres premiers de Fermat distincts.*

Démonstration. 1. Si n et m sont premiers entre eux, $e^{2\,\mathrm{i}\,\pi/(nm)}$ est constructible si et seulement si $e^{2\,\mathrm{i}\,\pi/n}$ et $e^{2\,\mathrm{i}\,\pi/m}$ le sont. Cela découle d'une identité de Bézout.

2. Les $e^{2\,\mathrm{i}\,\pi/2^\alpha}$ sont constructibles car on peut tracer des bissectrices.

2. Si $e^{2\,\mathrm{i}\,\pi/p^\alpha}$ est constructible avec p un nombre premier impair, et $\alpha \geqslant 1$ alors p est un nombre de Fermat et $\alpha = 1$. En effet, le polynôme cyclotomique Φ_{p^α} annule $e^{2\,\mathrm{i}\,\pi/p^\alpha}$, et il est irréductible sur $\mathbf{Q}$. C'est donc son polynôme minimal. Le degré de l'extension $\mathbf{Q}(e^{2\,\mathrm{i}\,\pi/p^\alpha})/\mathbf{Q}$ est donc

$$[\mathbf{Q}(e^{2\,\mathrm{i}\,\pi/p^\alpha}) : \mathbf{Q}] = \deg \Phi_{p^\alpha} = \phi(p^\alpha) = p^{\alpha-1}(p-1).$$

D'après le théorème de Wantzel, ce doit être une puissance de 2. Nécessairement $\alpha = 1$ et $p-1$ est une puissance de 2.

3. Si $p = 2^{2^k}+1$ est premier alors $\omega = e^{2\,\mathrm{i}\,\pi/p}$ est constructible. Considérons le groupe G des automorphismes de corps sur $\mathbf{Q}[\omega]$. Puisque $\Phi_p \in \mathbf{Z}[X]$, tout élément $\sigma \in G$ permute les racines de Φ_p. Or celles-ci sont les ω^j, pour $1 \leqslant j \leqslant p-1$. Notant $\psi(\sigma)$ l'unique élément de $[1, p-1]$ tel que $\sigma(\omega) = \omega^{\psi(\sigma)}$, on a un morphisme surjectif

$$G \longrightarrow (\mathbf{Z}/p\mathbf{Z})^\times.$$

Un élément de $\sigma \in G$ est entièrement déterminé par l'image $\sigma(\omega)$. Ainsi le morphisme précédent est un isomorphisme. Le groupe G est donc cyclique d'ordre $p-1 = 2^{2^k}$. Soit σ un générateur de G, et

$$L_j = \{z \in \mathbf{Q}[\omega] \ : \ \sigma^{2^j}(z) = z\}.$$

On a une suite d'extension de corps

$$\mathbf{Q} \subset L_0 \subset L_1 \subset \ldots \subset L_k = \mathbf{Q}[\omega].$$

Pour conclure, il suffit d'établir que chaque extension est de degré 2, il suffit en fait par double encadrement de montrer que pour tout $j \geqslant 1$, $L_{j-1} \neq L_j$. Pour cela on exhibe un élément dans $L_j \backslash L_{j-1}$. Posons

$$x = \sum_{m=0}^{2^{k-j}-1} \sigma^{2^j m}(\omega).$$

C'est évidemment un élément de L_j, puisque $\sigma^{2^k} = \mathrm{Id}$. Si c'était un élément de L_{j-1} on aurait une relation de dépendance $\mathbf{Q}$-linéaire entre les $\sigma^j(\omega), 0 \leqslant j \leqslant p-1$, c'est-à-dire entre les racines $(\omega, \omega^2, \ldots, \omega^{p-1})$ de Φ_p :

$$\sigma^{2^{j-1}}(x) = x.$$

Dans le membre de gauche le coefficient de ω est nul, tandis que dans le membre de droite il vaut 1. C'est absurde car $(\omega, \omega^2, \ldots, \omega^{p-1})$ est une base de $\mathbf{Q}[\omega]$ (le polynôme Φ_p est irréductible). □

Proposition 2. *Soit n un entier. Si $p = 2^n + 1$ est un nombre premier alors n est uns puissance de 2.*

Démonstration. Si $n = 2^j\alpha$, avec α impair, alors, puisque le polynôme $X + 1$ divise $X^\alpha + 1$ (ils sont unitaires et ont une racine en commun), $2^{2^j} + 1$ divise $2^{2^j\alpha} + 1$. □

Deuxième démonstration. Si $n = l \times n/l$, $(2^{n/l})^l = -1$ dans $\mathbf{Z}/p\mathbf{Z}$. donc $2^{n/l}$ est d'ordre divisant $2l$. Mais si $1 \leqslant j \leqslant l$, $3 \leqslant 2^{jn/l} < 2^n + 1 = p$, donc cet ordre excède strictement l, c'est donc $2l$. Ainsi $2l$ divise l'ordre de $\mathbf{Z}/p\mathbf{Z}$, à savoir $p - 1 = 2^n$. Nécessairement l est une puissance de 2. □

16. Théorème de Carathéodory et équations diophantiennes

Référence A. Pommelet, *Analyse pour l'agrégation* pour le théorème de Carathéodory, aucune pour l'application (d'après un document de Claudine Picaronny).

Leçons

- 126. Exemples d'équations diophantiennes
- 151. Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications
- 181. Barycentres dans un espace affine réel de dimension finie, convexité. Applications

Théorème 1 (Carathéodory)**.** *Soit A une partie non vide d'un espace vectoriel réel E de dimension n. Son enveloppe convexe est*

$$\left\{ \sum_{i=1}^{n+1} \lambda_i a_i \ : \ \lambda_i \geqslant 0, \sum \lambda_i = 1, a_i \in A \right\}.$$

Démonstration. Soit $x = \sum_{i=1}^{p} \lambda_i a_i$ dans l'enveloppe convexe de A, avec p minimal. Par l'absurde, supposons $p \geqslant n+2$. Considérons l'application linéaire

$$\phi : \left| \begin{array}{ccc} \mathbf{R}^p & \longrightarrow & E \times \mathbf{R} \\ (\alpha_i) & \longmapsto & (\sum \alpha_i a_i, \sum \alpha_i) \end{array} \right. .$$

Le théorème du rang donne

$$\dim \ker \phi = p - \dim \operatorname{Im} \phi \geqslant p - (n+1) \geqslant 1.$$

Soit donc $(\alpha_1, \ldots, \alpha_p)$ un élément non nul du noyau de ϕ. Considérons l'ensemble

$$F = \{t \in \mathbf{R} \ : \ \forall i, \ \lambda_i + t\alpha_i \geqslant 0\}.$$

Déjà $0 \in F$. Comme intersection d'intervalles fermés, F est un intervalle fermé. Puisqu'il existe i, j tels que $\alpha_i > 0$ et $\alpha_j > 0$, F est borné. Considérons sa borne inférieure τ. Il existe j tel que si $t < \tau_1$, $\lambda_j + t\alpha_j < 0$. Ainsi par continuité, $\lambda_j + \tau\alpha_j = 0$. Posons $\mu_i = \lambda_i + \tau\alpha_i \geqslant 0$ ($\tau \in F$). On a, puisque $(\alpha_i) \in \ker \phi$, $\sum \mu_i = 1$, et $x = \sum \mu_i a_i = \sum_{i \neq j} \mu_i a_i$. Ceci contredit la minimalité de p. □

Théorème 2. *Soit $m, n \geqslant 1$, et $A \in \mathcal{M}_{m,n}(\mathbf{Z})$. Le système diophantien $Ax = 0$ admet une solution non nulle dans $\mathbf{N}^n$ si et seulement si $0_{\mathbf{R}^n}$ est dans l'enveloppe convexe des colonnes de A.*

Démonstration. L'implication directe est évidente. Pour la réciproque soit l minimal tel que 0 soit dans l'enveloppe convexe de l colonnes $A_{i_1}, \ldots, A_{i_l}$ de A. Soit r le rang de la matrice $(A_{i_1}, \ldots, A_{i_l})$. Montrons dans un premier temps que $l = r+1$. Le théorème de Carathéodory donne déjà que $l \leqslant r+1$. Mais d'autre part $r < l$ car l'écriture $0 \in \operatorname{Conv}(A_{i_1}, \ldots, A_{i_l})$ donne un relation de dépendance linéaire entre ces l colonnes. L'algorithme du pivot de Gauss fournit une matrice $P \in \mathrm{GL}_m(\mathbf{Z})$ telle que

$$P(A_{i_1}, \ldots, A_{i_{r+1}}) = \begin{pmatrix} M \\ 0 \end{pmatrix},$$

avec $M \in \mathcal{M}_{r,r+1}(\mathbf{Z})$ de rang r. Ainsi M a un noyau de dimension 1 sur $\mathbf{Q}$ (ou $\mathbf{R}$). Et puisque $0 \in \operatorname{Conv}(A_{i_1}, \ldots, A_{i_l})$, on peut choisir un vecteur directeur $y \in \mathbf{Q}^{r+1}$ de ce noyau à coefficients positifs, et quitte à le multiplier par un entier, on peut le supposer à coordonnées entières. Il satisfait $My = 0$. On le complète par des zéros (pour $j \notin \{i_1, \ldots i_l\}$). □

Une autre démonstration. Soit $y \in \mathbf{R}^n$ à coordonnées positives tel que $Ay = 0$, et J l'ensemble des indices de ses coordonnées nulles. Considérons le $\mathbf{Q}$-espace vectoriel

$$V = \{x \in \mathbf{Q}^n \,:\, Ax = 0, x_j = 0 \text{ pour } j \in J\},$$

d sa dimension, et $e_1, \ldots, e_d$ une $\mathbf{Q}$-base de V. Par invariance du rang par changement de corps, c'est aussi la dimension sur $\mathbf{R}$ de

$$W = \{x \in \mathbf{R}^n \,:\, Ax = 0, x_j = 0 \text{ pour } j \in J\} = \mathrm{Vect}_{\mathbf{R}}(e_1, \ldots, e_d).$$

Ainsi V est dense dans W. Or $y \in W$. Soit $x \in V$, suffisamment proche de y pour que pour tout $j \notin J$, $x_j > 0$. Le vecteur non nul $x \in \mathbf{Q}^n$ est donc à coordonnées positives, et satisfait $Ax = 0$. Un de ses multiples est à coordonnées entières positives et non nul, et satisfait toujours $Ax = 0$. □

17. Théorème de Frobenius–Zolotarev

Référence V. Beck, J. Malick, G. Peyré, *Objectif Agrégation.*

Leçons

- 106. Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $\mathrm{GL}(E)$. Applications
- 120. Anneaux $\mathbf{Z}/n\mathbf{Z}$. Applications
- 121. Nombres premiers. Applications
- 152. Déterminant. Exemples et applications

Théorème 1. *Soit p un nombre premier impair, et $u \in \mathrm{GL}_n(\mathbf{F}_p)$, que l'on identifie à un élément de $\mathfrak{S}(\mathbf{F}_p^n)$. Sa signature est $\epsilon(u) = \left(\frac{\det(u)}{p}\right)$.*

Lemme 2. *Le symbole de Legendre $\left(\frac{\cdot}{p}\right)$ est l'unique morphisme non trivial $\mathbf{F}_p^\times \to \{-1, 1\}$.*

Démonstration. Le groupe $\mathbf{F}_p^\times$ est cyclique, il y a donc au plus deux tels morphismes. Le symbole de Legendre est non trivial car le morphisme

$$\left.\begin{array}{rcl} \mathbf{F}_p^\times & \longrightarrow & \mathbf{F}_p^\times \\ x & \longmapsto & x^2 \end{array}\right| :$$

est non injectif (p impair) donc non surjectif. □

Lemme 3. *Soit G un groupe abélien et $\phi : \mathrm{GL}_n(\mathbf{F}_p) \to G$ un homomorphisme de groupes. Il se factorise par le déterminant : il existe un morphisme $\delta : \mathbf{F}_p^\times \to G$ tel que $\phi = \delta \circ \det$.*

Démonstration. Puisque G est abélien, $D(\mathrm{GL}_n(\mathbf{F}_p)) < \ker \phi$. Or $D(\mathrm{GL}_n(\mathbf{F}_p)) = \mathrm{SL}_n(\mathbf{F}_p) = \ker \det$. Ainsi $\ker \det < \ker \phi$. Il existe une factorisation $\phi = \overline{\phi} \circ \det$ avec $\overline{\phi} : \mathrm{GL}_n(\mathbf{F}_p)/\mathrm{SL}_n(\mathbf{F}_p) \to G$. Mais aussi une factorisation $\overline{\det} : \mathrm{GL}_n(\mathbf{F}_p)/\mathrm{SL}_n(\mathbf{F}_p) \to \mathbf{F}_p^\times$, qui est un isomorphisme (injectif par construction et surjectif car le déterminant l'est). On conclut en posant $\delta = \overline{\phi} \circ \overline{\det}^{-1}$. □

Démonstration du théorème. Le morphisme signature satisfait aux hypothèses du seconde lemme, donc il existe un morphisme $\delta : \mathbf{F}_p^\times \to \{-1, 1\}$ tel que $\epsilon = \delta \circ \det$. Le premier lemme conclura pourvu qu'on montre que δ est non trivial, c'est-à-dire que $\epsilon : \mathrm{GL}_n(\mathbf{F}_p) \to \{-1, 1\}$ est non trivial. À cette fin constatons que le corps $\mathbf{F}_{p^n}$ a une structure de $\mathbf{F}_p$-espace vectoriel de dimension n. Donnons-nous un générateur g du groupe cyclique $\mathbf{F}_{p^n}^\times$ et considérons l'endomorphisme $x \mapsto gx$ du $\mathbf{F}_p$-espace vectoriel $\mathbf{F}_{p^n}$. La permutation associée est un $p^n - 1$-cycle, qui a donc pour signature $(-1)^{p^n-2} = -1$. Aussi le morphisme ϕ prend-il la valeur -1 pour toute matrice de cet endomorphisme. □

Remarque 4. On a utilisé le fait que $D(\mathrm{GL}_n(\mathbf{F}_p)) = \mathrm{SL}_n(\mathbf{F}_p)$. Ceci découle de ce que les transvections (c'est-à-dire les endomorphismes $u \neq \mathrm{Id}$ tels que $(u-1)^2 = 0$) engendrent $\mathrm{SL}_n(\mathbf{F}_p)$, et que deux transvections sont toujours conjuguées. De ce fait, si u est une transvection, u^2 aussi (...) donc $u^2 = vuv^{-1}$, donc $u = u^{-1}vuv^{-1}$ est un commutateur.

Application : Calcul de la signature de l'automorphisme de Frobenius Soit p un nombre premier impair et $n \geqslant 1$.

18. Étude topologique de $O(p,q)$

Référence P. Caldero, J. Germoni, *Histoires hédonistes de groupes et de géométries.*

Leçons

- 156. Exponentielle de matrices. Applications
- 158. Matrices symétriques réelles, matrices hermitiennes
- 171. Formes quadratiques réelles. Exemples et applications

On admettra les deux faits suivants.

Théorème 1. *La décomposition polaire*

$$\begin{array}{rcl} O(n)\times \mathrm{S}_n^{++}(\mathbf{R}) & \longrightarrow & \mathrm{GL}_n(\mathbf{R}) \\ (O,S) & \longmapsto & OS \end{array}$$

est un homéomorphisme.

Théorème 2. *L'exponentielle réalise un homéomorphisme* $\exp : \mathrm{S}_n(\mathbf{R}) \to \mathrm{S}_n^{++}(\mathbf{R})$.

On veut démontrer le théorème d'isomorphisme suivant.

Théorème 3. *On a un homéomorphisme*

$$O(p,q) \simeq O(p)\times O(q)\times \mathbf{R}^{pq}.$$

Démonstration. On notera $n=p+q$. Soit $M\in O(p,q)$, et $M=OS$ sa décomposition polaire. Montrons que O et S sont des éléments de $O(p,q)$. Déjà $O(p,q)$ est un groupe stable par transposée (...), donc $S^2 = M^\top M \in O(p,q)$.

Lemme 4. *Soit* $U\in \mathrm{S}_n(\mathbf{R})$. *On a l'équivalence*

$$\exp(U)\in O(p,q) \iff I_{p,q}U + U^\top I_{p,q} = 0.$$

Démonstration. On a les équivalences suivantes

$$\begin{aligned} \exp(U)\in O(p,q) &\iff \exp(U^\top) I_{p,q}\exp(U) = I_{p,q} \\ &\iff \exp(U) = I_{p,q}^{-1}\exp(-U^\top) I_{p,q} = \exp(-I_{p,q}^{-1}U^\top I_{p,q}) \\ &\iff U = -I_{p,q}^{-1}U^\top I_{p,q} \end{aligned}$$

vue la bijection fournie par le théorème 2. □

Pour ce qui nous intéresse, si $S=\exp(U)$, $S^2=\exp(2U)\in O(p,q)$ donc $I_{p,q}U+U^\top I_{p,q}=0$ puis $S=\exp(U)\in O(p,q)$. D'autre part $O=MS^{-1}\in O(p,q)$. La décomposition polaire induit donc un homéomorphisme

$$O(p,q)\simeq (O(n)\cap O(p,q))\times (\mathrm{S}_n^{++}(\mathbf{R})\cap O(p,q)).$$

Étudions $O(n)\cap O(p,q)$. Soit

$$M=\begin{pmatrix} A & B \\ C & D\end{pmatrix} \in O(n)\cap O(p,q).$$

Ces deux conditions donnent (entre autre) la conjonction des relations

$$\begin{cases} AA^\top + BB^\top = I_p \\ AA^\top - BB^\top = I_p \\ CC^\top + DD^\top = I_q \\ CC^\top - DD^\top = -I_q \end{cases}, \qquad \text{soit} \qquad \begin{cases} AA^\top = I_p \\ BB^\top = 0 \\ DD^\top = I_q \\ CC^\top 0 \end{cases},$$

donc $A \in O(p)$, $D \in O(q)$, $D = 0$ et $C = 0$.

Étudions enfin $\mathrm{S}_n^{++}(\mathbf{R}) \cap O(p,q)$. Considérons l'ensemble $L = \{U \in \mathcal{M}_n(\mathbf{R}) \,:\, I_{p,q}U + U^\top I_{p,q} = 0\}$. On a vu que l'exponentielle réalise une bijection entre $L \cap \mathrm{S}_n(\mathbf{R})$ et $\mathrm{S}_n^{++}(\mathbf{R}) \cap O(p,q)$. Puisque, $\exp : \mathrm{S}_n(\mathbf{R}) \to \mathrm{S}_n^{++}(\mathbf{R})$ est un homéomorphisme, elle réalise par restriction un homéomorphisme $L \cap \mathrm{S}_n(\mathbf{R}) \to \mathrm{S}_n^{++}(\mathbf{R}) \cap O(p,q)$. Constatons pour finir que

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in L \cap \mathrm{S}_n(\mathbf{R})$$

si et seulement si $A = D = 0$ et $B = C^\top$. Ainsi

$$L \cap \mathrm{S}_n(\mathbf{R}) = \left\{ \begin{pmatrix} 0 & B \\ B^\top & 0 \end{pmatrix} \,:\, B \in \mathcal{M}_{p,q}(\mathbf{R}) \right\}.$$

□

Remarque 5. La démonstration donne explicitement l'homéomorphisme en question : c'est

$$\begin{array}{rcl} O(p) \times O(q) \times \mathcal{M}_{p,q}(\mathbf{R}) & \longrightarrow & O(p,q) \\ (U,V,B) & \longmapsto & \begin{pmatrix} U & 0 \\ 0 & V \end{pmatrix} \exp\left(\begin{pmatrix} 0 & B \\ B^\top & 0 \end{pmatrix} \right) . \end{array}$$

Corollaire 6. *Si $p = 0$ ou $q = 0$, $O(p,q)$ est compact et a deux composantes connexes. Sinon il n'est pas compact et a quatre composantes connexes.*

Corollaire 7. *Si ni p ni q n'est nul, la composante connexe de l'identité dans $O(p,q)$ est*

$$\mathrm{SO}_0(\mathbf{R}) = \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{SO}(p,q) \,:\, A \in \mathrm{GL}_p(\mathbf{R})^+ \right\}.$$

19. Invariants de Smith

Référence D. Serre, *Matrices.*

Leçons

- 122. Anneaux principaux. Applications
- 126. Exemples d'équations diophantiennes
- 150. Exemples d'actions de groupes sur les espaces de matrices
- 162. Systèmes d'équations linéaires ; opérations, aspects algorithmiques et conséquences théoriques

Soit A un anneau principal, $n, m \geqslant 1$, et $M \in \mathcal{M}_{m,n}(A)$.

Théorème 1. *Il existe un unique $r \geqslant 0$ et une suite $a_1 | \cdots | a_r$, unique à association près, ainsi que des matrices $P \in \mathrm{GL}_m(A)$, $Q \in \mathrm{GL}_n(A)$ tels que*

$$PMQ = \begin{pmatrix} a_1 & & & & & 0 & \cdots & 0 \\ & \ddots & & & & \vdots & & \vdots \\ & & a_r & & & \vdots & & \vdots \\ & & & 0 & & \vdots & & \vdots \\ & & & & \ddots & \vdots & & \vdots \\ & & & & & 0 & \cdots & 0 \end{pmatrix}$$

Algorithme L'algorithme qui suit permet de construire une matrice équivalente à M de la forme

$$\begin{pmatrix} a & \\ & M' \end{pmatrix},$$

où a divise tous les éléments de M'. Il suffira alors d'itérer l'algorithme.

1. Si $m_{1,1}$ ne divise pas tous les éléments de la première ligne, soit $j \in [2, n]$ minimal tel que $m_{1,1} \nmid m_{1,j}$. Notons δ leur pgcd, et donnons-nous une relation de Bezout $m_{1,1}u + m_{1,j}v = \delta$ entre eux. Posons $w = -m_{1,j}/d$, $z = m_{1,1}/d$. La multiplication à droite par la matrice

$$\begin{pmatrix} u & & \cdots & & w & & & \\ & 1 & & & & & & \\ \vdots & & \ddots & & \vdots & & & \\ & & & 1 & & & & \\ v & & \cdots & & z & & & \\ & & & & & 1 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{pmatrix},$$

   qui est inversible car de déterminant 1, donne une matrice ayant pour premier coefficient δ. On recommence l'étape 1.

2. Si $m_{1,1}$ divise tous les éléments de la première ligne, mais ne divise pas tous les éléments de la première colonne, soit $j \in [2, n]$ minimal tel que $m_{1,1} \nmid m_{j,1}$. On applique la même méthode qu'à l'étape 1. Puis on revient à l'étape 1.

3. Si $m_{1,1}$ divise tous les éléments de la première ligne et de la première colonne, on effectue les opérations élémentaires
$$C_i \longleftarrow C_i - \frac{m_{1,i}}{m_{1,1}} C_1 \qquad \text{pour } i \geqslant 2,$$
et
$$L_j \longleftarrow L_j - \frac{m_{j,1}}{m_{1,1}} L_1 \qquad \text{pour } j \geqslant 2.$$
On dispose d'une matrice de la forme
$$\begin{pmatrix} a & \\ & M' \end{pmatrix},$$
mais où a priori $m_{1,1}$ ne divise pas tous les éléments de M'.
4. Si $m_{1,1}$ ne divise pas tous les éléments de M'. Soit $i, j \in [2, n]$ tels que $m_{1,1} \nmid m_{i,j}$. On effectue l'opération élémentaire
$$L_1 \longleftarrow L_1 + L_i.$$
Puis on retourne à l'étape 1.
5. Si $m_{1,1}$ divise tous les éléments de M', on a terminé.

Démonstration de la terminaison de l'algorithme. Soit (M_p) la suite de matrices ainsi formée, et $a_p = (M_p)_{1,1}$ leur premier coefficient. Par construction la suite des idéaux (a_p) est croissante.

Lemme 2. *Une suite croissante d'idéaux de A est stationnaire.*

Démonstration. Soit $I_1 \subset I_2 \subset \dots$ une telle suite. On vérifie que leur réunion $I = \bigcup_{n \geqslant 1} I_n$ est un idéal, principal puisque A est principal. Soit $a \in A$ tel que $I = (a)$, puis $N \geqslant 1$ tel que $a \in I_N$. Si $n \geqslant N$, on a $(a) \subset I_N \subset I_n \subset I = (a)$, d'où $I_N = I_n$. □

Ainsi la suite d'idéaux (a_p) stationne disons à partir du rang P. À l'étape suivante, nécessairement, on n'est ni dans le cas 1, ni dans le cas 2, qui vont croître strictement l'idéal engendré par le premier coefficient. Pour les mêmes raisons on n'est pas dans le cas 4. Ainsi l'algorithme est terminé. □

Démonstration de l'unicité. Elle repose sur le fait suivant, qui justifie aussi qu'en itérant l'algorithme, les invariants de Smith de la sous-matrice M' seront des multiples du coefficient a.

Lemme 3. *Soit $M \in \mathcal{M}_{m,n}(A)$, $P \in \mathrm{GL}_m(A)$ et $Q \in \mathrm{GL}_n(A)$. Pour tout $k \geqslant 1$, le* pgcd *des mineurs de taille k est le même pour M et PMQ.*

On démontrera ce lemme plus tard. reprenant les notations du théorème, r est le rang de M, et pour tout $k \in [1, r]$, $a_1 \dots a_k$ est le pgcd des mineurs de taille k de M. □

Proposition 4 (Formule de Cauchy-Binet)**.** *Soit B, C deux matrices de tailles $l \times m$ et $m \times n$, $p \leqslant n, l$, et des indices $i_1 < \dots < i_p$, $k_1 < \dots < k_p$. Le mineur de taille p de la matrice BC est*
$$(BC)\begin{pmatrix} i_1 & \dots & i_p \\ k_1 & \dots & k_p \end{pmatrix} = \sum_{1 \leqslant j_1 < \dots < j_p \leqslant m} (B)\begin{pmatrix} i_1 & \dots & i_p \\ j_1 & \dots & j_p \end{pmatrix} \cdot (C)\begin{pmatrix} j_1 & \dots & j_p \\ k_1 & \dots & k_p \end{pmatrix}$$

On en déduit le corollaire suivant.

Corollaire 5. *Si b divise le* pgcd *des mineurs de taille r de B et c divise le* pgcd *des mineurs de taille r de C, alors bc divise le* pgcd *des mineurs de taille r de BC.*

Le lemme 3 s'ensuit.

20. Théorème de Lie–Kolchin

Référence A. Chambert-Loir, *Algèbre corporelle.*

Leçons

- 106. Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $\mathrm{GL}(E)$. Applications
- 154. Sous-espaces stables par un endomorphisme ou une famille d'endomorphismes d'un espace vectoriel de dimension finie. Applications
- 157. Endomorphismes trigonalisables. Endomorphismes nilpotents
- 204

Théorème 1 (Lie-Kolchin)**.** *Tout sous-groupe résoluble connexe de* $\mathrm{GL}_n(\mathbf{C})$ *stabilise un drapeau complet.*

Énonçons deux lemmes sans démonstration.

Lemme 2. *Tout sous-groupe abélien de* $\mathrm{GL}_n(\mathbf{C})$ *stabilise un drapeau complet.*

Lemme 3.
- *Le groupe dérivé d'un groupe connexe est connexe.*
- *Le groupe dérivé d'un groupe résoluble est résoluble.*

Démonstration du théorème. On raisonne par récurrence forte sur n. Il est immédiat pour $n = 1$. Supposons donc le vérifié pour tout $k \leqslant n-1$. S'il existe un sous-espace G-stable non trivial. Notons le V, et $d \leqslant n-1$ sa dimension, puis soit $B_1 \cup B_2$ une base adaptée à l'inclusion $V \subset \mathbf{C}^n$. Dans cette base, écrivons les éléments $g \in G$ sous la forme

$$\begin{pmatrix} \phi_1(g) & \star \\ 0 & \phi_2(g) \end{pmatrix}.$$

L'application ϕ_1 étant un morphisme de groupes continu, $\phi_1(G)$ est un sous-groupe connexe résoluble de $\mathrm{GL}_d(\mathbf{C})$, donc, par hypothèse de récurrence, ses éléments sont cotrigonalisables, de même pour $\phi_2(G)$.

Supposons dorénavant qu'il n'existe aucun sous-espace non trivial stable par G. Déjà en vertu d'un des lemmes, G n'est pas abélien. Soit $m \geqslant 1$ minimal tel que $D^m(G) = \{1\}$. On sait que $m \geqslant 2$. Soit $H = D^{m-1}(G)$. Lui est abélien donc ses éléments sont cotriangulable : il existe en particulier une droite stable par H. Soit W les sous-espace engendré par tous les vecteurs propres communs aux éléments de H. On vérifie aisément qu'il est stable par G et, puisqu'il n'est pas réduit à $\{0\}$, c'est forcément $\mathbf{C}^n$. Aussi existe-t-il une base de vecteurs propres communs aux éléments de H : H est codiagonalisable. Montrons qu'en réalité ses éléments sont des homothéties. Pour $h \in H$, considérons l'application

$$\psi : \left| \begin{array}{ccc} G & \longrightarrow & H \lhd G \\ g & \longmapsto & ghg^{-1} \end{array} \right. .$$

Pour tout $g \in G$ et $\psi(g) = ghg^{-1} \in H$ commute avec h et lui est semblable, c'est donc une permutation de sa matrice diagonale. Ainsi $\psi(G)$ est fini. Puisque ψ est continu, il est aussi connexe donc réduit à un élément, qui est nécessairement h. Ceci prouve que $H \subset Z(G)$. Si $h \in H$, un sous-espace propre de H est donc stable par G, c'est dont $\mathbf{C}^n$, et h est une homothétie. On a prouvé que H était uniquement constitué d'homothéties. Par ailleurs, en tant que groupe dérivé, $\det(H) \subset \{1\}$. Ainsi H est fini. Étant aussi connexe, c'est $\{1\}$, contredisant ainsi la minimalité de m. □

21. Adhérence des matrices codiagonalisables

Référence RMS, 123-2.

Leçons

- 153. Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications
- 154. Sous-espaces stables par un endomorphisme ou une famille d'endomorphismes d'un espace vectoriel de dimension finie. Applications
- 155. Endomorphismes diagonalisables en dimension finie

Définition 1. Pour $n, N \geqslant 1$, on note

$$E_{n,N} = \{(PD_1P^{-1}, \dots, PD_NP^{-1}) \,:\, D_i \in \mathcal{M}_n(\mathbf{C}) \text{ diagonales}, P \in \mathrm{GL}_n(\mathbf{C})\}.$$

On dit que le couple (n, N) est admissible si l'adhérence de $E_{n,N}$ contient toutes les N-uplets de matrices commutant deux-à-deux.

On va étudier l'admissibilité des couples (n, N). Seuls les couples du type $(n, 3)$ avec $n \geqslant 4$ échapperont à notre étude. Commençons par énoncer le lemme facile mais très utile suivant.

Lemme 2. *Si $A_1 \in \mathcal{M}_n(\mathbf{C})$ et $A_2, \dots, A_N \in \mathbf{C}[A_1]$, alors $(A_1, \dots, A_N) \in \overline{E_{n,N}}$.*

Théorème 3. *Pour tout $n \geqslant 1$, $(n, 2)$ est admissible.*

Démonstration. On procède par récurrence forte sur n. Pour $n = 1$, c'est facile. Supposons par l'absurde que (A, B) est un couple de matrices qui commutent mais qui n'est pas dans l'adhérence de $E_{n,2}$.

Lemme 4. *Il existe un projecteur non trivial C commutant avec A.*

Démonstration. Si A admet deux valeurs propres distinctes, on prend pour C le projecteur sur un sous-espace caractéristique de A parallèlement aux autres. Sinon, notant λ sa seule valeur propre, d'après le théorème de réduction de Jordan, $\mathbf{C}^n = N_1 \oplus \dots \oplus N_s$, où $A - \lambda I$ est nilpotente d'ordre $\dim N_k$ sur N_k. Si $s = 1$ alors $B \in \mathbf{C}[A]$, contradiction. Donc $s \neq 1$ et on peut prendre pour C le projecteur sur N_1 parallèlement aux autres N_k. □

Considérons le polynôme

$$P(X) = (\mathrm{Tr}(XB + C))^n - n^n \det(XB + C).$$

Déjà $P(0) = \mathrm{Tr}(C)^n \neq 0$ donc P n'est pas le polynôme nul et il existe $\delta > 0$ tel que si $\epsilon \in]0, \delta[$, $P(\epsilon^{-1}) \neq 0$. Si la matrice $\epsilon^{-1}B + C$ admet une unique valeur propre λ alors $P(\epsilon^{-1}) = (n\lambda)^n - n^n\lambda^n = 0$, ce qui n'est pas possible vu le lemme 2. Soient donc $\epsilon^{-1}\lambda_1, \dots, \epsilon^{-1}\lambda_l$ ses valeurs propres, et $k_1, \dots, k_l$ leur multiplicité respective. On a

$$\mathbf{C}^n = \bigoplus_{s=1}^{l} \ker(B + \epsilon C - \lambda_s)^{k_s}.$$

Puisque A commute avec $B + \epsilon C$, ces sous-espaces non triviaux sont stables par A et $B + \epsilon C$. Par hypothèse de récurrence, il existe des couples matrices codiagonalisables $(D_1, \Delta_1), \dots, (D_s, \Delta_s)$ approchant leur restriction. On en déduit que $(A, B + \epsilon C)$ est dans l'adhérence de $E_{n,2}$, ce pour tout $\epsilon \in]0, \delta[$, donc (A, B) aussi. □

Théorème 5. *Pour tout $N \geqslant 1$, les paires $(1, N)$, $(2, N)$ et $(3, N)$ sont admissibles.*

Démonstration. Le cas $n = 1$ est facile. Pour $n = 2$. Soient $A_1, \dots, A_N \in \mathcal{M}_2(\mathbf{C})$ commutant deux-à-deux. Sans perte de généralité, on peut supposer qu'aucune d'elles n'est une homothétie. Dés lors A_1 est semblable soit à $\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ soit à $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$. Dans les deux cas son commutant est $\mathbf{C}[A_1]$ et le lemme 2 permet de conclure.

Passons au cas où $n = 3$. Soient $A_1, \dots, A_N \in \mathcal{M}_3(\mathbf{C})$ commutant deux-à-deux. Sans perte de généralité, on peut toujours supposer qu'aucune d'elles n'est une homothétie. Quitte à leur ajouter une homothétie, on peut supposer qu'elles sont toutes de trace nulle. Si A_1 a trois valeurs propres distinctes, son commutant est $\mathbf{C}[A_1]$, et le lemme 2 termine. Si A_1 est semblable à

$$\begin{pmatrix} \lambda & \star & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & -2\lambda \end{pmatrix},$$

Les autres matrices laissent stable le dernier vecteur de cette base et le plan engendré par les deux premiers. On est ramené au cas $n = 2$. Si A_1 est semblable à

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix},$$

son commutant est là encore $\mathbf{C}[A_1]$ et le lemme 2 conclut. Il reste le cas où A_1, et en fait toutes les matrices A_i, sont chacune semblable à

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

□

Enfin énonçons le résultat négatif.

Théorème 6. *Pour tout $N \geqslant 4$, $n \geqslant 4$, (n, N) n'est pas admissible.*

On aura besoin du lemme suivant.

Lemme 7. *Si $(A_1, \dots, A_N) \in \overline{E_{n,N}}$, alors $\dim \mathbf{C}[A_1, \dots, A_N] \leqslant n$.*

Démonstration. Soit $(B_{1,k}, \dots, B_{N,k})$ des matrices codiagonalisables approchant $(A_1, \dots, A_N)$: on se donne des matrices $Q_k \in \mathrm{GL}_n(\mathbf{C})$ telles que les matrice $Q_k B_{1,k} Q_k^{-1}, \dots, Q_k B_{N,k} Q_k^{-1}$ soient diagonales. Si $P_1, \dots, P_s \in \mathbf{C}[X_1, \dots, X_N]$,

$$P_j(B_{1,k}, \dots, B_{N,k}) = Q_k^{-1} P_j(D_{1,k}, \dots, D_{N,k}) \in Q_k^{-1} \mathbf{C}[D_{1,k}, \dots, D_{N,k}] Q_k,$$

qui est de dimension au plus n. Ainsi le rang de la famille $(P_j(B_{1,k}, \dots, B_{N,k}))_j$ est inférieur à n, et par semi-continuité inférieure du rang, celui de la famille $(P_j(A_1, \dots, A_N))_j$ aussi, ce qui conclut. □

Démonstration. Évidemment il suffit de démontrer que pour tout $n \geqslant 4$, $(n, 4)$ n'est pas admissible. Commençons par $n = 4$. Notons $e_{i,j}$ les matrices de la base canonique de $\mathcal{M}_4(\mathbf{C})$ et considérons le 4-uplet $(e_{1,3}, e_{1,4}, e_{2,3}, e_{2,4})$ qui commutent deux-à-deux mais dont l'algèbre engendré est de dimension au moins 5. Par suite $(4, 4)$ n'est pas admissible.
Soit maintenant $n \geqslant 4$. (voir la référence pour la fin de la preuve). □

22. Sous-groupes finis de $\mathrm{SO}(\mathbf{R}^3)$

Référence F. Combes, *Algèbre et géométrie.*

Leçons

- 101. Groupe opérant sur un ensemble. Exemples et applications
- 106. Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $\mathrm{GL}(E)$. Applications
- 161. Isométries d'un espace affine euclidien de dimension finie. Applications en dimension 2 et 3
- 183. Utilisation des groupes en géométrie
- 190. Méthodes combinatoires, problèmes de dénombrement

Remarque 1. Ma démonstration diffère de celle du Combes pour le cas $\mathfrak{A}_5$ en ce que je ne suppose pas connu le groupe d'isométries de l'icosaèdre. Celui-ci est obtenu comme corollaire. Le prix à payer est l'étude des sous-groupes d'ordre 60 du $\mathfrak{S}_6$, qui me semble assez intéressante, mais qui est si on veut la traiter convenablement assez longue. Je me contente d'en donner les grandes idées.

Théorème 2. *Tout sous-groupe fini de* $\mathrm{SO}(\mathbf{R}^3)$ *est soit un groupe cyclique, soit un groupe diédral, soit isomorphe à* $\mathfrak{A}_4$, $\mathfrak{S}_4$ *ou* $\mathfrak{A}_5$.

Démonstration. Soit G un sous-groupe fini de $\mathrm{SO}(\mathbf{R}^3)$, de cardinal noté n. Tout élément distinct de l'identité a une droite de points fixes, qui intersecte la sphère euclidienne en deux pôles P et $-P$. Considérons l'ensemble $\mathcal{P}$ des pôles des éléments de $G\backslash\{1\}$. G agit sur $\mathcal{P}$ par la restriction de l'action naturelle sur $\mathbf{R}^3$. En effet, si P est un pôle de g, et $h \in G$ alors $h(P)$ est un pôle de hgh^{-1}. On va décrire le groupe G grâce à son action sur $\mathcal{P}$. Soit k le nombre d'orbites de cette action. La formule des classes donne

$$k = \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)| = \frac{1}{n}(|\mathcal{P}| + 2(n-1)).$$

Constatons d'autre part que $2 \leqslant \mathcal{P} \leqslant 2(n-1)$, donc $2 \leqslant k < 4$, soir $k = 2$ ou $k = 3$.

Cas 1 : $k = 2$. Dans ce cas $|\mathcal{P}| = 2$. Autrement dit tous les éléments de G ont les mêmes pôles et stabilisent donc le plan orthogonal. Le groupe G est ainsi isomorphe à un sous-groupe fini de $\mathrm{SO}(\mathbf{R}^2)$, donc est cyclique.

Cas 2 : $k = 3$, dans ce cas $\mathcal{P} = n + 2$. Soient $\mathcal{P}_1$, $\mathcal{P}_2$ et $\mathcal{P}_3$ ces orbites et m_1, m_2, m_3 les cardinaux des stabilisateurs de ces orbites. On a

$$\frac{1}{m_1} + \frac{1}{m_1} + \frac{1}{m_1} = \frac{1}{n}|\mathcal{P}| = 1 + \frac{2}{n}.$$

On constate que les seules valeurs possibles sont

1. $m_1 = m_2 = 2$, $m_3 = n/2$;
2. $m_1 = 2$, $m_2 = 3$, $m_3 = 3$, $n = 12$, et donc $|\mathcal{P}_1| = 6$, $|\mathcal{P}_2| = 4$ et $|\mathcal{P}_3| = 4$;
3. $m_1 = 2$, $m_2 = 3$, $m_3 = 4$, $n = 24$, et donc $|\mathcal{P}_1| = 12$, $|\mathcal{P}_2| = 8$ et $|\mathcal{P}_3| = 6$;
4. $m_1 = 2$, $m_2 = 3$, $m_3 = 5$, $n = 60$, et donc $|\mathcal{P}_1| = 30$, $|\mathcal{P}_2| = 20$ et $|\mathcal{P}_3| = 12$.

On traite le dernier cas. Le troisième se traite de la même manière et les deux premiers sont bien traités dans le Combes.
Cas 2.4 : Constatons déjà que vus les cardinaux des orbites, $P \in \mathcal{P}_3$ si et seulement si $\mathrm{Stab}(P)$ est de cardinal 5. Or $\mathrm{Stab}(P) = \mathrm{Stab}(-P)$, ainsi $\mathcal{P}_3$ s'écrit $\{\pm P_1, \ldots, \pm P_6\}$. Le groupe G agit sur l'ensemble

$$X = \{\{-P_1, P_1\}, \ldots, \{-P_6, P_6\}\}.$$

L'action est fidèle. En effet si $g \in G$ fixe ces six paires. Si $g \neq 1$, g ne peut pas fixer quatre points distincts de la sphère donc on peut supposer $g \cdot P_1 = -P_1$, ..., $g \cdot P_5 = -P_5$. Si $g \cdot P_6 = P_6$, alors $g \in \mathrm{Stab}(P_6)$, qui est d'ordre 5. C'est absurde car $g \neq 1$ et $g^2 = 1$. Ainsi $g \cdot P_6 = -P_6$, et g est une rotation d'angle π et les points de $\mathcal{P}_3$ sont tous coplanaires. Un élément non trivial du stabilisateur de P_1 est d'ordre 5 donc il est impossible qu'il envoie P_2 sur un élément de ce plan. D'où l'absurdité. On a établi que l'action de G sur X est fidèle, et donc que G est isomorphe à un sous-groupe de $\mathfrak{S}_6$. On sait aussi depuis le début que G est d'ordre $n = 60$. On conclut grâce au théorème suivant. □

Théorème 3. *Les sous-groupes d'ordre* 60 *de* $\mathfrak{S}_6$ *sont isomorphes à* $\mathfrak{A}_5$.

Démonstration. Soit G un tel sous-groupe. Il contient un élément d'ordre 3 (lemme de Cauchy). C'est soit un 3-cycle soit un produit de deux 3-cycles à support disjoints. Le second cas se ramène au premier en utilisant un automorphisme extérieur de $\mathfrak{S}_6$ (ceux-ci envoient les transpositions sur les triple-transpositions et les 3-cycles sur les double 3-cycles. On peut donc supposer que G contient un 3-cycle c. Il contient aussi un élément d'ordre 5, qui est un 5-cycle σ. Quitte à les multiplier et conjuguer, on peut supposer que le 3-cycle a un support inclus dans celui du 5-cycle. Disons $\sigma = (1\,2\,3\,4\,5)$. Quitte à conjuguer/renuméroter/ (prendre des puissance de σ et c), on peut supposer que $c = (1\,2\,3)$. Dés lors $c' = \sigma c \sigma^{-1} = (2\,3\,4)$. Avec c et c', on construit le groupe de Klein de $\mathfrak{A}_4$. Finalement le sous-groupe de G engendré par σ et c est d'ordre au moins $4 \times 3 \times 4 = 60$, c'est donc G tout entier. Mais ce sous-groupe $\langle c, \sigma \rangle$ est inclus dans $\mathfrak{A}_5$. Ainsi $G = \mathfrak{A}_5$. □

Corollaire 4. *Le groupe d'isométries de l'icosaèdre est* $\mathfrak{A}_5 \times \mathbf{Z}/2\mathbf{Z}$. *Son groupe d'isométries positives est* $\mathfrak{A}_5$.

Démonstration. Le groupe d'isométries positives G^+ de l'icosaèdre est un sous-groupe de $\mathrm{SO}(\mathbf{R}^3)$, qui est fini car il agit fidèlement sur l'ensemble des sommets de l'icosaèdre. C'est donc soit un groupe cyclique, soit un groupe diédral, soit un groupe isomorphe à $\mathfrak{A}_4$, $\mathfrak{S}_4$ ou $\mathfrak{A}_5$. Mais G^+ contient au moins (bien plus en fait) 8 éléments d'ordre 5 (des rotations), alors que $\mathfrak{A}_4$ et $\mathfrak{S}_4$ n'en contiennent pas, et les groupes diédraux et cycliques en contiennent au plus 4. La seule possibilité est que $G^+ \simeq \mathfrak{A}_5$.
Puisque $-\mathrm{Id}$ est dans le groupe d'isométries G de l'icosaèdre, et qu'ils commute à toutes les isométries positives, on a $G \simeq \mathfrak{A}_5 \times \mathbf{Z}/2\mathbf{Z}$. □

On trouve de même les groupes d'isométries du cube.

23. Réduction de Frobenius

Référence X. Gourdon, *Algèbre.*

Leçons

— 153. Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications

— 154. Sous-espaces stables par un endomorphisme ou une famille d'endomorphismes d'un espace vectoriel de dimension finie. Applications

— 159. Formes linéaires et hyperplans en dimension finie. Exemples et applications

24. Théorème de l'élément primitif

Référence S. Francinou, H. Gianella, *Exercices de mathématiques pour l'agrégation.*

Leçons

— 125. Extensions de corps. Exemples et applications

25. Loi de réciprocité quadratique et formes quadratiques

Référence P. Caldero, J. Germoni, *Histoire hédonistes de groupes et de géométries.*

Leçons

— 101. Groupe opérant sur un ensemble. Exemples et applications

— 121. Nombres premiers. Applications

— 170. Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications

— 190. Méthodes combinatoires, problèmes de dénombrement

26. Théorème de la borne de Bezout

Référence ,

Leçons

— 142. Algèbre des polynômes à plusieurs indéterminées. Applications

— 143. Résultant. Applications

— 152. Déterminant. Exemples et applications

27. Automorphismes de $\mathfrak{S}_n$

Référence D. Perrin, *Cours d'algèbre.*

Leçons

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

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

28. Table de caractères de $\mathfrak{S}_4$

Référence

Leçons

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

— 107. Représentations et caractères d'un groupe fini sur un $\mathbf{C}$-espace vectoriel

— 109. Représentations de groupes finis de petit cardinal

29. Ellipsoide de John-Lowner

Référence Francinou Gianella Nicolas, *Oraux x-ens.*

Leçons

— 170. Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications

— 171. Formes quadratiques réelles. Exemples et applications

— 219. Extremums : existence, caractérisation, recherche. Exemples et applications

30. Fractions rationnelles et Séries formelles

Référence J.-Y. Merindol, *Nombres et algèbre.*

Leçons

— 124. Anneau des séries formelles. applications

— 140. Corps des fractions rationnelles à une indéterminée sur un corps commutatif. Applications

Développements d'analyse

31. Méthode QR

Référence Ciarlet, *Analyse numérique*

Leçons

- 232. Méthodes d'approximation des solutions d'une équation $F(X) = 0$. Exemples
- 233. Analyse numérique matricielle : résolution approchée de systèmes linéaires, recherche de vecteurs propres, exemples

Nous notrerons $T_n^+(\mathbf{C})$ l'ensemble des matrices triangulaires supérieures de $\mathcal{M}_n(\mathbf{C})$ dont les coefficients diagonaux sont des réels strictement positifs.

Proposition 1 (Décomposition QR)**.** *L'application*

$$\begin{aligned}(Q, R) &\mapsto QR \\ U_n(\mathbf{C}) \times T_n^+(\mathbf{C}) &\to \mathrm{GL}_n(\mathbf{C})\end{aligned}$$

est un homéomorphisme.

Démonstration. L'injectivité et la continuité de l'application ne posent pas de problème. Sa surjectivité repose sur le procédé d'orthononormalisation de Gram–Schmidt. La continuité de l'application réciproque peu être établie grâce à la compacité de $U_n(\mathbf{C})$. □

Théorème 2. *Soit $A \in \mathrm{GL}_n(\mathbf{C})$. Supposons qu'existent des nombres complexes $\lambda_1, \ldots, \lambda_n$ satisfaisant*

$$|\lambda_1| > \ldots > |\lambda_n| > 0, \tag{5}$$

ainsi qu'une matrice inversible P dont l'inverse admet une décomposition LU, tels que

$$P^{-1}AP = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}.$$

Considérons la suite définie par récurrence comme suit : $A_1 = A$, et si $Q_k R_k$ est la décomposition QR de A_k, $A_{k+1} := R_k Q_k$. La partie triangulaire inférieure de cette suite de matrice tend vers celle de la matrice diagonale $(\lambda_1, \ldots, \lambda_n)$.

Démonstration. Notons $\mathcal{Q}_k = Q_1 \ldots Q_k$ et $\mathcal{R}_k = R_k \ldots R_1$. On a :

$$A_k = \mathcal{Q}_k^* A \mathcal{Q}_k.$$

Par ailleurs,

$$A^k = (Q_1R_1)^k = Q_1(R_1Q_1)^{k-1}R_1 = Q_1(Q_2R_2)^{k-1}R_1 = \ldots = \mathcal{Q}_k\mathcal{R}_k,$$

mais aussi

$$A^k = PD^kP^{-1} = Q_PR_PD^kLU = Q_PR_P\underbrace{D^kLD^{-k}}_{=:L_k}D^kU.$$

La matrice L est triangulaire supérieure de diagonale 1 donc, vue l'hypothèse (5), L_k converge vers la matrice I_n, et $\tilde{L}_k := RL_kR^{-1}$ aussi. Soit $\tilde{L}_k = O_kV_k$ sa décomposition QR. S'agissant d'un homéomorphisme, on a $O_k \to I_n$ et $V_k \to I_n$.
Par ailleurs la décomposition QR de A^k est

$$A^k = \mathcal{Q}_k\mathcal{R}_k = Q_PR_PL_kD^kU = Q\tilde{L}_kR_PD_k = [Q_PO_k][V_kR_PD^kU].$$

Pour invoquer l'unicité, il faut que le produit de droite, qui est déjà une matrice triangulaire supérieure, ait une diagonale positive. Pour cela factorisons D et U par la diagonale des modules de leurs termes diagonaux : $D = \Delta_1|D|$, $U = \Delta_2U'$. Puis on écrit

$$A^k = [Q_PO_k\Delta_1^k\Delta_2][\Delta_2^{-1}\Delta_1^{-k}V_kR_P\Delta_1^k|D|^k\Delta_2U'].$$

L'unicité donne $\mathcal{Q}_k = Q_PO_k\Delta_1^k\Delta_2$. De cette convergence et de la relation $A_k = \mathcal{Q}_k^{\mathbf{T}}A\mathcal{Q}_k$ découle

$$A_k = (\Delta_1^k\Delta_2)^*[O_k^*(Q_P^*AQ_P)O_k](Delta_1^k\Delta_2) \tag{6}$$

Or, comme $P = Q_PR_P$,

$$Q_P^{\mathbf{T}}AQ_P = Q_P^{\mathbf{T}}Q_PR_PD(Q_PR_P)^{-1}Q_P = R_PDR_P^{-1} = \begin{pmatrix} \lambda_1 & & (*) \\ & \ddots & \\ & & \lambda_n \end{pmatrix}.$$

Aussi le terme entre crochets dans (6) converge vers cette dernière matrice triangulaire supérieure dont la partie triangulaire inférieure n'est pas affecté par la conjugaison par $\Delta_1^k\Delta_2$. □

Remarque 3. Si la matrice A est réelle et satisfait aux hypothèses, alors ses valeurs propres sont réelles et la suite A^k est aussi à valeurs réelles.

Remarque 4. L'algorithme ne fonctionne pas s'il existe deux valeurs propres de même module. Par exemple si A est orthogonale, sa décomposition QR est triviale, et pour tout k, $A_k = A$.

Méthode de Householder de calcul de la décomposition QR : Au procédé d'othonormailisation de Gram-Schmidt, instable numériquement, on préfère la méthode de Householder. SI u est un vecteur de norme 1, la matrice de Householder est la matrice orthogonale (et symétrique !)

$$H(u) = I - 2uu^{\mathbf{T}}$$

Soit $e_1 = (1, 0, \ldots, 0)^{\mathbf{T}}$, x la première colonne de A et enfin $\alpha = \varepsilon\|x\|$, ε étant le signe de la première coordonnée de x (si elle n'est pas nulle). Si x est proportionnel à e_1, on prend $u = 0$, sinon $u = \frac{x-\alpha e_1}{\|x-\alpha e_1\|}$. Dans tous les cas on a

$$H(u)A = \begin{pmatrix} \alpha & \star & \ldots & \star \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix}.$$

On applique le même algorithme à la matrice A'. Ultimement, on dispose d'une matrice triangulaire supérieure, que l'on factorise ensuite par la diagonale des signes.

32. Théorèmes de l'application ouverte et du graphe fermé.

Référence

Leçons

— 205. Espaces complets. Exemples et applications

— 208. Espaces vectoriels normés, applications linéaires continues. Exemples

Soient E et F deux espaces de Banach, et T une application linéaire de E dans F.

Théorème 1 (Théorème de l'application ouverte)**.** *Si l'application T est continue et surjective alors elle est ouverte. Si elle est bijective et continue, son inverse aussi.*

Démonstration. On souhaite montrer qu'il existe $\delta > 0$ tel que $B_F(0,\delta) \subset T(B_E(0,1))$, ce qui par linéarité de T conclura. Soit le fermé

$$F_n = \overline{T(B_E(0,n))}.$$

Puisque T est surjective,

$$\bigcup_{n\geqslant 1} F_n = F.$$

Et comme F est complet, la propriété de Baire assure que l'un des F_n est d'intérieur non vide : soit $n \geqslant 1$, $u \in F$ et $r > 0$ tel que

$$F_n \supset B_F(u,r).$$

Par linéarité, $F_n \supset B_F(-u,r)$, puis $B_F(0,r) \subset F_n = \overline{T(B_E(0,n))}$ et

$$B_F(0,r/n) \subset F_n = \overline{T(B_E(0,1))}$$

. Utilisons maintenant la complétude de E. Soit $y \in B(0,\frac{r}{10n})$; Il existe $x_0 \in B_E(0,\frac{1}{10})$ tel que

$$\|Tx_0 - y\|_F \leqslant \frac{r}{10n}\frac{1}{2}.$$

Par récurrence on construit $x_1 \ldots, x_k$ tels que $x_k \in B_E(0,\frac{1}{10\cdot 2^k})$ et

$$\|(Tx_0 + \ldots + Tx_k) - y\|_F \leqslant \frac{r}{10n}\frac{1}{2^{k+1}}.$$

Comme E est complet, $\sum x_k$ converge, disons vers $x \in B_E(0,1)$, et comme T est continue, $T(x_0 \cdots x_k)$ tend vers Tx. Enfin $\|Tx - y\|_F = 0$. On a montré que $T(B_E(0,1)) \supset B_F(0,\frac{r}{10n})$. □

Théorème 2 (Théorème du graphe fermé)**.** *L'application T est continue si et seulement si son graphe $G = \{(x,Tx) : x \in E\}$ est fermé.*

Démonstration. Si T est continue, soit $(x_n) \in E$ telle que $(x_n, Tx_n) \to (x,y)$. Comme T est continu, $Tx = y$.
Si $G \subset E \times F$ est fermé, alors c'est un espace de Banach, et l'application

$$\Pi : \left| \begin{array}{ccc} (x,Tx) & \longmapsto & x \\ G & \longrightarrow & E \end{array} \right.$$

est continue et bijective donc d'inverse continue, c'est-à-dire que T est continue. □

Application Soit $1 \leqslant p \leqslant \infty$, $(E, \mathcal{A}, \mu)$ un espace mesuré σ-fini et f une application mesurable sur E telle que pour toute $g \in L^p$, $fg \in L^p$. Alors $f \in L^\infty$.
Si $p = \infty$, on conclut en prenant $g = 1$. Sinon on considère l'application

$$\Phi : \left| \begin{array}{ccc} g & \longmapsto & fg \\ L^p & \longrightarrow & L^p \end{array} \right. .$$

Si $(g_n) \in L^p$ est une suite telle que $(g_n, \Phi(g_n)) \to (g, h)$. Alors il existe une extraction g_{n_k} convergeant presque partout vers g. Dés lors $\Phi(g_n) \to \Phi(g)$ presque partout. Nécessairement, $\Phi(g) = h$. Ceci prouve, grâce au théorème du graphe fermé, que Φ est continue. Soit M sa norme. On va montrer que $\|f\|_\infty \leqslant M + 1$. Pour cela considérons E_n une suite croissante d'éléments de $\mathcal{A}$ de mesure finie et dont la réunion est E. On a pour $g_n = \mathbf{1}_{|f|>M+1}\mathbf{1}_{E_n}$

$$\|g_n f\| \leqslant M\|g_n\|,$$

et a fortiori

$$(M+1)\mu(E_n \cap \{|f| > M+1\})^{1/p} \leqslant M\mu(E_n \cap \{|f| > M+1\})^{1/p}.$$

Nécessairement

$$\mu(E_n \cap \{|f| > M+1\}) = 0,$$

et par σ-additivité,

$$\mu(\{|f| > M+1\}) = 0,$$

ce qui conclut.

33. Processus de branchement critique

Ce développement suppose une certaine familiarité avec le développement usuel autour du processus de branchement. On pourra l'utiliser dans les leçons suivantes :

- 226. Suites vectorielles et réelles définies par une relation de récurrence $u_{n+1} = f(u_n)$. Exemples et applications
- 229. Fonctions monotones. Fonctions convexes. Exemples et applications
- 241. Suites et séries de fonctions. Exemples et contre-exemples
- 243. Convergence des séries entières, propriétés de la somme. Exemples et applications
- 260. Espérance, variance et moments d'une variable aléatoire
- 261. Fonction caractéristique et transformée de Laplace d'une variable aléatoire. Exemples et applications
- 262. Modes de convergence d'une suite de variables aléatoires. Exemples et applications
- 264. Variables aléatoire discrètes. Exemples et applications

Référence : K.B. Athreya and P. E. Ney, *Branching processes.*

On se propose ici d'étudier le processus de Bienaymé–Galton–Watson dans le cas critique d'une loi de reproduction d'espérance 1. Soit μ une mesure de probabilité sur $\mathbf{N}$ de moyenne 1, telle que $\mu(1) \neq 1$. On suppose aussi que μ admet un moment d'ordre 2 : on note

$$Var(\mu) = \sigma^2 = \sum_{k=0}^{\infty} k^2 \mu(k) - \left[\sum_{k=0}^{\infty} k\mu(k) \right]^2 .$$

Constatons que comme on a supposé $E[\mu] = \sum_{k=0}^{\infty} k\mu(k) = 1$, on a l'égalité

$$Var(\mu) = \sigma^2 = \sum_{k=0}^{\infty} k(k-1)\mu(k).$$

Considérons le processus de branchement (Z_n) de loi de reproduction μ et partant d'un individu $(Z_0 = 1)$.

Théorème 1. *Sous ces hypothèses on a*

$$P(Z_n > 0) \sim \frac{2}{n\sigma^2}.$$

Ainsi que la convergence en loi suivante

$$\mathcal{L}\left(\frac{Z_n}{n} | Z_n > 0 \right) \longrightarrow \mathcal{E}\left(\frac{2}{\sigma^2} \right),$$

au sens où pour tout $u > 0$,

$$P\left(\frac{Z_n}{n} \leqslant u | Z_n > 0 \right) \longrightarrow \frac{2}{\sigma^2} \int_0^u \exp \frac{2t}{\sigma^2} \, \mathrm{d}t$$

Lemme 2. *Notons G la fonction génératrice de la loi μ : $G(s) = \sum_{k=0}^{\infty} s^k \mu(k)$. C'est une fonction de classe C^2, strictement monotone et convexe sur $[0, 1]$, satisfaisant : $G(1) = 1$, $G'(1) = 1$, $G''(1) = \sigma^2$.*

Démonstration. Il est clair que G est C^2, convexe sur $[0,1[$. Par convergence monotone, elle est continue en 1,

$$G'(s) = \sum_{k=1}^{\infty} k s^{k-1} \mu(k) \underset{s\to 1^-}{\to} E[\mu] = 1,$$

et

$$G''(s) = \sum_{k=2}^{\infty} k(k-1) s^{k-2} \mu(k) \underset{s\to 1^-}{\to} Var(\mu) = \sigma^2.$$

On conclut avec un théorème de prolongement de la dérivée. □

Lemme 3. *Notant $G^n = G \circ \ldots \circ G$, on a*

$$\frac{1}{n}\left[\frac{1}{1-G^n(t)} - \frac{1}{1-t}\right] \underset{n\to\infty}{\to} \frac{\sigma^2}{2}$$

uniformément sur $[0,1[$.

Démonstration. L'idée est d'appliquer un lemme de Césaro : écrivons pour cela une somme télescopique.

$$\frac{1}{n}\left[\frac{1}{1-G^n(t)} - \frac{1}{1-t}\right] = \frac{1}{n}\sum_{k=1}^{n} \underbrace{\left[\frac{1}{1-G^k(t)} - \frac{1}{1-G^{k-1}(t)}\right]}_{\phi_k(t)}.$$

Un développement de Taylor-Young en $t = 1$ donne

$$G(t) = G(1) + G'(1)(t-1) + \frac{1}{2}G''(1)(t-1)^2 + \underset{t\to 1}{o}((t-1)^2)$$

C'est-à-dire

$$1 - G(t) = 1 - t + \frac{\sigma^2}{2}(t-1)^2 + \underset{t\to 1}{o}((t-1)^2).$$

Par conséquent

$$\frac{1}{1-G(t)} - \frac{1}{1-t} = \frac{\sigma^2}{2} + \rho(t),$$

avec $\rho(t) \underset{t\to 1}{\to} 0$. Ainsi on obtient

$$\phi_k(t) = \frac{\sigma^2}{2} + \rho(G^{k-1}(t)),$$

puis

$$\sup_{t\in[0,1[} \left|\frac{1}{n}\left[\frac{1}{1-G^n(t)} - \frac{1}{1-t}\right] - \frac{\sigma^2}{2}\right| \leqslant \frac{1}{n}\sum_{k=1}^{n} \sup_{t\in[0,1[} |\rho(G^{k-1}(t))|.$$

Mais, vue la croissance de G, on a pour tout $k \geqslant 1$ et $t \in [0,1[$, $G^{k-1}(0) \leqslant G^{k-1}(t) \leqslant 1$. D'autre part $G^{k-1}(0) \underset{k\to\infty}{\to} 1$. Ainsi,

$$\sup_{t\in[0,1[} |\rho(G^{k-1}(t))| \underset{k\to\infty}{\to} 0.$$

Le théorème de Césaro donne alors

$$\frac{1}{n}\sum_{k=1}^{n} \sup_{t\in[0,1[} |\rho(G^{k-1}(t))| \underset{n\to\infty}{\to} 0.$$

Le résultat s'ensuit. □

Démonstration du théorème. Le lemme précédent, appliqué à $t = 0$ donne

$$\frac{1}{n}\left[\frac{1}{P(Z_n > 0)} - 1\right] = \frac{1}{n}\left[\frac{1}{1 - G^n(t)} - \frac{1}{1-t}\right] \underset{n\to\infty}{\to} \frac{\sigma^2}{2},$$

c'est-à-dire

$$P(Z_n > 0) \sim \frac{2}{n\sigma^2}.$$

D'autre part, si l'on calcule la transformée de Laplace de la loi $\mathcal{L}\left(\frac{Z_n}{n} | Z_n > 0\right)$, on a

$$E\left[e^{-tZ_n/n} | Z_n > 0\right] = \frac{G^n(t_n) - G^n(0)}{1 - G^n(0)} = 1 - \frac{1 - G^n(t_n)}{1 - G^n(0)},$$

où $t_n = \exp(-t/n)$. La convergence uniforme du lemme précédent donne donc

$$E\left[e^{-tZ_n/n} | Z_n > 0\right] \underset{n\to\infty}{\to} \frac{2}{t\sigma^2 + 2},$$

qui est la transformée de Laplace de la loi $\mathcal{E}(2/\sigma^2)$. □

34. Théorème de Brouwer

Référence S. Gonnord et N. Tosel *Thèmes d'analyse pour l'agrégation, tome 2.*

Leçons

- 203. Utilisation de la notion de compacité
- 204. Connexité. Exemples et applications
- 206. Théorèmes de point fixe. Exemples et applications
- 214. Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications
- 215. Applications différentiables définies sur un ouvert de $\mathbf{R}^n$. Exemples et applications
- 253. Utilisation de la notion de convexité en analyse

Soit $n \in \mathbf{N}^*$. On note $\bar{B}$ (resp. B) la boule unité fermée (resp. ouverte) de $\mathbf{R}^n$, et S la sphère unité, pour la norme euclidienne. Enfin on notera λ la mesure de Lebesgue sur $\mathbf{R}^n$.

Lemme 1 (Lemme de non-rétraction C^1)**.** *Il n'existe pas de fonction $f : \bar{B} \to S$ de classe C^1 telle que $f|_S = Id_S$.*

Démonstration. Supposons qu'une telle fonction existe, notons la f. Posons $v = f - Id : \bar{B} \to \mathbf{R}^n$, et pour $t \in \mathbf{R}$, $v_t = Id + tv$, qui sont des fonctions de classe C^1. Notons enfin $\delta = \sup_{x\in\bar{B}} \|Dv(x)\|$. SI $|t| < 1/\delta$, $Dv_t(x) = Id + tDv(x)$ est inversible, et v_t est injective : v_t définit donc un C^1-difféomorphisme local.
D'un changement de variable C^1 découle, si $|t| < 1/\delta$, l'égalité

$$\begin{aligned}\lambda(v_t(B)) &= \int_{v_t(B)} \mathrm{d}\lambda(x) \\ &= \int_B |jv_t(x)|\,\mathrm{d}\lambda(x) \\ &= \int_B jv_t(x)\,\mathrm{d}\lambda(x).\end{aligned}$$

En particulier $t \mapsto \lambda(v_t(B))$ est polynomiale sur $]\pm 1/\delta[$. On sait que $v_t(\bar{B}) \subset \bar{B}$ (convexité). Par ailleurs $v_t(B)$ est ouvert dans B (inversion locale). D'autre part

$$v_t(\bar{B}) = v_t(B) \sqcup S.$$

Mais par compacité, $v_t(\bar{B})$ est fermé, donc, d'après l'égalité précédente, $v_t(B)$ est fermé dans B. Par connexité, $v_t(B) = B$.
Enfin considérons l'application polynomiale $\psi : t \mapsto \int_B jv_t(x)\,\mathrm{d}\lambda(x)$. On vient de voir que si $|t| < 1/\delta$, $\psi(t) = \lambda(B) \neq 0$. Ainsi ψ est une fonction constante non nulle. Mais $\psi(1) = 0$ car $jv_1(x) = 0$ ($v_1 = f : B \to S$). On a donc obtenu une contradiction. □

Théorème 2 (Théorème de Brouwer)**.** *Soit K un convexe compact de $\mathbf{R}^n$. Toute fonction continue $K \to K$ admet un point fixe.*

Démonstration. 1. Si $f : \bar{B} \to \bar{B}$ est de classe C^1 et n'admet pas de point fixe. Pour tout $x \in \bar{B}$ on considère l'unique point $h(x)$ de S situé sur la demi-droite $[f(x), x)$. Plus précisément, on cherche $t_x \geqslant 0$ tel que

$$h(x) = x + t_x(x - f(x)) \in S.$$

Le réel t_x est l'unique racine positive du polynôme de degré 2

$$P(t) = \|x + t(x - f(x))\|^2 - 1.$$

Le coefficient dominant est $\|f(x) - x\|^2$, qui est non nul, et le discriminant non plus : en effet $P(-1) \leqslant 0$, $P(0) \leqslant 0$, et $P(t) \to +\infty$ lorsque $t \to \pm\infty$. Finalement $x \mapsto t_x$ définit une application C^1 sur $\bar{B}$, donc h aussi. La fonction h est par suite une rétraction de classe C^1, ce qui est impossible. On a donc établi que f admet un point fixe.

2. Si $f : \bar{B} \to \bar{B}$ est continue. Soit p_n une suite de fonctions C^∞, convergeant uniformément vers f sur $\bar{B}$. Notons $\epsilon_n = \|p_n - f\|$. Les polynômes $\tilde{p}_n := \frac{1}{1+\epsilon_n} p_n$ satisfont les hypothèses de 1. donc admettent un point fixe $x_n \in \bar{B}$. Toute valeur d'adhérence de la suite x_n est un point fixe de f.

3. Enfin si $f : K \to K$ est une fonction continue. Soit $R > 0$ tel que $K \subset \bar{B}(0, R)$. La projection $\pi : \bar{B}(0, R) \to K$ sur le convexe compact K est continue, donc $f \circ \pi : \bar{B}(0, R) \to K \subset \bar{B}(0, R)$ aussi. Le point précédent donne l'existence d'un point fixe $x \in \bar{B}(0, R)$ de $f \circ \pi$. Mais $x = f \circ \pi(x) \in K$. Donc $\pi(x) = x$ puis $f(x) = x$. □

On en déduit le lemme de non-rétraction continue.

Théorème 3 (Lemme de non-rétraction continue)**.** *Il n'existe pas de fonction continue $f : \bar{B} \to S$ telle que $f_{|S} = Id_S$.*

Démonstration. Si f était une telle fonction, $-f$ serait une transformation continue de B sans point fixe. □

35. Construction du pré-mouvement brownien

Référence J.-F. le Gall, *Mouvement brownien, martingales et calcul stochastique*

Leçons

- 201. Espaces de fonctions. Exemples et applications
- 213. Espaces de Hilbert. Bases hilbertiennes. Exemples et applications
- 234. Espaces L^p, $1 \leqslant p \leqslant +\infty$
- 241. Suites et séries de fonctions. Exemples et contre-exemples
- 262. Modes de convergence d'une suite de variables aléatoires. Exemples et applications
- 263. Variables aléatoire à densité. Exemples et applications

On se place sur un espace probabilisé $(\Omega, \mathcal{F}, P)$.

Définition 1. Un prémouvement brownien est un famille $(B_t)_{t\in\mathbf{R}_+}$ de variables aléatoires gaussiennes centrées telles que

- $B_0 = 0$ presque sûrement ;
- pour tout $t \geqslant 0$, $B_t \sim \mathcal{N}(0, t)$;
- pour tous $0 \leqslant s_1 \leqslant t_1 \leqslant \ldots \leqslant s_n \leqslant t_n$, les variables $(B_{t_i} - B_{s_i})_{1\leqslant i\leqslant n}$ sont indépendantes.

Définition 2 (Espace gaussien)**.** Un espace gaussien est un sous-espace vectoriel fermé de $L^2(P)$ constitué uniquement de variables aléatoires gaussiennes centrées.

Propriété 3. *Un espace gaussien est un espace de Hilbert.*

Démonstration. C'est une partie fermée d'un espace de Hilbert. □

Proposition 4. *Des éléments d'un espace gaussien sont deux-à-deux orthogonaux si et seulement s'ils forment une famille indépendante.*

Démonstration. C'est en fait une propriété des vecteurs gaussiens. Soit $\mathcal{G}$ un espace gaussien et $Z_1, \ldots, Z_n$ des éléments de $\mathcal{G}$: on note $Z = (Z_1, \ldots, Z_n)$. C'est un fait général (non spécifique aux variables gaussiennes) que des variables indépendantes et centrées sont orthogonales. Pour établir la réciproque, supposons que les variables Z_i soient deux-à-deux orthogonales et prenons un élément $t \in \mathbf{R}^n$. La variable aléatoire $\langle t, Z\rangle = \sum t_i Z_i$ est un élément de $\mathcal{G}$: c'est donc une variable gaussienne centrée. Sa variance est

$$\sigma_t^2 = Var(\langle t, Z\rangle) = \sum_{i,j} t_i t_j E[Z_i Z_j] = \sum_i t_i^2 Var(Z_i).$$

S'agissant d'une variable gaussienne, on a

$$E[e^{i\langle t,Z\rangle}] = \exp\left(-\frac{\sigma_t^2}{2}\right) = \prod_i \exp\left(-\frac{t_i^2 Var(Z_i)}{2}\right).$$

C'est-à-dire

$$E[e^{i\langle t,Z\rangle}] = \prod_i E[e^{it_i Z_i}].$$

Ce qui conclut quant à l'indépendance des variables aléatoires (Z_i). □

Proposition 5. *Soit Z_k une suite de variables gaussiennes. Si elle converge dans L^2, alors la limite est gaussienne.*

Démonstration. Supposons que

$$Z_k \xrightarrow{L^2} Z.$$

A fortiori la convergence a lieu dans L^1 et $m_k := E[Z_k]$ converge vers $m = E[Z]$. La convergence L^2 donne alors la convergence de $\sigma_k^2 := Var(Z_k)$ vers $\sigma^2 = Var(Z)$. Ainsi pour tout $t \in \mathbf{R}$

$$E[e^{itZ}] = \lim_{k\to\infty} E[e^{itZ_k}] = \lim_{k\to\infty} e^{itm_k} e^{-\sigma_k^2 t^2/2} = e^{itm} e^{-\sigma^2 t^2/2}.$$

Finalement $Z \sim \mathcal{N}(m, \sigma^2)$. □

Corollaire 6 (Exemple fondamental)**.** *Soit (X_n) une suite de variables aléatoires i.i.d. de loi gaussienne centrée réduite. L'adhérence dans L^2 de $\mathrm{Vect}(X_n, n \geqslant 0)$ est un espace gaussien. La suite (X_n) en est une base hilbertienne.*

Démonstration. Une combinaison linéaire de variables gaussiennes **indépendantes** est une variable gaussienne. Par conséquent une suite d'éléments de $\mathrm{Vect}(X_n, n \geqslant 0)$ est une suite de variables gaussiennes Y_k centrées. La proposition précédente permet de conclure. □

Donnons-nous une suite (X_n) de variables aléatoires *i.i.d.* de loi gaussienne centrée réduite, et notons $\mathcal{G}$ l'espace gaussien $\overline{\mathrm{Vect}(X_n, n \geqslant 0)}$. Fixons par ailleurs une base hilbertienne (h_n) de $H = L^2(\mathbf{R}_+, \mathrm{d}x)$. Considérons l'application

$$\begin{aligned} W : H &\to \mathcal{G} \\ h &\mapsto \sum_{n=0}^{\infty} \langle h, h_n \rangle X_n \end{aligned}$$

Propriété 7. *W est une isométrie d'espaces de Hilbert. En particulier, pour tout $h \in H$, $W(h) \sim \mathcal{N}(0, \|h\|_{L^2}^2)$. D'autre part si (h_i) est une famille de fonctions othogonales (dans H) alors les variables $W(h_i)$ sont des variables gaussiennes indépendantes.*

Démonstration. Ces propriétés reposent sur le fait que W envoie une base hilbertienne sur une autre, puis sur la proposition 4. □

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

$$B_t := W(\mathbf{1}_{[0,t]}).$$

Proposition 8. *(B_t) est un pré-mouvement brownien.*

Démonstration. Déjà, comme $\|\mathbf{1}_{[0,t]}\|_{L^2}^2 = t$, on a pour tout $t \geqslant 0$, $B_t \sim \mathcal{N}(0, t)$. D'autre part si $0 \leqslant s_1 \leqslant t_1 \leqslant \ldots \leqslant s_n \leqslant t_n$, les fonctions $(\mathbf{1}_{]s_i,t_i]})$ sont deux-à-deux orthogonales dans H donc les variables $B_{t_i} - B_{s_i} = W(\mathbf{1}_{]s_i,t_i]})$ sont indépendantes. □

Remarque 9. Un mouvement brownien est un pré-mouvement brownien dont les trajectoires sont presque sûrement continues. Un critère de régularisation dû à Kolmogorov garantit l'existence d'un processus $(\tilde{B}_t)_{t\in\mathbf{R}_+}$ dont les trajectoires sont presque sûrement continues et tel que pour tout $t \geqslant 0$, on a presque sûrement $B_t = \tilde{B}_t$ (remarquer que la subtilité réside dans l'impossibilité d'échanger «pour tout t» et «presque sûrement»). Quoi qu'il en soit le fait que pour tout $t \geqslant 0$, *p.s.* $B_t = \tilde{B}_t$, garantit que $(\tilde{B}_t)$ est encore un pré-mouvement brownien. C'est donc un (vrai) mouvement brownien.

36. Inégalité de Carleman et une application.

Référence

— S. Francinou, H. Gianella, S. Nicolas, *Oraux x-ens, Analyse 1*

— RMS, numéro 120-1

Leçons

— 230. Séries de nombres réels ou complexes. Comportement des restes ou des sommes partielles des séries numériques. Exemples

Théorème 1 (Inégalité de Carleman)**.** *Soit une série convergente $\sum u_n$ à termes positifs. Posons $v_n = (u_1 \dots u_n)^{1/n}$. La série $\sum v_n$ converge et*

$$\sum_{n\geqslant 1} v_n \leqslant e \sum_{n\geqslant 1} u_n.$$

Démonstration. Constatons déjà qu'une décomposition en éléments simples donne, si $n \geqslant 1$,

$$\frac{1}{n} = \sum_{k\geqslant n} \frac{1}{k(k+1)}.$$

Le théorème de Fubini-Tonelli permet alors d'écrire

$$\sum_{n\geqslant 1} u_n = \sum_{n\geqslant 1} nu_n \sum_{k\geqslant n} \frac{1}{k(k+1)} = \sum_{k\geqslant 1} \frac{1}{k(k+1)} \sum_{n\leqslant k} nu_n.$$

L'inégalité arithmético-géométrique fournit l'inégalité

$$\frac{1}{k} \sum_{n\leqslant k} nu_n \geqslant (1 \cdot u_1 \times \dots k \cdot u_k)^{1/k} = (k!)^{1/k} v_k$$

pour tout $k \geqslant 1$, dont découle l'inégalité

$$\sum_{n\geqslant 1} u_n \geqslant \sum_{k\geqslant 1} \frac{(k!)^{1/k}}{k+1} v_k.$$

Enfin, grâce à une comparaison série-intégrale, on a pour tout $k \geqslant 1$

$$\sum_{j=1}^{k+1} \log j \geqslant \int_0^{k+1} \log x \,\mathrm{d}x = k\log(k+1) - (k+1) + \log(k+1),$$

soit

$$\log(k!) \geqslant k\log(k+1) - k - 1 \geqslant k\log(k+1) - k,$$

et donc

$$\frac{(k!)^{1/k}}{k+1} \geqslant \frac{1}{e},$$

ce qui conclut. □

Remarque 2. La constante e est optimale : si C est une autre constante satisfaisant l'inégalité de Carleman pour toute suite, on aurait, en considérant la suite $u^{(N)} = (\frac{1}{n}\mathbf{1}_{n\leqslant N})$,

$$\sum_{n\geqslant 1} u_n^{(N)} \sim \log N,$$

et $v_n^{(N)} = (n!)^{-1/n} \sim \frac{e}{n}$, donc

$$\sum_{n\geqslant 1} v_n^{(N)} \sim e \log N.$$

Nécessairement, $C \geqslant e$.

Corollaire 3. *Soient deux suites (a_n), et (b_n) à termes strictement positifs, telles que pour tout $n \geqslant 0$, $a_n \leqslant b_n$ et*

$$b_n^{n+1} \leqslant b_0 b_{n+1}^n.$$

Si de plus $\sum \frac{a_n}{a_{n+1}}$ converge alors $\sum \frac{b_n}{b_{n+1}}$ aussi.

Démonstration. On va montrer que

$$\sum \frac{a_n}{a_{n+1}} < \infty \Longrightarrow \sum (a_n)^{-1/n} < \infty,$$

et

$$\sum (b_n)^{-1/n} < \infty \Longrightarrow \sum \frac{b_n}{b_{n+1}} < \infty,$$

ce qui conclura vu que pour tout n, $b_n^{-1/n} \leqslant a_n^{-1/n}$.

Pour la première implication, on applique l'inégalité de Carleman à $u_n = \frac{a_{n-1}}{a_n}$, qui donne

$$\sum a_0^{1/n} a_n^{-1/n} = \sum (u_0 \dots u_n)^{1/n} \leqslant e \sum u_n < \infty,$$

donc, puisque $a_0^{1/n} \to 1$, $\sum (a_n)^{-1/n} < \infty$.

Pour la seconde implication, on utilise simplement l'hypothèse sur (b_n) qui donne l'inégalité

$$\frac{b_n}{b_{n+1}} \leqslant \underbrace{a_0^{1/(n+1)}}_{\to 1} a_{n+1}^{-1/(n+1)}.$$

□

37. Inégalité de Hoeffding

Référence V. Stein, G. Stoltz, *Statistiques en action.*

Leçons

— 239. Fonctions définies par une intégrale dépendant d'un paramètre. Exemples et applications

On peut ajouter la démonstration de la loi des grands nombres pour les variables de bornées ou le résultat plus fort suivant.

Proposition 1. *Si (X_n) désigne une suite de variables aléatoires iid centrées et telles que presque sûrement $a \leqslant X_i \leqslant b$ alors presque sûrement*

$$\limsup \frac{1}{\sqrt{n \log n}} \left| \sum_{k=1}^{n} X_k \right| \leqslant \frac{b-a}{\sqrt{2}}.$$

Démonstration. Il s'agit d'utiliser le lemme de Borel-Cantelli. Déjà l'inégalité de Hoeffding donne, pour tout $t > 0$,

$$P\left(\left| \sum_{k=1}^{n} X_k \right| \geqslant t \right) \leqslant 2 \exp\left(-\frac{2t^2}{n(b-a)^2} \right).$$

En l'appliquant à $t_n = \sqrt{n \log n} \left(\frac{b-a}{\sqrt{2}} + \epsilon \right)$ (pour un $\epsilon > 0$ quelconque), on obtient

$$P\left(\left| \sum_{k=1}^{n} X_k \right| \geqslant t_n \right) \leqslant 2 \exp\left(-\frac{2t_n^2}{n(b-a)^2} \right) = 2n^{-\left(1+\sqrt{2}\epsilon/(b-a)\right)^2},$$

qui est le terme général d'une série sommable. Aussi le lemme de Borel-Cantelli assure-t-il que

$$P\left(\limsup \left\{ \left| \sum_{k=1}^{n} X_k \right| \geqslant t_n \right\} \right) = 0,$$

c'est-à-dire que presque sûrement

$$\limsup \frac{1}{\sqrt{n \log n}} \left| \sum_{k=1}^{n} X_k \right| \leqslant \frac{b-a}{\sqrt{2}} + \epsilon.$$

Ceci étant vrai pour tout $\epsilon > 0$ on obtient que presque sûrement

$$\limsup \frac{1}{\sqrt{n \log n}} \left| \sum_{k=1}^{n} X_k \right| \leqslant \frac{b-a}{\sqrt{2}}.$$

(la probabilité d'une limite décroissante d'événements (ici on fait tendre ϵ vers 0) est le limite décroissante de leur probabilité). □

38. Équation de la chaleur sur le cercle

Référence Dym et McKean *Fourier series and integrals*

Leçons

- 209. Approximation d'une fonction par des polynômes et des polynômes trigonométriques. Exemples et applications
- 213. Espaces de Hilbert. Bases hilbertiennes. Exemples et applications
- 222. Exemples d'équations aux dérivées partielles linéaires
- 235. Problèmes d'interversion de limites et d'intégrales
- 246. Séries de Fourier. Exemples et applications
- 247. Exemples de problèmes d'interversion de limites

On note $\mathbf{T} = \mathbf{R}/2\pi\mathbf{Z}$.

Théorème 1. *Soit f une fonction continue sur $\mathbf{T}$. Il existe une fonction continue $u : \mathbf{T} \times \mathbf{R}_+ \to \mathbf{R}$, de classe C^∞ sur $\mathbf{T} \times \mathbf{R}_+^*$, et solution de l'équation*

$$\begin{cases} \partial_t u = \partial_{xx} u, \\ u(\cdot, 0) = f. \end{cases} \tag{7}$$

Démonstration. 1. Unicité : Supposons que u soit une telle fonction. Pour tout $t > 0$, $u(\cdot, t)$ est une fonction de classe C^1 sur $\mathbf{T}$: elle est donc somme de sa série de Fourier. Considérons ses coefficients de Fourier

$$c_n(t) = \frac{1}{2\pi} \int_0^{2\pi} u(x,t) e^{-\mathrm{i}\, nx} \, \mathrm{d}x, \qquad n \in \mathbf{Z}.$$

Dérivant sous l'intégrale, on obtient que $t \mapsto c_n(t)$ est C^1 et

$$c_n'(t) = \frac{1}{2\pi} \int_0^{2\pi} \partial_t u(x,t) e^{-\mathrm{i}\, nx} \, \mathrm{d}x = \frac{1}{2\pi} \int_0^{2\pi} \partial_{xx} u(x,t) e^{-\mathrm{i}\, nx} \, \mathrm{d}x.$$

Puis une intégration par partie fournit

$$c_n'(t) = -n^2 c_n(t).$$

Utilisant la continuité de u, on a donc pour tout $t \geqslant 0$

$$c_n(t) = c_n(f) e^{-n^2 t},$$

assurant l'unicité de u : si $t > 0$

$$u(x,t) = \sum_{n \in \mathbf{Z}} c_n(f) e^{\mathrm{i}\, nx - n^2 t}. \tag{8}$$

2. Existence (étude sur $]0, \infty[$) : Définissons u par l'expression (8). Comme la suite $(c_n(f))$ est bornée, cette série et les séries des dérivées partielles convergent uniformément sur $\mathbf{T} \times [a, \infty[$ pour tout $a > 0$, et définit donc une fonction C^∞ sur $\mathbf{T} \times \mathbf{R}_+^*$ satisfaisant à l'équation

$$\partial_t u = \partial_{xx} u.$$

Il s'agit d'établir que cette fonction, prolongée par $u(\cdot, 0) = f$, est continue en $t = 0$.

3. Continuité en $t = 0$ pour f de classe C^2 : Si f est de classe C^2, alors $\sum |c_n(f)| < \infty$ donc la série

(8) converge normalement sur $\mathbf{T} \times \mathbf{R}_+$. Par suite sa somme est continue, et coïncide avec f en $t = 0$.

4. Principe du maximum : Supposons que f soit une fonction positive de classe C^2, et établissons que u ne prend aussi que des valeurs positives. Par l'absurde, supposons que $u(x_0, t_0) < 0$ pour un certain $(x_0, t_0) \in \mathbf{T} \times \mathbf{R}_+$. Évidemment dans ce cas $t_0 > 0$. Fixons $\beta < 0$ quelconque. La fonction continue $v : (x, t) \mapsto u(x, t)e^{\beta t}$ admet un minimum global sur le compact $\mathbf{T} \times [0, t_0]$, qui est donc strictement négatif. Considérons un point (x_1, t_1) où il est atteint. Nécessairement

$$\begin{cases} \partial_t v(t_1, x_1) = \beta e^{\beta t_1} u(x_1, t_1) + e^{\beta t_1} \partial_t u(x_1, t_1) \leqslant 0, \\ \partial_{xx} v(x_1, t_1) = e^{\beta t_1} \partial_{xx} u(x_1, t_1) \geqslant 0. \end{cases}$$

C'est incompatible avec le fait que $u(x_1, t_1) < 0$. Finalement u est une fonction positive.

5. Norme du noyau de la chaleur : Introduisons le noyau de la chaleur défini pour $(x, t) \in \mathbf{T} \times]0, \infty[$ par

$$p_t(x) = \sum_{n \in \mathbf{Z}} e^{\mathrm{i}\, nx - n^2 t},$$

de sorte que pour tout $t > 0$, p_t soit une fonction continue et $u(\cdot, t) = p_t \star f$. La suite des noyaux de Féjer K_N est une approximation de l'unité, donc pour tout $t > 0$,

$$p_t \star K_N \underset{N \to \infty}{\longrightarrow} p_t,$$

uniformément sur $\mathbf{T}$. Par ailleurs comme K_N est de classe C^2, le point précédent donne $p_t \star K_N \geqslant 0$. Ainsi pour tout $(x, t) \in \mathbf{T} \times]0, \infty[$, $p_t(x) \geqslant 0$. Par suite $\|p_t\|_1 = c_0(p_t) = 1$ si $t > 0$.

6. Continuité en $t = 0$ pour f continue : Si $t > 0$, $|u(x, t)| = |p_t \star f(x)| \leqslant \|p_t\|_1 \|f\|_\infty = \|f\|_\infty$. Si $t = 0$ aussi. Ainsi, si f est continue, u est bornée et $\|u\|_\infty \leqslant \|f\|_\infty$. On dispose donc d'un opérateur (continu)

$$\Delta : \left| \begin{array}{ccc} C(\mathbf{T}) & \longrightarrow & L^\infty(\mathbf{T} \times \mathbf{R}_+) \\ f & \longmapsto & u \end{array} \right. .$$

Comme $\Delta(C^2(\mathbf{T})) \subset C(\mathbf{T} \times \mathbf{R}_+)$, et que $C = C(\mathbf{T} \times \mathbf{R}_+)$ est un fermé de $L^\infty(\mathbf{T} \times \mathbf{R}_+)$, $\Delta^{-1}(C)$ est un fermé de $C(\mathbf{T})$ contenant $C^2(\mathbf{T})$, c'est donc $C(\mathbf{T})$ (théorème de Stone-Weierstrass). Autrement dit pour toute fonction $f \in C(\mathbf{T})$, $\Delta(f)$ est une fonction continue. □

39. Espérance conditionnelle et convergence L^p

Référence Aucune à ma connaissance (d'après un document de Pierre Bertin)

Leçons

- 202. Exemples de parties denses et applications
- 234. Espaces L^p, $1 \leqslant p \leqslant +\infty$
- 235. Problèmes d'interversion de limites et d'intégrales

Soit $p \geqslant 1$ et X une variable aléatoire définie sur un espace probabilisé $(\Omega, \mathcal{F}, P)$

Théorème 1. *Si $(\mathcal{F}_n)$ est une filtration de sous-tribus de $\mathcal{F}$, et $\mathcal{F}_\infty = \bigvee_{n\geqslant 1} \mathcal{F}_n$, alors*

$$E[X|\mathcal{F}_n] \xrightarrow[n\to\infty]{L^p} E[X|\mathcal{F}_\infty].$$

Théorème 2. *Soit $\mathcal{A}_n$ une famille de sous-tribus de $\mathcal{F}$ indépendantes. Posant $\mathcal{G}_n = \sigma(\mathcal{A}_k, k \geqslant n)$, on a*

$$E[X|\mathcal{G}_n] \xrightarrow[n\to\infty]{L^p} E[X].$$

Lemme 3. *Soit E un espace vectoriel normé et B une partie dense de E. Si (T_n), T sont des opérateurs de E tels que*

$$\sup_n \|T_n\| < \infty,$$

et pour tout $x \in B$,

$$T_n(x) \longrightarrow T(x),$$

alors cette dernière convergence a lieu pour tout $x \in E$.

Démonstration du lemme 3. Fixons $x \in E$, et $\epsilon > 0$. Donnons-nous un élément y de B tel que $\|x - y\| \leqslant \epsilon$, et $N \geqslant 1$ tel que pour tout $n \geqslant N$ on ait $\|T_n(y) - T(y)\| \leqslant \epsilon$. On a, si $n \geqslant N$,

$$\|T_n(x) - T(x)\| \leqslant \epsilon(\sup_n \|T_n\| + \|T\|) + \epsilon,$$

concluant la preuve. □

Lemme 4. *Si $\mathcal{G}_n$ est une suite de sous-tribus de $\mathcal{F}$, alors* $\mathrm{Vect}\,(\mathbf{1}_A\,;\, A \in \mathcal{G}_n, n \geqslant 1)$ *est dense dans $L^p(\mathcal{G}_\infty)$.*

Démonstration du lemme 4. Notons $W = \mathrm{Vect}\,(\mathbf{1}_A\,;\, A \in \mathcal{G}_n, n \geqslant 1)$ et considérons

$$\mathcal{C} = \{A \in \mathcal{F} \,:\, \mathbf{1}_A \in \overline{W}\}.$$

Bien évidemment, $\mathcal{C}$ contient $\bigcup_n \mathcal{G}_n$, qui forme une partie de $\mathcal{F}$ stable par intersection finie et contenant Ω. Par ailleurs $\mathcal{C}$ est stable par différence ordonnée : si $A \subset B$ sont des éléments de $\mathcal{C}$ alors $\mathbf{1}_A \in \overline{W}$, et $\mathbf{1}_B \in \overline{W}$, donc $\mathbf{1}_{B\setminus A} = \mathbf{1}_B - \mathbf{1}_A \in \overline{W}$, c'est-à-dire $B\setminus A \in \mathcal{C}$. Par ailleurs, si (A_n) est une suite croissante d'éléments de $\mathcal{C}$, soit $\epsilon > 0$ et N tel que $P(A_N) \geqslant P(\bigcup_{n\geqslant 0} A_n) - \epsilon$, en particulier

$$\|\mathbf{1}_{A_N} - \mathbf{1}_{\bigcup A_n}\| \leqslant \epsilon^{1/p}.$$

Comme pour tout N, $\mathbf{1}_{A_N} \in \bar{W}$, $\mathbf{1}_{\bigcup A_n} \in \bar{W}$ aussi. Finalement $\mathcal{C}$ est une classe monotone. Le théorème des classes monotones conclut. □

Démonstration du théorème 1. Considérons

$$T_n : \begin{array}{ll} L^p & \to L^p \\ Y & \mapsto E[Y|\mathcal{F}_n] \end{array},$$

et

$$T : \begin{array}{ll} L^p & \to L^p \\ Y & \mapsto E[Y|\mathcal{F}_\infty] \end{array}.$$

La convergence du théorème a lieu pour les $\mathbf{1}_A$ pour $A \in \mathcal{F}_m$: si $n \geqslant m$,

$$E[\mathbf{1}_A|\mathcal{F}_n] = \mathbf{1}_A = E[\mathbf{1}_A|\mathcal{F}_\infty].$$

D'après le lemme 3, dont les hypothèses sont ici satisfaites, et au lemme 4, la convergence du théorème a donc lieu pour toute variable aléatoire Y qui soit $\mathcal{F}_\infty$-mesurable. Ainsi pour notre variable X

$$E[X|\mathcal{F}_n] = E[E[X|\mathcal{F}_\infty]|\mathcal{F}_n] \xrightarrow[n\to\infty]{L^p} E[E[X|\mathcal{F}_\infty]|\mathcal{F}_\infty] = E[X|\mathcal{F}_\infty].$$

□

Démonstration du théorème 2. Considérons

$$T_n : \begin{array}{ll} L^p & \to L^p \\ Y & \mapsto E[Y|\mathcal{G}_n] \end{array},$$

et

$$T : \begin{array}{ll} L^p & \to L^p \\ Y & \mapsto E[Y] \end{array}.$$

La convergence du théorème a lieu pour les $\mathbf{1}_A$ pour $A \in \mathcal{A}_m$: si $n > m$,

$$E[\mathbf{1}_A|\mathcal{G}_n] = E[\mathbf{1}_A].$$

D'après le lemme 3, dont les hypothèses sont ici satisfaites, et au lemme 4, la convergence du théorème a donc lieu pour toute variable aléatoire Y qui soit $\mathcal{A}_\infty = \bigvee_{n\geqslant 1} \mathcal{A}_n$-mesurable. Ainsi pour notre variable X

$$E[X|\mathcal{G}_n] = E[E[X|\mathcal{A}_\infty]|\mathcal{G}_n] \xrightarrow[n\to\infty]{L^p} E[E[X|\mathcal{A}_\infty]] = E[X].$$

□

40. Existence de géodésiques.

Référence Aucune (d'après un document de Patrick Bernard).

Leçons

— 203. Utilisation de la notion de compacité

— 219. Extremums : existence, caractérisation, recherche. Exemples et applications

Définition 1. Une fonction réelle f définie sur un espace topologique E est semi-continue inférieurement (sci) si ses sous-niveaux $\{f \leqslant C\}$ sont fermés.

Proposition 2. *Un suprémum de fonctions semi-continues inférieurement l'est.*

Proposition 3. *Une fonction sci sur un compact admet un minimum.*

Soit K un espace métrique compact. Pour tout $\gamma \in C([0,1],K)$, on note

$$\ell(\gamma) = \sup_n \sup_{0\leqslant t_0\leqslant\ldots\leqslant t_n\leqslant 1} \sum_{i=0}^{n-1} \mathrm{d}(\gamma(t_i),\gamma(t_{i+1}))$$

sa longueur.

Théorème 4. *S'il existe un chemin de longueur finie entre deux points de K, il existe un chemin de longueur minimale les reliant.*

Le théorème suit immédiatement des trois lemmes suivant.

Lemme 5. *Si γ est de longueur est un chemin continu de longueur finie L, alors il existe une chemin continu de longueur inférieure, $L-$-lipschitz*

On munit $C([0,1],K)$ de la norme de la convergence uniforme.

Lemme 6. *Si $L>0$, l'ensemble $\{\gamma \in C([0,1],K)$ L-lipschitz$\}$ est compact.*

Lemme 7. *La fonction longueur*

$$\ell : \left| \begin{array}{ccc} C([0,1],K) & \longrightarrow & \mathbf{R} \\ \gamma & \longmapsto & \ell(\gamma) \end{array} \right.$$

est semi-continue inférieurement.

Démonstration du lemme 6. C'est une conséquence du théorème d'Ascoli. □

Démonstration du lemme 7. C'est une conséquence de la proposition 2. □

Démonstration du lemme 5. C'est la partie délicate. L'idée est de faire une nouvelle paramétrisation du chemin de longueur finie γ. On étend la définition de longueur aux chemins non continus, et paramétrés par un autre segment que $[0,1]$. Dés lors la longueur de la concaténation de deux chemins est la somme de leurs longueurs.

Considérons l'application

$$\tau : \left| \begin{array}{ccc} [0,1] & \longrightarrow & \mathbf{R} \\ t & \longmapsto & \frac{\ell(\gamma_{|[0,t]})}{\ell(\gamma)} \end{array} \right. .$$

Elle est croissante. Établissons sa continuité, sa continuité à droite par exemple. Soit $t_0 \in [0,1[$, et $\epsilon > 0$. Par définition il existe $t_0 < t_1 \leqslant \ldots \leqslant t_n$ tels que

$$\ell(\gamma_{|[t_0,1]}) \leqslant \sum_{i=0}^{n-1} \mathrm{d}(\gamma(t_i), \gamma(t_{i+1})) + \epsilon.$$

Ainsi si $s \in [t_0, t_1]$, l'inégalité triangulaire donne

$$\ell(\gamma_{|[t_0,1]}) \leqslant \mathrm{d}(\gamma(t_0), \gamma(s)) + \mathrm{d}(\gamma(s), \gamma(t_1)) + \sum_{i=1}^{n-1} \mathrm{d}(\gamma(t_i), \gamma(t_{i+1})) + \epsilon \leqslant \mathrm{d}(\gamma(t_0), \gamma(s)) + \ell(\gamma_{|[s,1]}) + \epsilon,$$

qui donne la continuité à droite. Pour la continuité à gauche, on constate qu'elle équivaut à la continuité à droite pour le chemin retourné.

Considérons son inverse à droite $f(t) = \min\{s \in [0,1] \,:\, \tau(s) = t\}$, de sorte que $\tau \circ f = Id$. Enfin posons $\tilde{\gamma} = \gamma \circ f$. Certes f n'est pas continue, mais on va voir que $\tilde{\gamma}$ l'est. Si $s \leqslant t$,

$$\begin{aligned}
\ell(\tilde{\gamma}_{|[s,t]}) &\leqslant \ell(\gamma_{|[f(s),f(t)]}) \\
&= \ell(\gamma_{|[0,f(t)]}) - \ell(\gamma_{|[0,f(s)]}) \\
&= \ell(\gamma)\tau \circ f(t) - \ell(\gamma)\tau \circ f(s) \\
&= \ell(\gamma)(t-s).
\end{aligned}$$

A fortiori

$$\mathrm{d}(\tilde{\gamma}(s), \tilde{\gamma}(t)) \leqslant \ell(\tilde{\gamma}_{|[s,t]}) \leqslant \ell(\gamma)(t-s).$$

Ainsi le chemin $\tilde{\gamma}$ est $\ell(\gamma)-$lipschitz. □

41. Lemme d'Artin, $\int_0^1 \log\Gamma$ et formules de multiplication.

Référence A. Chambert-Loir, D. Firmigier, *tome2*

Leçons

- 229. Fonctions monotones. Fonctions convexes. Exemples et applications
- 236. Illustrer par des exemples quelques méthodes de calcul d'intégrales de fonctions d'une ou plusieurs variables réelles
- 239. Fonctions définies par une intégrale dépendant d'un paramètre. Exemples et applications

Théorème 1 (Lemme d'Artin)**.** *Si $F :]0,\infty[\to]0,\infty[$ est logarithmiquement convexe et satisfait pour tout $x > 0$, $F(x+1) = xF(x)$, alors pour tout $x > 0$, $F(x) = F(1)\Gamma(x)$.*

Démonstration. En tant que fonction logarithmiquement convexe, F est continue et dérivable à gauche en tout point. Considérons $H = \frac{F}{\Gamma}$. Vue la relation $F(x+1) = xF(x)$, H est une fonction 1-périodique. Calculons sa dérivée logarithmique à gauche (nous noterons δ les dérivées à gauche) :

$$\frac{\delta H}{H} = \frac{\delta F}{F} - \frac{\Gamma'}{\Gamma}.$$

Puisque Γ et F sont logarithmiquement convexe, les fonctions $\frac{\delta F}{F}$ et $\frac{\Gamma'}{\Gamma}$ sont croissantes. Ainsi si $x \in [n, n+1[$,

$$\frac{\delta F}{F}(n) - \frac{\Gamma'}{\Gamma}(n+1) \leqslant \frac{\delta H}{H}(x) \leqslant \frac{\delta F}{F}(n+1) - \frac{\Gamma'}{\Gamma}(n).$$

Mais $\frac{\Gamma'}{\Gamma}(n+1) = \frac{\Gamma'}{\Gamma}(n) + \frac{1}{n}$, donc,

$$\frac{\delta H}{H}(n) - \frac{1}{n} \leqslant \frac{\delta H}{H}(x) \leqslant \frac{\delta H}{H}(n+1) + \frac{1}{n}.$$

Comme H est 1-périodique, pour tout $x \in]0,\infty[$,

$$\frac{\delta H}{H}(1) - \frac{1}{n} \leqslant \frac{\delta H}{H}(x) \leqslant \frac{\delta H}{H}(1) + \frac{1}{n}.$$

Ainsi laissant n tendre vers $+\infty$, on obtient que $\frac{\delta H}{H}(x)$ est constante, donc que $\log H$ est affine. S'agissant d'une fonction périodique, elle est constante. □

Corollaire 2 (Formule de multiplication)**.** *Soit p un entier naturel non nul. Notons $C_p = \Gamma(1/p)\dots\Gamma((p-1)/p)$. On a pour tout $x > 0$*

$$p^x \Gamma\left(\frac{x}{p}\right)\Gamma\left(\frac{x+1}{p}\right)\dots\Gamma\left(\frac{x+(p-1)}{p}\right) = p\,C_p\,\Gamma(x).$$

Démonstration. La fonction

$$F : x \mapsto p^x \Gamma\left(\frac{x}{p}\right)\Gamma\left(\frac{x+1}{p}\right)\dots\Gamma\left(\frac{x+(p-1)}{p}\right)$$

est logarithmiquement convexe (son logarithme est somme de fonctions convexe) et satisfait $F(x+1) = xF(x)$. □

Proposition 3. *On a*

$$\int_0^1 \log\Gamma = \log\sqrt{2\pi},$$

et

$$C_p = \Gamma(1/p)\dots\Gamma((p-1)/p) = \frac{1}{\sqrt{p}}(2\pi)^{(p-1)/2}.$$

Démonstration. La fonction $\log\Gamma$ est continue sur $]0,1]$, et $\log\Gamma(x) \sim_{x\to 0} -\log x$. Par conséquent $\log\Gamma$ est intégrable sur $]0,1]$. Soit $p \geqslant 2$. Vu le corollaire précédent, on a

$$\log p \int_0^1 x\,\mathrm{d}x + \underbrace{\sum_{k=0}^{p}\int_0^1 \log\Gamma\left(\frac{x+k}{p}\right)\mathrm{d}x}_{=p\int_0^1\log\Gamma} = \log p + \log C_p + \int_0^1 \log\Gamma.$$

Pour $p = 2$, on sait que $C_2 = \sqrt{\pi}$: on obtient

$$\int_0^1 \log\Gamma = \log\sqrt{2\pi}.$$

Pour $p \geqslant 3$, on peut donc calculer C_p :

$$\log C_p = (p-1)\log\sqrt{2\pi} - \frac{1}{2}\log p,$$

c'est-à-dire

$$C_p = \frac{1}{\sqrt{p}}(2\pi)^{(p-1)/2}.$$

□

Remarque 4. Si l'on disposait déjà de l'expression de C_p pour tout entier p, on pouvait calculer $\int_0^1 \log\Gamma$, grâce à une somme de Riemann :

$$\int_0^1 \log\Gamma = \lim_{p\to\infty}\frac{1}{p}\sum_{k=1}^{p}\log\Gamma(k/p) = \lim_{p\to\infty}\frac{1}{p}\log C_p = \frac{1}{2}\log(2\pi).$$

42. Théorème de Joris

Référence RMS 2005

Leçons

- 124 Anneau des séries formelles. Applications ;
- 207 Prolongement de fonctions. Exemples et applications
- 218. Applications des formules de Taylor
- 228. Continuité et dérivabilité des fonctions réelles d'une variable réelle. Exemples et contre-exemples

Définition 1. Soit A un anneau commutatif et $B \subset A$ un pseudo sous-anneau. On dit que B vérifie $(\star)$ si pour tout $a \in A$,

$$[\forall r \geqslant 2,\ a^r \in B] \Longrightarrow a \in B.$$

Théorème 2 (Lemme de transfert)**.** *Si $B \subset A$ vérifie $(\star)$ alors $B[[X]] \subset A[[X]]$ aussi.*

Théorème 3. *Soit f une fonction $\mathbf{R} \to \mathbf{R}$. Si pour tout $n \geqslant 2$, f^n est C^∞ alors f est elle-même C^∞.*

Lemme 4. *Si $g \in C^\infty(\mathbf{R}, \mathbf{R})$ et $g(a) = \ldots = g^{(n-1)}(a) = 0$, alors il existe une fonction $h \in C^\infty(\mathbf{R}, \mathbf{R})$ telle que pour tout $x \in \mathbf{R}$, $g(x) = (x-a)^n h(x)$, et $h(a) = \frac{g^{(n)}(a)}{n!}$.*

Démonstration. Écrivons la formule de Taylor avec reste intégral en 0 : pour tout $x \in \mathbf{R}$,

$$g(x) = \int_a^x \frac{(x-t)^{n-1}}{(n-1)!} g^{(n)}(t)\,\mathrm{d}t = (x-a)^n \underbrace{\int_0^1 \frac{(1-t)^{n-1}}{(n-1)!} g^{(n)}(a+(x-a)t)\,\mathrm{d}t}_{h(x)}.$$

Un théorème de régularité des intégrales à paramètres assure que h est C^∞. □

Lemme 5. *Soit D est un ouvert de $\mathbf{R}$, et f, g des fonctions continues sur $\mathbf{R}$ satisfaisant*

1. *f est dérivable sur D et pour tout $x \in D$, $f'(x) = g(x)$;*
2. *$f = 0$ sur D^c ;*
3. *$g = 0$ sur D^c.*

Sous ces conditions $f \in C^1(\mathbf{R})$ et $f' = g$.

Démonstration. Fixons $x \in D^c$, et considérons le taux d'accroissement

$$\tau(y) = \frac{f(y)}{y-x}.$$

Constatons que $\tau(y) = 0$ si $y \notin D$. Fixons momentanément $y \in D$. Sans restriction on peut supposer $y \geqslant x$. Soit $]\alpha, \beta[$ la composante connexe de y dans D. On a

$$|f(y)| = |f(y) - f(\alpha)| \leqslant \sup_{[\alpha,y]} |g||y-\alpha| \leqslant \sup_{[x,y]} |g||y-x|.$$

Finalement pour tout $y \in \mathbf{R}$, $|\tau(y)| \leqslant \sup_{[x,y]} |g|$, qui tend vers 0 lorsque $y \to x$ car g est continue et $g(0) = 0$. Ceci assure que f est dérivable en x et que $f'(x) = 0 = g(x)$ pour tout $x \in D^c$. □

Si $g \in C(\mathbf{R}, \mathbf{R})$, on note

$$P(g) = \left\{ a \in \mathbf{R} \,:\, \forall \gamma > 0,\ \frac{|g(a)|}{|x-a|^\gamma} \underset{x \to a}{\to} 0 \right\},$$

l'ensemble des «points plats» de g.

Lemme 6. *On a les propriétés élémentaires suivantes*

1. *Si $a \in P(g)$ alors $g(a) = 0$;*
2. *Pour tout $k \geqslant 1$, $P(g^k) = P(g)$;*
3. *Si g est de classe C^∞ alors $P(g) = \bigcap_{n \geqslant 0} (g^{(n)})^{-1}(0)$. C'est en particulier une partie fermée de $\mathbf{R}$.*

Démonstration. Le troisième point découle de la formule de Taylor–Young. □

Démonstration du théorème. 1. Continuité et points plats. Comme $f = \sqrt[3]{f^3}$, c'est une fonction continue. Comme f^n est C^∞, $P(f) = P(f^n)$ est une partie fermée de $\mathbf{R}$. Considérons l'ouvert $D = P(f)^c$.

2. f est C^∞ sur D. Si $a \in D$, il existe $k \geqslant 0$ tel que $(f^2)^{(k)}(a) \neq 0$, et ainsi, avec le lemme 4, $f^2(x) = (x-a)^k g_2(x)$ pour une fonction $g_2 \in C^\infty(\mathbf{R})$ telle que $g_2(a) \neq 0$. De même $f^3(x) = (x-a)^l g_3(x)$, pour un $l \geqslant 0$ et une fonction C^∞ g_3 ne s'annulant pas en a. Ainsi au voisinage de a,

$$f(x) = \frac{f^3(x)}{f^2(x)} = (x-a)^{l-k} \frac{g_3(x)}{g_2(x)}.$$

Puisque f est continue (en a), on a nécessairement $l \geqslant k$. Ainsi f est C^∞ au voisinage de a.

3. Vers l'utilisation du lemme de transfert. Considérons l'anneau $A = C(D)$ et son pseudo sous-anneau

$$B = \{ g_{|D} \,:\, g \in C(\mathbf{R}) \text{ et } g_{|D^c} = 0 \}.$$

L'inclusion $B \subset A$ satisfait $(\star)$: Si $f^r = g_{|D}$ alors $f = \sqrt[r]{g^r}|_D$ pour r impair. Ainsi, d'après le lemme de transfert, $B[[X]] \subset A[[X]]$ satisfait $(\star)$ aussi.

3. Un morphisme d'anneaux. Considérons le morphisme d'anneaux

$$J : \begin{array}{ll} C^\infty(D) & \longrightarrow A[[X]] \\ g & \longmapsto \sum \frac{g^{(n)}}{n!} X^n \end{array}.$$

On a pour tout $r \geqslant 2$, $J(f_{|D})^r = J({f_{|D}}^r) \in B[[X]]$ donc $J(f_{|D}) \in B[[X]]$. Soient des fonctions $g_n \in C(\mathbf{R})$ telles que pour tout $n \in \mathbf{N}$, $g_{n\,|D} = f^{(n)}|_D$, et $g_{n\,|D^c} = 0$.

4. Conclusion. Grâce au lemme 5, une récurrence donne $f \in C^n(\mathbf{R})$ pour tout $n \in \mathbf{N}$, et $f^{(n)} = g_n$. □

43. Inégalité de Gross

Référence : Massart, *Concentration inequalities and model selection : Ecole d'été de probabilités de Saint-Flour XXXIII*, 2003

Leçons :

- 235. Problèmes d'interversion de limites et d'intégrales
- 249. Suites de variables de Bernoulli indépendantes
- 260. Espérance, variance et moments d'une variable aléatoire
- 263. Variables aléatoire à densité. Exemples et applications
- 264. Variables aléatoire discrètes. Exemples et applications

On admettra le théorème suivant, dont on donne ici une démonstration.

Théorème 1 (Inégalité d'Efron–Stein)**.** *Soient $X_1, \dots, X_n$ des variables aléatoires indépendantes, f une fonction mesurable sur $\mathbf{R}^n$. On note $\hat{X}_i = (X_j, j \neq i)$. Si $Z = f(X_1, \dots, X_n)$ est de carré intégrable, alors*

$$\mathrm{Var}(Z) \leqslant \sum_{i=1}^{n} E[\mathrm{Var}(Z|\hat{X}_i)].$$

Démonstration. On commence par «désymétriser» le problème, en considérant la tribu $\mathbf{F}_i = \sigma(X_1, \dots, X_i)$, et en posant

$$\Delta_i = E_i[Z] - E_{i-1}[Z].$$

On constate que si $i \neq j$, alors $j - i \geqslant i$, donc

$$E[\Delta_i \Delta_j] = E[E_{j-1}[\Delta_i \Delta_j]] = E[\Delta_i \underbrace{E_{j-1}[\Delta_j]}_{=0}] = 0.$$

Or on a

$$\sum_{i=1}^{n} \Delta_i = Z - E[Z].$$

Ainsi

$$\mathrm{Var}(Z) = \sum_{i=1}^{n} E[\Delta_i^2].$$

Afin de majorer $E[\Delta_i^2]$, on resymétrise :

$$\begin{aligned} E[\Delta_i^2] &= E[(E_i[Z] - E_{i-1}[Z])^2] \\ &= E\left[\left(E_i[Z - E[Z|\hat{X}_i]]\right)^2\right] \\ &\leqslant E\left[E_i\left[\left(Z - E[Z|\hat{X}_i]\right)^2\right]\right] \qquad \text{(inégalité de Jensen)} \\ &= E[\mathrm{Var}(Z|\hat{X}_i)]. \end{aligned}$$

□

Théorème 2 (Inégalité de Gross)**.** *Soient $X_1, \dots, X_n$ des variables aléatoires* i.i.d. *de loi gaussienne $\mathcal{N}(0,1)$, et $f : \mathbf{R}^n \to \mathbf{R}$ une fonction de classe C^1. Si $f(X)$ est de carré intégrable, alors*

$$\mathrm{Var}\, f(X) \leqslant E[\|\nabla f(X)\|^2].$$

Démonstration. 1. Grâce à l'inégalité d'Efron–Stein, il suffit de l'établir pour $n = 1$.

2 On commence par traiter le cas où f est C^1 et à support compact. Pour cela donnons-nous une suite (ε_i) de variables aléatoires *i.i.d.* de loi Rad(1/2) et notons $S_N = \frac{1}{\sqrt{N}} \sum_{i=1}^N \varepsilon_i$. Le théorème central limite donne

$$S_N \xrightarrow{\text{loi}} X \sim \mathcal{N}(0,1).$$

On a en particulier

$$\operatorname{Var} f(S_N) \longrightarrow \operatorname{Var} f(X),$$

et

$$E[f'(S_N)^2] \longrightarrow E[f'(X)^2].$$

On va établir que

$$\operatorname{Var} f(S_N) \leqslant E[f'(S_N)^2] + o(1).$$

Soit ε' une copie indépendante de ε, et

$$S'_{N,i} = S_N + \frac{\varepsilon'_i - \varepsilon_i}{\sqrt{N}}.$$

L'inégalité d'Efron–Stein donne

$$\operatorname{Var} f(S_N) \leqslant \frac{1}{2} \sum_{i=1}^N E[(f(S_N) - f(S_{N,i}))^2].$$

S'agissant de variables de Rademacher, on a, en distinguant les cas

$$E[(f(S_N) - f(S_{N,i}))^2] = \frac{1}{2} E\left[\Big(\underbrace{f(S_N) - f\left(S_N - \frac{2\epsilon_i}{\sqrt{N}}\right)}_{f'(S_N)\frac{2}{\sqrt{N}} \pm \frac{2}{\sqrt{N}} \omega_{f'}(2/\sqrt{N})} \Big)^2 \right]$$

Puis

$$E[(f(S_N) - f(S_{N,i}))^2] \leqslant \frac{1}{2} \left(\frac{4}{N} E[f'(S_N)^2] + \frac{1}{N} \underbrace{(\omega_{f'}(2/\sqrt{N})^2 + \omega_{f'}(2/\sqrt{N}) \|f'\|_\infty)}_{o(1)} \right).$$

Ainsi, en sommant,

$$\operatorname{Var}(S_N) \leqslant E[f'(S_N)^2] + o(1)$$

L'inégalité de Gross est donc établie pour les fonctions C^1 à support compact.

3. On établit le théorème pour f quelconque. L'idée est bien entendue d'approcher f par des fonctions C^1 à support compact. Remarquons au préalable que si $E[f'(X)^2] = +\infty$, il n'y a rien à démontrer, on peut donc supposer cette espérance finie. On se donne une suite (ϕ_k) de fonctions plateaux croissant vers 1 (et raisonnablement construites) et on pose $f_k = \phi_k f$. Ce qui précède donne l'inégalité

$$\operatorname{Var}(f_k(X)) \leqslant E[f'_k(X)^2].$$

Montrons que les deux membres de l'inégalité convergent vers les quantités souhaitées. Pour le membre de droite,

$$E[f'_k(X)^2] = E[\phi_k^2 f(X)^2] + E[f^2 \phi'_k(X)^2] + 2E[f(X)f'(X)\phi_k(X)\phi'_k(X)].$$

Les deux derniers termes tendent vers 0 par convergence dominée ; le premier vers $E[f'(X)^2]$ par convergence monotone. Ainsi

$$E[f_k'(X)^2] \longrightarrow E[f'(X)^2].$$

Pour le membre de gauche, comme $f(X)$ est intégrable, $f_k(X)$ l'est aussi et

$$\mathrm{Var}(f_k(X)) = E[f_k(X)^2] - E[f_k(X)]^2.$$

Le premier terme converge, par convergence monotone vers $E[f(X)^2]$. Le second vers $E[f(X)]^2$ par convergence dominée. Aussi a-t-on la convergence

$$\mathrm{Var}(f_k(X)) \longrightarrow \mathrm{Var}(f(X)),$$

qui conclut cette démonstration □

44. Polynômes de Bernstein

Référence C. Zuily, H. Queffélec, *Analyse pour l'agrégation.*

Leçons

- 209. Approximation d'une fonction par des polynômes et des polynômes trigonométriques. Exemples et applications
- 228. Continuité et dérivabilité des fonctions réelles d'une variable réelle. Exemples et contre-exemples
- 249. Suites de variables de Bernoulli indépendantes

Définition 1. Si $f \in C([0,1], \mathbf{R})$, son module de continuité est la fonction définie pour $h > 0$ par

$$\omega(h) = \sup_{|u-v| \leqslant h} |f(u) - f(v)|.$$

Théorème 2. *Soit $f \in C([0,1], \mathbf{R})$. On se donne sur un espace probabilisé des variables aléatoires $S_n^{(x)}$ de loi binomiale de paramètres n et x pour tout $x \in [0,1]$, et on note $B_n f(x) = E[f(\frac{S_n^{(x)}}{n})]$. Il s'agit d'une fonction polynômiale, qui converge uniformément vers f sur $[0,1]$ et satisfait l'estimation*

$$\|f - B_n f\|_\infty \leqslant \frac{3}{2}\omega\left(\frac{1}{\sqrt{n}}\right).$$

En outre il existe une fonction continue f pour laquelle pour tout entier n,

$$\|f - B_n f\|_\infty \geqslant \frac{1}{2\sqrt{e}}\omega\left(\frac{1}{\sqrt{n}}\right).$$

Démonstration. Soit $x \in [0,1]$. On commence par majorer brutalement par inégalité triangulaire :

$$|f(x) - B_n f(x)| \leqslant E\left[\left|f(x) - f\left(\frac{S_n^{(x)}}{n}\right)\right|\right] \leqslant E\left[\omega\left(\left|x - \frac{S_n^{(x)}}{n}\right|\right)\right].$$

On utilise le lemme suivant :

Lemme 3. *Pour tout $h > 0$, et $\lambda \geqslant 0$, $\omega(\lambda h) \leqslant (\lambda + 1)\omega(h)$.*

Démonstration. Soit $u, v \in [0,1]$ tels que $|u - v| \leqslant \lambda h$. Il existe $u_0 = u$, $u_2, \ldots, u_{[\lambda]+1} = v$ tels que pour tout j, $|u_j - u_{j+1}| \leqslant h$. Ainsi

$$|f(u) - f(v)| \leqslant \sum_{j=0}^{[\lambda]} |f(u_j) - f(u_{j+1})| \leqslant ([\lambda] + 1)\omega(h) \leqslant (\lambda + 1)\omega(h).$$

On conclut en prenant le suprémum sur les tels u, v. □

On applique le lemme brutalement avec $h = \frac{1}{\sqrt{n}}$:

$$|f(x) - B_n f(x)| \leqslant E\left[\left(1 + \sqrt{n}\left|x - \frac{S_n^{(x)}}{n}\right|\right)\omega\left(\frac{1}{\sqrt{n}}\right)\right] = \left(1 + \sqrt{n}E\left|x - \frac{S_n^{(x)}}{n}\right|\right)\omega\left(\frac{1}{\sqrt{n}}\right).$$

Or avec l'inégalité de Cauchy-Schwarz, on obtient

$$E\left|x-\frac{S_n^{(x)}}{n}\right| \leqslant E\left[\left(x-\frac{S_n^{(x)}}{n}\right)^2\right]^{1/2} = \sqrt{\frac{x(1-x)}{n}}.$$

Ainsi pour tout $x \in [0,1]$

$$|f(x)-B_nf(x)| \leqslant \left(1+\sqrt{x(1-x)}\right)\omega\left(\frac{1}{\sqrt{n}}\right) \leqslant \frac{3}{2}\omega\left(\frac{1}{\sqrt{n}}\right).$$

Il reste à établir l'optimalité : elle repose soit sur l'inégalité de Khintchine soit sur le théorème central limite. Considérons la fonction définie par $f(x) = |x-1/2|$, qui est 1-lipschitzienne donc satisfait $\omega(h) \leqslant h$. Si $n \geqslant 1$,

$$\|f-B_nf\|_\infty \geqslant |f(1/2)-B_nf(1/2)| = |B_nf(1/2)| = E\left[\left|\frac{S_n^{(1/2)}}{n}-1/2\right|\right] = \frac{1}{2n}E|\epsilon_1+\ldots\epsilon_n|,$$

où les ϵ_j sont des variables de Rademacher centrées indépendantes. L'inégalité de Khintchine donne

$$E|\epsilon_1+\ldots\epsilon_n| \geqslant \frac{1}{\sqrt{e}}E[(\epsilon_1+\ldots\epsilon_n)^2]^{1/2} = \frac{1}{\sqrt{e}}\sqrt{n}.$$

Le théorème central limite donne quant à lui

$$\frac{1}{\sqrt{n}}E|\epsilon_1+\ldots\epsilon_n| \geqslant P(\epsilon_1+\ldots\epsilon_n \geqslant \sqrt{n}) \underset{n\to\infty}{\longrightarrow} \int_1^\infty e^{-x^2/2}\frac{\mathrm{d}x}{\sqrt{2\pi}}.$$

Dans ce dernier cas on a donc

$$\liminf_{n\to\infty}\frac{1}{\sqrt{n}}E|\epsilon_1+\ldots\epsilon_n| > 0,$$

et, ce premier terme n'étant jamais nul,

$$\inf_{n\geqslant 1}\frac{1}{\sqrt{n}}E|\epsilon_1+\ldots\epsilon_n| > 0,$$

Ainsi

$$\|f-B_nf\|_\infty \geqslant \frac{1}{2\sqrt{e}}\frac{1}{\sqrt{n}} \geqslant \frac{1}{2\sqrt{e}}\omega\left(\frac{1}{\sqrt{n}}\right).$$

□

Théorème 4 (Inégalité de Khintchine)**.** *Soient des réels $a_1,\ldots a_n$ et des variables de Rademacher i.i.d. centrées $\epsilon_1,\ldots,\epsilon_n$. On a*

$$E\left|\sum a_j\epsilon_j\right| \geqslant \frac{1}{\sqrt{e}}E\left[\left|\sum a_j\epsilon_j\right|^2\right]^{1/2}.$$

Démonstration. Déjà on peut supposer par homogénéité que $\|\sum a_j\epsilon_j\|_2 = \sum a_j^2 = 1$. On va procéder par dualité : on va choisir un élément $g \in L^\infty$ et écrire

$$\|\sum a_j\epsilon_j\|_1 \geqslant \frac{|E[g\sum a_j\epsilon_j]|}{\|g\|_\infty}.$$

Prenons

$$g = \prod_{j=1}^n(1+\mathrm{i}\,a_j\epsilon_j).$$

Ainsi

$$|g| = \prod \sqrt{1 + a_j^2 \epsilon_j^2} = \prod \sqrt{1 + a_j^2} \leqslant \prod \sqrt{\exp(a_j^2)} = \sqrt{e}.$$

On calcule d'autre part, vue l'indépendance,

$$E[g \sum a_j \epsilon_j] = \sum_{j=1}^{n} a_j E\left[r_j (1 + \mathrm{i}\, a_j r_j) \prod_{k \neq j} (1 + \mathrm{i}\, a_k \epsilon_k) \right] = \sum_{j=1}^{n} a_j \times \mathrm{i}\, a_j = \mathrm{i}\,.$$

Finalement

$$\| \sum a_j \epsilon_j \|_1 \geqslant \frac{|\,\mathrm{i}\,|}{\sqrt{e}} = \frac{1}{\sqrt{e}}.$$

□

45. Principe de localisation

Référence Je ne sais pas... (d'après un document d'Arthur Leclaire)

Leçons

- 209. Approximation d'une fonction par des polynômes et des polynômes trigonométriques. Exemples et applications
- 235. Problèmes d'interversion de limites et d'intégrales
- 239. Fonctions définies par une intégrale dépendant d'un paramètre. Exemples et applications
- 246. Séries de Fourier. Exemples et applications

Théorème 1. *Soit $f \in L^1(\mathbf{T})$, de classe C^1 sur l'intervalle ouvert I. $S_n(f)$ converge uniformément vers f sur tout compact de I.*

Démonstration. Soit pour $a \in I$

$$\psi_a : \left| \begin{array}{ccc} \mathbf{T} & \longrightarrow & \mathbf{C} \\ x & \longmapsto & \frac{f(a-2u)-f(a)}{\sin(u)} \end{array} \right. .$$

On va montrer que les coefficients de Fourier des ψ_a convergent uniformément (en a) sur les compacts de I vers 0. On conclura en exprimant cette convergence en terme de convolution.

Les fonctions ψ_a dépendent continûment de a. Plus précisément l'application

$$\psi : \left| \begin{array}{ccc} I & \longrightarrow & L^1(\mathbf{T}) \\ a & \longmapsto & \psi_a \end{array} \right.$$

est continue. On commence par constater que ψ_a est bien intégrable car f l'est et qu'en 0 et π, seuls points où le sinus s'annule, la fonction ψ_a est prolongeable par continuité. Pour établir la continuité de ψ, on admet que l'opérateur de translation

$$\tau : \left| \begin{array}{ccc} \mathbf{T} & \longrightarrow & \mathcal{L}(L^1(\mathbf{T})) \\ h & \longmapsto & \tau_h : f \mapsto f(\cdot - h) \end{array} \right.$$

est continu.

$$\|\psi_a - \psi_b\|_{L^1} = 2 \int_{-\pi/2}^{\pi} /2 \left| \frac{f(a-2u)-f(a)}{\sin(u)} - \frac{f(b-2u)-f(a)}{\sin(u)} \right| \mathrm{d}u.$$

Découpons cette intégrale en deux. Soit $\delta > 0$ tel que $[a \pm 2\delta], [b \pm 2\delta] \subset [\alpha, \beta] \subset I$. On a alors

$$\begin{aligned} \int_{-\delta}^{\delta} \left| \frac{f(a-2u)-f(a)}{\sin(u)} - \frac{f(b-2u)-f(a)}{\sin(u)} \right| \mathrm{d}u &= \int_{-\delta}^{\delta} \frac{1}{|\sin(u)|} \left| \int_a^{a-2u} f' - \int_b^{b-2u} f' \right| \mathrm{d}u \\ &\leqslant \int_{-\delta}^{\delta} \frac{4u}{|\sin(u)|} \|f'\|_{[\alpha,\beta]} \, \mathrm{d}u. \end{aligned}$$

Cette dernière intégrale tendant vers 0 lorsque $\delta \to 0$, on fixe $\delta > 0$ tel qu'elle n'excède pas ϵ. Soit maintenant $C > 0$ tel que $\frac{1}{|\sin(u)|} \leqslant C$ sur $[\pm\pi/2]\backslash[\pm\delta]$. On a

$$\begin{aligned}\int_{[\pm\pi/2]\backslash[\pm\delta]} \left| \frac{f(a-2u)-f(a)}{\sin(u)} - \frac{f(b-2u)-f(a)}{\sin(u)} \right| \mathrm{d}u \\ &\leqslant C \int_{[\pm\pi/2]\backslash[\pm\delta]} |f(a-2u)-f(b-2u)| + |f(a)-f(b)| \,\mathrm{d}u \\ &\leqslant C \int_{-\pi/2}^{\pi/2} |f(a-2u)-f(b-2u)| \,\mathrm{d}u + C\pi|f(a)-f(b)|.\end{aligned}$$

Lorsque $a \to b$, le premier tend vers 0 par continuité de l'opérateur τ, le second par continuité de f (sur I).

Convergence de leurs coefficients de Fourier. Soit $[\alpha, \beta]$ un segment de I. L'ensemble

$$H = \{\psi_a \,:\, a \in [\alpha, \beta]\} = \psi([\alpha, \beta])$$

est compact. Et les applications c_n, toutes 1−lipschitziennes, convergent simplement (sur L^1) vers 0 lorsque $n \to \pm\infty$. Le théorème de Dini («version Lipschitz») assure que cette convergence est uniforme sur H :

$$\sup_{a\in[\alpha,\beta]} |c_n(\psi_a)| \underset{n\to\pm\infty}{\longrightarrow} 0.$$

Conclusion. Aussi a-t-on

$$\sup_{a\in[\alpha,\beta]} |c_{2N+1} - c_{-(2N+1)}|(\psi_a) \underset{n\to\pm\infty}{\longrightarrow} 0.$$

Soit, moyennant un changement de variable

$$\sup_{a\in[\alpha,\beta]} \left| \int_{\mathbf{T}} \frac{\sin((N+\frac{1}{2})u)}{\sin(u/2)} (f(a-u)-f(a)) \,\mathrm{d}u \right| \underset{N\to+\infty}{\longrightarrow} 0,$$

c'est-à-dire

$$\sup_{a\in[\alpha,\beta]} |D_N \star f(a) - f(a)| \underset{N\to+\infty}{\longrightarrow} 0.$$

□

Remarque 2. J'ai présenté ce développement lors de mon oral d'analyse (leçon 246). La continuité de l'opérateur de translation figurait dans mon plan. On m'a demandé de préciser pourquoi ψ_a est prolongeable par continuité en 0, puis d'énoncer et de démontrer le théorème de Dini «version Lipschitz». Note : 18.75/20.

46. Théorème de Prokhorov

Références :

— Parthasarathy, *Probability measures on metric spaces.*

— Stein and Shakarchi, *Functional analysis : introduction to further topics in analysis*

— (Billinglsey, *Convergence of probability measures.*)

Il s'agit d'un développement autour de la convergence en loi et des fonctions caractéristique. De ces pages, on peut en fait tirer deux développements, d'intersection non triviale.

Leçons :

— 201. Espaces de fonctions. Exemples et applications

— 202. Exemples de parties denses et applications

— 203. Utilisation de la notion de compacité

— 205. Espaces complets. Exemples et applications

— 262. Modes de convergence d'une suite de variables aléatoires. Exemples et applications

Soit (E,d) un espace métrique. On note $\mathbf{M}_1(E)$ l'ensemble des mesures de probabilité sur E.

Définition 1. Une partie $\Gamma \subset \mathbf{M}_1(E)$ est dite tendue si pour tout $\epsilon > 0$, il existe un compact $K_\epsilon \subset E$ tel que pour tout $\mu \in \Gamma$, $\mu(K_\epsilon) \geqslant 1-\epsilon$.

Théorème 2 (Prokhorov)**.** *Soit (E,d) un espace métrique séparable complet, et (μ_n) une suite d'éléments de $\mathbf{M}_1(E)$. Cette suite est relativement compacte (au sens où toute-suite extraite de (μ_n) admet une extraction convergente) si et seulement si elle est tendue.*

Preuve de l'implication «⇐» (voir le Stein et Shakarshi). Commençons par supposer que (μ_n) est tendue. Pour tout $p \geqslant 1$, il existe un compact $K_p \subset E$ tel que pour tout $n \geqslant 0$, on ait

$$\mu_n(K_p) \geqslant 1 - \frac{1}{p}.$$

Comme K_p compact, l'espace $C(K_p)$ est séparable : donnons-nous, pour chaque $p \geqslant 1$ une suite dense de fonctions $(g_{p,k})_{k\geqslant 0}$. Le théorème de Tietze donne l'existence de fonctions $f_{k,p} \in C(E)$ prolongeant respectivement les fonctions $g_{k,p}$ et ayant les mêmes bornes.
Pour tout (k,p), la suite $(\mu_n(f_{k,p}))_n$ est à valeurs dans le segment (compact donc) $[\pm\|f_{k,p}\|_\infty]$. On peut donc procéder à une extraction diagonale : il existe une extractrice ϕ telle que pour tous k,p, la suite $(\mu_{\phi(n)}(f_{k,p}))_n$ converge.
Prouvons maintenant que si $f \in C(E)$, $(\mu_{\phi(n)}(f))_n$ converge. On montre pour cela que c'est une suite de Cauchy. Fixons $\epsilon > 0$, et $p \geqslant 1$ tel que $\frac{1}{p}\|f\|_\infty \leqslant \epsilon$. Choisissons aussi k tel que $\|g_{k,p} - f\mathbf{1}_{K_p}\| \leqslant \epsilon$ (rappelons que $(g_{p,k})_{k\geqslant 0}$ est dens dans $C(K_p)$), qui entraîne l'inégalité $\|f_{k,p}\| = \|g_{k,p}\| \leqslant \|f\| + \epsilon$.
Enfin, comme la suite $(\mu_{\phi(n)}(f_{k,p}))_n$ converge, prenons N tel que si $n, \tilde{n} \geqslant N$,

$$\left|\mu_{\phi(n)}(f_{k,p}) - \mu_{\phi(\tilde{n})}(f_{k,p})\right| \leqslant \epsilon.$$

Toutes ces quantités étant fixé, nous sommes prêts à faire des majoration : si $n, \tilde{n} \geqslant N$, on a

$$\begin{aligned}\left|\mu_{\phi(n)}(f) - \mu_{\phi(\tilde{n})}(f)\right| &\leqslant |\mu_{\phi(n)}(f\mathbf{1}_{K_p^c})| + |\mu_{\phi(n)}((f-f_{k,p})\mathbf{1}_{K_p})| + |\mu_{\phi(n)}(f_{k,p}\mathbf{1}_{K_p^c})| + (\text{idem avec } \tilde{n}) \\ &\quad + |\mu_{\phi(n)}(f_{k,p}) - \mu_{\phi(\tilde{n})}(f_{k,p})| \\ &\leqslant 2(\epsilon + \epsilon + (\|f\| + \epsilon)\frac{1}{p}) + \epsilon\end{aligned}$$

Ceci prouve que $(\mu_{\phi(n)}(f))_n$ est une suite (réelle) de Cauchy donc converge : notons $\ell(f)$ sa limite. L'application ℓ est linéaire, continue ($|\ell(f)| = \lim |\mu_{\phi(n)}(f)| \leqslant \|f\|$) et positive (si $f \geqslant 0$, $\ell(f) = \lim \mu_{\phi(n)}(f) \geqslant 0$). Le théorème de représentation de Riesz garantit l'existence d'une mesure μ telle que $\ell = \mu(\cdot)$, concluant aisin la première partie du théorème. □

Preuve de l'implication «⇒» (voir le Parthasarathy). Soit maintenant (μ_n) une suite d'éléments de $\mathbf{M}_1(E)$ dont toute suite extraite admet une extraction convergente.

Lemme 3 (Lemme de Portmanteau)**.** *Si G est un ouvert de E et si ν_n converge étroitement vers ν alors*

$$\liminf_{n\to\infty} \nu_n(G) \geqslant \nu(G).$$

Preuve du lemme. Considérons les fonctions $f_k = \min(1, kd(\cdot, G^c))$. Cette suite de fonctions continues bornées converge simplement en croissant vers $\mathbf{1}_G$. On a donc, par définition de la convergence étroite, pour tout k,

$$\liminf_{n\to\infty} \nu_n(G) \geqslant \liminf_{n\to\infty} \nu_n(f_k) = \nu(f_k).$$

Puisque par convergence monotone, $\nu(f_k) \underset{k\to\infty}{\to} \nu(G)$, on a le résultat. □

Donnons-nous maintenant une suite (x_p) dense dans E. Pour tout $k \geqslant 1$, on a

$$\bigcup_p B(x_p, 1/k) = E. \tag{9}$$

Considérons l'ouvert

$$G_{q,k} := \bigcup_{p=1}^{q} B(x_p, 1/k)$$

Lemme 4. *Pour tout $\epsilon > 0$, et tout $k \geqslant 1$, il existe $q_{k,\epsilon}$ tel que pour tout $n \geqslant 1$, on ait $\mu_n(G_{q_{k,\epsilon},k}) \geqslant 1 - \epsilon$.*

Preuve du lemme, version 1. On admet ici que l'on peut munir $\mathcal{M}_1(E)$ d'une distance métrisant la convergence en loi (cette propriété est toujours vraie mais est difficile à établir). Considérons l'adhérence Ξ de $\{\mu_n, n \geqslant 0\}$, qui est compacte vue l'hypothèse. Introduisons les fonctions

$$\begin{aligned} f_q : \Xi &\to [0,1] \\ \mu &\mapsto \mu(G_{k,q}). \end{aligned}$$

C'est une suite de fonctions semi-continue inférieurement (lemme de Portmanteau) convergeant simplement en croissant vers la fonction continue 1 (grâce à l'égalité (9)). Le théorème de Dini garantit que la convergence est uniforme sur le compact Ξ : c'est ce que l'on souhaitait établir. □

Preuve du lemme, version 2. Cette preuve du lemme est moins élégante, mais rend la preuve auto-suffisante. Supposons qu'il n'en soit rien : il existe dans ce cas $\epsilon_0 > 0$, $k_0 \geqslant 1$, ainsi qu'une suite q_r tendant vers l'infini et une suite de mesure ν_r éléments de $\{\mu_n, n \geqslant 0\}$ tels que pour tout r,

$$\nu_r(G_{q_r,k_0}) \leqslant 1 - \epsilon_0.$$

Par hypothèse, on peut extraire de ν_r une suite convergeant étroitement. Pour ne pas alourdir les notations, on peut se permettre de supposer que ν_r converge, vers une loi ν. Le théorème de Portmanteau donne l'inégalité, pour tout r

$$\nu(G_{q_r,k_0}) \leqslant \liminf_{\tilde{r}\to\infty} \nu_{\tilde{r}}(G_{q_r,k_0}) \leqslant 1 - \epsilon_0.$$

Ce qui donne en faisant tendre r vers $+\infty$,

$$\nu(E) \leqslant 1 - \epsilon_0,$$

qui est une absurdité. □

Achevons maintenant la démonstration du théorème. On fixe $\epsilon > 0$ et pour chaque $k \geqslant 1$, on choisit q_k tel que pour tout n,

$$\mu_n \left(\bigcup_{p=1}^{q_k} B(x_p, 1/k) \right) \geqslant 1 - \frac{\epsilon}{2^k}.$$

La partie fermée

$$K_\epsilon := \bigcap_{k \geqslant 1} \bigcup_{p=1}^{q_k} \bar{B}(x_p, 1/k)$$

est alors de mesure supérieure à $1 - \sum_{k \geqslant 1} \epsilon/2^k = 1 - \epsilon$ pour chaque μ_n. Par ailleurs elle est précompacte par construction et complète en tant que partie fermée de l'espace complet E : K_ϵ est donc compact. □

47. Théorème de Lévy

Références :

— Parthasarathy, *Probability measures on metric spaces.*
— Stein and Shakarchi, *Functional analysis : introduction to further topics in analysis.*
— Cottrell et al., *Exercices de probabilités.*
— (Billinglsey, *Convergence of probability measures.*)

Leçons

— 240. Produit de convolution, transformation de Fourier. Applications
— 261. Fonction caractéristique et transformée de Laplace d'une variable aléatoire. Exemples et applications

On commence par établir une partie du théorème de Prokhorov.
Soit (E,d) un espace métrique. On note $\mathbf{M}_1(E)$ l'ensemble des mesures de probabilité sur E.

Définition 1. Une partie $\Gamma \subset \mathbf{M}_1(E)$ est dite tendue si pour tout $\epsilon > 0$, il existe un compact $K_\epsilon \subset E$ tel que pour tout $\mu \in \Gamma$, $\mu(K_\epsilon) \geqslant 1-\epsilon$.

Théorème 2 (Prokhorov)**.** *Soit (E,d) un espace métrique séparable complet, et (μ_n) une suite d'éléments de $\mathbf{M}_1(E)$. Cette suite est relativement compacte (au sens où toute-suite extraite de (μ_n) admet une extraction convergente) si et seulement si elle est tendue.*

Preuve de l'implication «⇐» (voir le Stein et Shakarshi). Commençons par supposer que (μ_n) est tendue. Pour tout $p \geqslant 1$, il existe un compact $K_p \subset E$ tel que pour tout $n \geqslant 0$, on ait

$$\mu_n(K_p) \geqslant 1 - \frac{1}{p}.$$

Comme K_p compact, l'espace $C(K_p)$ est séparable : donnons-nous, pour chaque $p \geqslant 1$ une suite dense de fonctions $(g_{p,k})_{k\geqslant 0}$. Le théorème de Tietze donne l'existence de fonctions $f_{k,p} \in C(E)$ prolongeant respectivement les fonctions $g_{k,p}$ et ayant les mêmes bornes.
Pour tout (k,p), la suite $(\mu_n(f_{k,p}))_n$ est à valeurs dans le segment (compact donc) $[\pm\|f_{k,p}\|_\infty]$. On peut donc procéder à une extraction diagonale : il existe une extractrice ϕ telle que pour tous k,p, la suite $(\mu_{\phi(n)}(f_{k,p}))_n$ converge.
Prouvons maintenant que si $f \in C(E)$, $(\mu_{\phi(n)}(f))_n$ converge. On montre pour cela que c'est une suite de Cauchy. Fixons $\epsilon > 0$, et $p \geqslant 1$ tel que $\frac{1}{p}\|f\|_\infty \leqslant \epsilon$. Choisissons aussi k tel que $\|g_{k,p} - f\mathbf{1}_{K_p}\| \leqslant \epsilon$ (rappelons que $(g_{p,k})_{k\geqslant 0}$ est dens dans $C(K_p)$), qui entraîne l'inégalité $\|f_{k,p}\| = \|g_{k,p}\| \leqslant \|f\| + \epsilon$.
Enfin, comme la suite $(\mu_{\phi(n)}(f_{k,p}))_n$ converge, prenons N tel que si $n, \tilde{n} \geqslant N$,

$$\left|\mu_{\phi(n)}(f_{k,p}) - \mu_{\phi(\tilde{n})}(f_{k,p})\right| \leqslant \epsilon.$$

Toutes ces quantités étant fixé, nous sommes prêts à faire des majoration : si $n, \tilde{n} \geqslant N$, on a

$$\begin{aligned}\left|\mu_{\phi(n)}(f) - \mu_{\phi(\tilde{n})}(f)\right| &\leqslant |\mu_{\phi(n)}(f\mathbf{1}_{K_p^c})| + |\mu_{\phi(n)}((f-f_{k,p})\mathbf{1}_{K_p})| + |\mu_{\phi(n)}(f_{k,p}\mathbf{1}_{K_p^c})| + (\text{idem avec } \tilde{n}) \\ &\quad + |\mu_{\phi(n)}(f_{k,p}) - \mu_{\phi(\tilde{n})}(f_{k,p})| \\ &\leqslant 2(\epsilon + \epsilon + (\|f\| + \epsilon)\frac{1}{p}) + \epsilon\end{aligned}$$

Ceci prouve que $(\mu_{\phi(n)}(f))_n$ est une suite (réelle) de Cauchy donc converge : notons $\ell(f)$ sa limite. L'application ℓ est linéaire, continue ($|\ell(f)| = \lim|\mu_{\phi(n)}(f)| \leqslant \|f\|$) et positive (si $f \geqslant 0$, $\ell(f) = \lim \mu_{\phi(n)}(f) \geqslant 0$). Le théorème de représentation de Riesz garantit l'existence d'une mesure μ telle que $\ell = \mu(\cdot)$, concluant aisin la première partie du théorème. □

Corollaire 3 (Théorème de Lévy)**.** *Soit X_n une suites de variables aléatoires à valeurs dans $\mathbf{R}^d$ dont les fonctions caractéristiques ϕ_n convergent simplement vers une fonction ϕ continue en 0. Dans ce cas ϕ est la fonction caractéristique d'une variable aléatoire X et X_n converge en loi vers X.*

Démonstration. (elle se trouve dans le Cottrell). Si l'on montre que la suite (X_n), est tendue, le théorème de Prokhorov assurera de l'existence de points limites pour toute suite extraite ; et la convergence des fonctions caractéristiques donnera l'unicité du point limite en question (voir le théorème suivant), concluant la démonstration. Il s'agit donc de montrer que la suite est tendue. Soit $u > 0$. Le théorème de Fubini donne

$$\begin{aligned}
\frac{1}{u^d}\int_{[-u,u]^d}(1-\phi_n(t))\,\mathrm{d}t &= E\left[\frac{1}{u^d}\int_{[-u,u]^d}(1-e^{\mathrm{i}\langle t,X_n\rangle})\,\mathrm{d}t\right]\\
&= 2^d E\left[1-\prod_{i=1}^{d}\frac{\sin(uX_n^{(i)})}{uX_n^{(i)}}\right]\\
&\geqslant 2^d E\left[1-\prod_{i=1}^{d}\left|\frac{\sin(uX_n^{(i)})}{uX_n^{(i)}}\right|\right]\\
&\geqslant 2^d \underbrace{\left(1-1^{d-1}\frac{1}{2}\right)}_{=1/2}\mathrm{P}\Big(\exists i\,:\,|X_n^{(i)}|\geqslant 2/u\Big),
\end{aligned}$$

car pour tout réel s, $\left|\frac{\sin s}{s}\right| \leqslant 1$, et si $|s| \geqslant 2$ alors $\left|\frac{\sin s}{s}\right| \leqslant 1/2$. Ainsi

$$\mathrm{P}\Big(\exists i\,:\,|X_n^{(i)}|\geqslant 2/u\Big) \leqslant \frac{1}{u^d}\int_{[-u,u]^d}(1-\phi_n(t))\,\mathrm{d}t \leqslant \frac{1}{u^d}\int_{[-u,u]^d}|1-\phi_n(t)|\,\mathrm{d}t.$$

Le lemme de Fatou donne

$$\limsup_{n\to\infty}\mathrm{P}\Big(\exists i\,:\,|X_n^{(i)}|\geqslant 2/u\Big) \leqslant \frac{1}{u^d}\int_{[-u,u]^d}|1-\phi(t)|\,\mathrm{d}t.$$

Puis, comme ϕ est continue en 0,

$$\frac{1}{u^d}\int_{[-u,u]^d}|1-\phi(t)|\,\mathrm{d}t \underset{u\to 0}{\longrightarrow} 0.$$

Finalement

$$\limsup_{u\to 0}\limsup_{n\to\infty}\mathrm{P}\Big(\exists i\,:\,|X_n^{(i)}|\geqslant 2/u\Big) = 0,$$

c'est-à-dire

$$\limsup_{M\to\infty}\limsup_{n\to\infty}\mathrm{P}(\|X_n\| > M) = 0 :$$

la suite (X_n) est tendue. □

Appendice hord développement

Théorème 4. *Deux mesures de probabilité sur $\mathbf{R}^d$ ayant la même fonction caractéristique sont égales.*

Démonstration. Soit μ et ν deux mesures de probabilité sur $\mathbf{R}^d$ ayant la même fonction caractéristique. Il suffit de prouver que pour toute fonction f continue à support compact sur $\mathbf{R}^d$, $\mu(f) = \nu(f)$. Soit $\epsilon > 0$, puis $A > 0$ tel que

$$\mu([-A,A]^d) \geqslant 1-\epsilon, \qquad \nu([-A,A]^d) \geqslant 1-\epsilon,$$

et tel que le support de f soit contenu dans $[-A,A]^d$. Le théorème de Stone-Weierstrass garantit l'existence d'un polynôme trigonométrique $2A$-périodique P à d indéterminées tel que $\sup_{[-A,A]^d} \|f-P\|_\infty \leqslant \epsilon$. Comme μ et ν ont la même fonction caractéristique, on a l'égalité $\mu(P)=\nu(P)$. Ainsi

$$\begin{aligned}
|\mu(f)-\nu(f)| &\leqslant |\mu(f)-\mu(P)| + |\nu(f)-\nu(P)| \\
&\leqslant 2 \sup_{[-A,A]^d} \|f-P\|_\infty + \mu(|P|\mathbf{1}_{([-A,A]^d)^c}) + \nu(|P|\mathbf{1}_{([-A,A]^d)^c}), \\
&\leqslant \epsilon + \|P\|_\infty \mu(([-A,A]^d)^c), \\
&\leqslant \epsilon + (\|f\|_\infty + \epsilon)\epsilon.
\end{aligned}$$

Finalement $\mu(f)=\nu(f)$. □

48. Théorème de Sarkowski

Référence S. Francinou, H. Gianella, S. Nicolas, *Analyse 1*

Leçons

- 223. Suites numériques. Convergence, valeurs d'adhérence. Exemples et applications
- 226. Suites vectorielles et réelles définies par une relation de récurrence $u_{n+1} = f(u_n)$. Exemples et applications
- 228. Continuité et dérivabilité des fonctions réelles d'une variable réelle. Exemples et contre-exemples

Théorème 1. *Soit f une fonction réelle continue définie sur un intervalle réel. Si elle admet un 3-cycle, elle admet des cycles de tous ordres.*

On fixe une fonction continue réelle f définie sur un intervalle réel.

Définition 2. On dit qu'un segment I couvre un segment J et on note $I \twoheadrightarrow J$ si $f(I) \supset J$.

Lemme 3. *Si I couvre I alors f admet un point fixe dans I.*

Démonstration. Écrivons $I = [a, b]$. Soit $\alpha, \beta \in [a, b]$ tels que $f(\alpha) = a$ et $f(\beta) = b$. On a $f(\beta) - \beta = b - \beta \geqslant 0$ et $f(\alpha) - \alpha = a - \alpha \leqslant 0$. Par le théorème des valeurs intermédiaires f admet un point fixe dans $[\alpha, \beta]$. □

Lemme 4. *Si I couvre J, il existe $K \subset I$ tel que $f(K) = J$.*

Démonstration. Écrivons $J = [a, b]$. Soit $\alpha, \beta \in [a, b]$ tels que $f(\alpha) = a$ et $f(\beta) = b$. Disons $\alpha \leqslant \beta$. Prenons $u = \max\{x \in [\alpha, \beta] \,:\, f(x) = a\}$ puis $v = \min\{x \in [u, \beta] \,:\, f(x) = b\}$. Si $f([u, v]) \supsetneq J$, disons qu'il existe $t < a$ et $t \in f([u, v])$. Alors le théorème des valeurs intermédiaires donne l'existence d'un point dans $[t, v]$ tel que $f(t) = a$, contredisant la maximalité de u. □

Lemme 5. *Supposons que soient donnés des segments satisfaisant le cycle de recouvrement*

$$I_0 \twoheadrightarrow I_1 \twoheadrightarrow \cdots \twoheadrightarrow I_{n-1} \twoheadrightarrow I_0.$$

Alors il existe $x \in I_0$ tel que $f^n(x) = x$ et pour tout k, $f^k(x) \in I_k$.

Démonstration. Le lemme 4 fournit l'existence d'un segment $J_1 \subset$ tel que $f(J_1) = I_1$. Puis, comme $f^2(J_1) \supset f(I_1) \supset I_2$. Soit donc, d'après le même lemme, et puisque f^2 est continue, $J_2 \subset J_1$ tel que $f^2(J_2) = I_2$. Ainsi de suite jusqu'à un segment J_n tel que $f^n(J_n) = I_0$. A fortiori $f^n(J_n) \supset J_n$. D'après le lemme 3, f^n admet un point fixe $x \in J_n \subset I_0$. Enfin pour tout k, $f^k(x)$ est dans $f^k(J_n) \subset f^k(J_k) = I_k$. □

Démonstration du théorème de Sarkowski. Soit a un point d'ordre 3. Notons $b = f(a)$ et $c = f^2(a)$. Par symétrie des rôles de a, b, c, disons que $a < b$ et $a < c$. Traitons dans un premier temps le cas où $a < b < c$. Notons $I_0 = [a, b]$, $I_1 = [b, c]$. D'après le théorème des valeurs intermédiaires, I_0 couvre I_1 et I_1 couvre I_0 et I_1.

On a donc un cycle de recouvrement

$$I_0 \twoheadrightarrow I_1 \twoheadrightarrow I_0.$$

Le lemme 5 donne l'existence d'un point fixe $x \in I_0$ de f^2 tel que $f(x) \in I_1$. On a $x \neq f(x)$ sinon $x \in I_0 \cap I_1 = \{b\}$, or b n'est pas un point fixe de f^2. On a donc un cycle d'ordre 2.

On a, si $n \geqslant 4$, un cycle de recouvrement

$$I_0 \twoheadrightarrow \underbrace{I_1 \twoheadrightarrow \cdots \twoheadrightarrow I_1}_{n-1 \text{ apparitions}} \twoheadrightarrow I_0.$$

Le lemme 5 donne l'existence d'un point fixe $x \in I_0$ de f^n tel que pour tout $k \in [1, n-1]$, $f^k(x) \in I_1$. On a $x \neq f^k(x)$ sinon $x \in I_0 \cap I_1 = \{b\}$, or $a = f^2(b) \notin I_1$. On a donc un cycle d'ordre n. □

Remarque 6. Il existe des fonctions admettant des cycles d'ordre 5 mais pas d'ordre 3. Le théorème général de Sarkowski affirme que s'il existe un point fixe d'ordre k, il existe des points fixes de tous ordres inférieurs à k, pour l'ordre suivant

$$\begin{aligned} 3 \rhd 5 \rhd 7 \rhd 9 \rhd \cdots \rhd 2 \times 3 \rhd 2 \times 5 \rhd 2 \times 7 \rhd 2 \times 9 \rhd \cdots \\ \cdots \rhd 2^p \times 3 \rhd 2^p \times 5 \rhd 2^p \times 7 \rhd 2^p \times 9 \rhd \cdots \\ \cdots \rhd 2^q \rhd 2^{q-1} \rhd \cdots \rhd 2^2 \rhd 2 \rhd 1. \end{aligned}$$

49. Théorème de Steinhaus

Référence O. Garet et A. Kurtzmann, *De l'intégration aux probabilités*

Leçons

- 207 Prolongement de fonctions. Exemples et applications
- 243. Convergence des séries entières, propriétés de la somme. Exemples et applications
- 244. Fonctions développables en série entière, fonctions analytiques. Exemples
- 245. Fonctions holomorphes sur un ouvert de C. Exemples et applications
- 263. Variables aléatoire à densité. Exemples et applications

Attention ! Dans le livre *De l'intégration aux probabilités* la rédaction de ce qui sera la première partie de mon point 4 est peut-être un peu rapide.

On note D le disque ouvert de centre 0 et de rayon 1 du plan complexe $\mathbf{C}$ et $\mathbf{T}$ sa frontière.

Théorème 1. *Soit $\sum a_n z^n$ une série entière de rayon de convergence 1 et (ζ_n) une suite de variables aléatoires i.i.d. de loi uniforme sur le cercle $\mathbf{T}$. Presque sûrement, $\mathbf{T}$ est une coupure pour la série entière $\sum a_n \zeta_n z^n$.*

Lemme 2. *Il existe un point singulier sur le cercle.*

Démonstration. Supposons qu'il n'en soit rien. Pour tout $z \in \mathbf{T}$, il existe $r_z > 0$ tel que $f(z) = \sum_{n=0}^{+\infty} a_n z^n$ soit prolongeable en une fonction holomorphe sur $D \cup D(z, r_z)$. Par compacité, il existe $\epsilon > 0$ tel que f soit prolongeable en une fonction holomorphe sur $D(0, 1+\epsilon)$. La formule de Cauchy garantit que $(a_n(1+\epsilon/2)^n)_{n\geqslant 0}$ est bornée, donc $\sum_n a_n z^n$ a un rayon de convergence supérieur à $1+\epsilon/2$. C'est une contradiction. □

Lemme 3. *L'ensemble des points réguliers est un ouvert de $\mathbf{T}$.*

Démonstration du théorème. La série entière $\sum a_n \zeta_n z^n$ a pour rayon de convergence 1 : on note F sa somme. Pour tout $z \in D$, introduisons l'événement

$$A(z) = \left\{ \limsup_{n\to\infty} \left| \frac{1}{n!} F^{(n)}(z) \right|^{1/n} < \frac{1}{1-|z|} \right\}.$$

1. Ce qu'est l'événement $A(z)$. Soit $\xi \in \mathbf{T}$. On va voir que c'est un point régulier si et seulement s'il existe $r \in [0,1[$ tel que l'événement $A(r\xi)$ soit réalisé. Constatons le fait plus précis suivant : à ω fixé, si $b < 1$, $r < 1$, et

$$\limsup_{n\to\infty} \left| \frac{1}{n!} F^{(n)}(r\xi) \right|^{1/n} \leqslant b \frac{1}{1-r}$$

alors les points de

$$D\left(r\xi, \frac{1-r}{b}\right) \cap \mathbf{T}$$

sont réguliers pour F : en effet, le lemme de Hadamard garantit que la série entière

$$\sum_n \frac{1}{n!} F^{(n)}(r\xi)(z-r\xi)^n$$

a alors un rayon de convergence supérieur à $\frac{1-r}{b}$. Réciproquement si F est prolongeable en une fonction holomorphe sur un voisinage $D(\xi, \rho)$ de ξ alors c'est encore le cas sur $D((1-\rho/3)\xi, 2\rho/3)$,

donc l'événement $A((1-\rho/3)\xi)$ est réalisé.

2. La probabilité $P(A(z))$ ne dépend que de $|z|$. Soit $\xi \in \mathbf{T}$, on veut montrer que si $z \in D$, $P(A(z)) = P(A(z\xi))$. C'est le cas car $(\zeta_n)_n \overset{\text{loi}}{=} (\zeta_n \xi^n)_n$.

3. Pour tout $z \in D$, $P(A(z)) \in \{0,1\}$. Notons, si $N \geqslant 1$, $\mathcal{F}_N = \sigma(\zeta_n, n \geqslant N)$. Pour tout $n \geqslant 1$, $|F^{(n)}(z)|^{1/n}$ est $\mathcal{F}_n$-mesurable. Donc $\limsup_{n\to\infty} |F^{(n)}(z)|^{1/n}$ est $\bigcap_{n\geqslant 1} \mathcal{F}_n$-mesurable. La loi du $0-1$ conclut.

4. Conclusion. Supposons qu'il existe z tel que $P(A(z)) = 1$. Il existe donc $b < 1$ tel que la probabilité de l'événement

$$\tilde{A}(z) = \left\{ \limsup_{n\to\infty} |F^{(n)}(z)|^{1/n} \leqslant b \frac{1}{1-|z|} \right\}$$

soit supérieure à $1/2$. En réalité elle vaut 1 encore pour les mêmes raisons que précédemment, de même $P(\tilde{A}(|z|\xi)) = 1$ pour tout $\xi \in \mathbf{T}$. Par compacité il existe $\xi_1, \ldots, \xi_p \in \mathbf{T}$ tels que

$$\mathbf{T} = \bigcup_{j=1}^{p} D\left(|z|\xi_j, \frac{1-|z|}{b}\right) \cap \mathbf{T}.$$

Ainsi sur l'événement

$$\bigcap_{j=1}^{p} \tilde{A}(|z|\xi_j),$$

qui est de probabilité 1, tous les points du cercle sont réguliers, contredisant ainsi le lemme 2. Ainsi pour tout $z \in D$, $P(A(z)) = 0$. Conséquemment l'événement

$$\bigcup_{\substack{q\in\mathbf{Q} \\ r\in[0,1[\cap\mathbf{Q}}} A(re^{2\mathrm{i}\,\pi q})$$

est de probabilité nulle. Sur son complémentaire, grâce au point 1, tous les $e^{2\mathrm{i}\,\pi q}$, $q \in \mathbf{Q}$, sont des points singuliers de F ; puis avec le lemme 3, tous les points du cercle sont singuliers pour F. □

50. Théorème taubérien fort de Hardy et Littlewood

Référence D. Choimet, H. Queffelec, *Analyse mathématique.*

Remarque importante. J'avais rédigé ici la version du Gourdon. Mais je conseille de suivre plutôt le Choimet-Queffélec, qui proposent une démonstration on ne peut plus limpide.

Leçons

- 230. Séries de nombres réels ou complexes. Comportement des restes ou des sommes partielles des séries numériques. Exemples
- 241. Suites et séries de fonctions. Exemples et contre-exemples
- 243. Convergence des séries entières, propriétés de la somme. Exemples et applications
- 244. Fonctions développables en série entière, fonctions analytiques. Exemples

Théorème 1. *Soit $\sum a_n z^n$ une série entière de rayon de convergence 1, telle que $a_n = O(\frac{1}{n})$ et que sa fonction somme f ait une limite finie ℓ en 1. La série $\sum a_n$ converge, et sa somme est ℓ.*

Démonstration. Étape 0, où on dévoile l'astuce. Quitte à retrancher ℓ à a_0, on peut supposer que $\ell = 0$. Considérons l'ensemble W des fonctions $\phi : [0,1] \to \mathbf{R}$ telles que $\sum a_n \phi(x^n)$ converge pour $x \in [0,1[$ et tende vers 0 en 1. Constatons que pour conclure, il suffit d'établir que $g = \mathbf{1}_{]1/2,1]}$ est un élément de W. Pour cela, on va approcher g par des polynômes de premier coefficient nul qui eux, on va le voir, sont des éléments de W.

Étape 1 : les polynômes P tels que $P(0) = 0$ sont dans W. On commence par s'apercevoir que W est un espace vectoriel. Ensuite, si $p \in \mathbf{N}^*$, pour tout $x \in [0,1[$, $|x|^p < 1$ donc $\sum a_n x^{pn}$ converge, de somme $f(x^p)$, qui tend vers 0 lorsque $x \to 1$. Par linéarité les polynômes de premier coefficient nul sont des éléments de W.

Étape 2 : on approche g par des polynômes. Déjà si $x \in [0,1[$, $g(x_n) = \mathbf{1}_{n \leqslant \frac{\log 2}{\log 1/x}}$, donc $\sum a_n g(x^n)$ converge. Considérons la fonction h définie sur $]0,1[$ par

$$h(x) = \frac{g(x) - x}{1 - x}.$$

Fixons $\epsilon > 0$. Soient s_1 et s_2 continues telles $s_1 \leqslant h \leqslant s_2$, et $\int_0^1 s_2 - s_1 \leqslant \epsilon$.
Le théorème de Weierstrass fournit deux polynômes P_1 et P_2 tels que $\|P_i - s_i\| \leqslant \epsilon$. Posons enfin $Q_1 = P_1 - \epsilon$ et $Q_2 = P_2 + \epsilon$, de sorte que

$$Q_1 \leqslant h \leqslant Q_2.$$

On a par ailleurs la majoration

$$Q = Q_2 - Q_1 \leqslant s_2 - s_1 + 4\epsilon, \qquad \text{donc} \qquad \int_0^1 Q_2 - Q_1 \leqslant 5\epsilon.$$

En outre, notant $P_i = X + X(1-X)Q_i$, on a

$$P_1 \leqslant g \leqslant P_2$$

.

Étape 3 : on conclut. Soit $M = \sup_n |na_n|$. On a

$$\begin{aligned}\left|\sum_n a_n g(x^n) - \sum a_n P_1(x^n)\right| &\leqslant \sum_n |a_n|(P_2 - P_1)(x^n) \\ &\leqslant \sum_n \frac{M}{n}(P_2 - P_1)(x^n) \\ &\leqslant \sum_n \frac{M}{n}(X(1-X)(Q_2 - Q_1))(x^n) \\ &\leqslant M \sum_n \frac{x^n(1-x^n)}{n} Q(x^n).\end{aligned}$$

Constatons que si $Q = X^k$ est un monôme,

$$\sum_n \frac{x^n(1-x^n)}{n} x^{kn} = \log \frac{1-x^k}{1-x^{k+1}} \underset{x\to 1}{\longrightarrow} \frac{1}{k+1} = \int_0^1 x^k \,\mathrm{d}x.$$

Aussi a-t-on par linéarité

$$\sum_n \frac{x^n(1-x^n)}{n} Q(x^n) \underset{x\to 1}{\longrightarrow} \int_0^1 Q \leqslant 5\epsilon.$$

On a donc établi que

$$\limsup_{x\to 1} \left|\sum_n a_n g(x^n) - \sum a_n P_1(x^n)\right| \leqslant 5M\epsilon = 5M\epsilon.$$

Finalement $g \in W$. □

51. Un calcul d'intégrale

Référence J. Saint-Raymond, *Topologie, etc.*

Leçons

— 236. Illustrer par des exemples quelques méthodes de calcul d'intégrales de fonctions d'une ou plusieurs variables réelles

— 245. Fonctions holomorphes sur un ouvert de C. Exemples et applications

Proposition 1.

$$\int_0^{+\infty} \frac{\log x}{(x+1)^3}\,\mathrm{d}x = -\frac{1}{2}.$$

Démonstration. Soit Log la détermination du logarithme sur $U = \mathbf{C}\backslash\mathbf{R}_+$ telle que $\mathrm{Log}(-1) = \mathrm{i}\,\pi$ (en fait si log est la détermination principale du logarithme, on a $\mathrm{Log}(x) = \log(-x) + \mathrm{i}\,\pi$). C'est une fonction holomorphe sur U. On a en outre pour tout $x > 0$,

$$\mathrm{Log}(x + \mathrm{i}\,\epsilon) \underset{\epsilon\to 0^+}{\longrightarrow} \log x, \qquad \text{et} \qquad \mathrm{Log}(x - \mathrm{i}\,\epsilon) \underset{\epsilon\to 0^+}{\longrightarrow} \log x + 2\,\mathrm{i}\,\pi.$$

La fonction $f : z \mapsto \frac{(\mathrm{Log}\, z)^2}{(z+1)^3}$ est méromorphe sur U. En -1, son seul pôle, un développement de Taylor de Log assure que son résidu est

$$\frac{1}{2}(\mathrm{Log}^2)''(-1) = \frac{1 - \mathrm{Log}(z)}{z^2}\Big|_{z=-1} = 1 - \mathrm{i}\,\pi.$$

Le contour d'intégration γ_n pour la formule des résidus est le suivant

Le théorème des résidus donne si $n \geqslant 2$, puique le contour ne rencontre alors aucun pôle,

$$\int_{\gamma_n} f = 2\,\mathrm{i}\,\pi(1 - \mathrm{i}\,\pi).$$

Montrons que $\gamma_n^{(1)}$ et $\gamma_n^{(3)}$ ont une contribution négligeable. On utilise que pour tout $z \in U$, $\mathrm{Log}(z) = \log|z| + \mathrm{i}\,\theta$ pour un $\theta \in]0, 2\pi[$. Ainsi $|\mathrm{Log}(z)|^2 \leqslant \log^2|z| + 4\pi^2$. Sur $\gamma_n^{(1)}$, on obtient

$$\Big|\int_{\gamma_n^{(1)}} f\Big| \leqslant 2\pi r_n \frac{\log^2 r_n + 4\pi^2}{(r_n - 1)^3} \underset{n\to\infty}{\longrightarrow} 0.$$

Et sur $\gamma_n^{(3)}$,

$$\Big|\int_{\gamma_n^{(3)}} f\Big| \leqslant \pi \frac{1}{n} \frac{\log^2 n + 4\pi^2}{(1 - \frac{1}{n})^3} \underset{n\to\infty}{\longrightarrow} 0.$$

Contribution de $\gamma_n^{(2)}$ et $\gamma_n^{(4)}$. Déjà vérifions que

$$\int_{\gamma_n^{(2)}} f = \int_0^{\infty} \frac{\mathrm{Log}(x+\mathrm{i}/n)^2}{(x+1+\mathrm{i}/n)^3} \mathbf{1}_{[0,n]}(x)\,\mathrm{d}x \underset{n\to\infty}{\longrightarrow} \int_0^{+\infty} \frac{\log(x)^2}{(x+1)^3}\,\mathrm{d}x.$$

Il s'agit d'une application du théorème de convergence dominée. La convergence ponctuelle ne pose pas de problème. Pour la domination, on a

$$\left|\frac{\mathrm{Log}(x+\mathrm{i}/n)^2}{(x+1+\mathrm{i}/n)^3}\mathbf{1}_{[0,n]}(x)\right| \leqslant \frac{(\log\sqrt{x^2+1/n^2})^2+4\pi^2}{(x+1)^3} \leqslant \frac{(|\log x|+\log(x+1))^2+4\pi^2}{(x+1)^3}.$$

De même on a

$$\int_{\gamma_n^{(4)}} f \underset{n\to\infty}{\longrightarrow} \int_0^{+\infty} -\frac{(\log(x)+2\,\mathrm{i}\,\pi)^2}{(x+1)^3}\,\mathrm{d}x.$$

Ainsi, en les sommant

$$\int_{\gamma_n^{(2)}} f + \int_{\gamma_n^{(4)}} f \underset{n\to\infty}{\longrightarrow} -2\times 2\,\mathrm{i}\,\pi \int_0^{+\infty} \frac{\log(x)}{(x+1)^3}\,\mathrm{d}x + 4\pi^2 \int_0^{+\infty} \frac{1}{(x+1)^3}\,\mathrm{d}x.$$

En prenant la partie imaginaire on obtient l'égalité souhaitée. □

52. Théorèmes de Morera, de Weierstrass et d'Osgood

Référence M. Zavidovique, *Un max de maths.*

Leçons

- 235. Problèmes d'interversion de limites et d'intégrales
- 241. Suites et séries de fonctions. Exemples et contre-exemples
- 245. Fonctions holomorphes sur un ouvert de C. Exemples et applications
- 247. Exemples de problèmes d'interversion de limites

Théorème 1 (Morera)**.** *Une fonction continue sur un ouvert de* $\mathbf{C}$ *dont l'intégrale sur tout contour fermé est nulle est holomorphe.*

Démonstration. Soit f une telle fonction, et $D(0,r)$ un disque de l'ouvert. Définissons F par

$$F(z) = \int_{[0,z]} f.$$

Dés lors F est holomorphe, donc analytique sur le disque, de dérivée f elle aussi holomorphe donc. □

Théorème 2 (Weierstrass)**.** *Si une suite de fonctions holomorphes sur un ouvert de* $\mathbf{C}$ *converge uniformément sur tout compact vers une fonction, celle-ci est holomorphe, et il y a convergence uniforme des dérivées sur tout compact.*

Démonstration. La fonctions limite est continue par convergence uniforme et holomorphe grâce au théorème de Morera. La convergence uniforme des dérivées découle de la formule de Cauchy

$$f'(z) = \frac{1}{2\mathrm{i}\,\pi} \int_{\partial D(0,1)} \frac{f(u)}{(u-z)^2}\,\mathrm{d}u,$$

si $|z| < 1$. □

Théorème 3 (Osgood)**.** *Si une suite de fonctions holomorphes converge simplement sur un ouvert* U *de* $\mathbf{C}$ *alors la limite est holomorphe sur un ouvert dense dans* U*.*

Démonstration. Soit O un ouvert de U. Puisque les f_n sont continues, les ensembles

$$F_k = \{x \in O \,:\, \sup_n |f_n(x)| \leqslant k\}$$

forment une suite croissante exhaustive (car pour tout x, $(f_n(x))$ converge) de fermés de O. Par complétude, l'un de ces fermés est d'intérieur non vide dans O, c'est-à-dire d'intérieur non vide dans $\mathbf{C}$. Soit Ω une boule ouverte contenue dans l'intérieur de F_k. La formule de Cauchy assure que

$$f_n(z) = \frac{1}{2\mathrm{i}\,\pi} \int_{\partial\Omega} \frac{f_n(u)}{u-z}\,\mathrm{d}u.$$

Par convergence dominée, la convergence de f_n vers f est uniforme sur tout compact inclus dans Ω. Le théorème de Weierstrass garantit donc l'holomorphie de f sur Ω.
Considérons la réunion V des ouverts sur lesquels f est holomorphe. Si O est un ouvert de U, tout ce qui précède assure que $V \cap O \neq \varnothing$, concluant la démonstration. □

Complément : limite de fonctions méromorphes. Soit (f_n) une suite de fonctions méromorphes sur un ouvert Ω de $\mathbf{C}$.

Définition 4. On dit que la série $\sum f_n$ converge uniformément sur le compact $K \subset \Omega$ s'il existe $n_0 \geqslant 1$ tel que les fonctions $(f_n)_{n \geqslant n_0}$ soient holomorphes sur un même voisinage de K et $\sum_{n \geqslant n_0} f_n$ converge uniformément sur K.

Théorème 5. *Si $\sum f_n$ converge uniformément sur tout compact de Ω alors sa somme définit une fonction méromorphe sur Ω.*

Démonstration. Découle immédiatement du théorème de Weierstrass. □

53. Nombre de zéros d'une équation différentielle

Référence C. Zuily, H. Queffélec, *Éléments d'analyse pour l'agrégation.*

Leçons

- 220. Équations différentielles $X' = f(t, X)$. Exemples d'étude des solutions en dimension 1 et 2
- 221. Equations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications
- 224. Exemples de développements asymptotiques de suites et de fonctions

Théorème 1. *Soit q une fonction de classe C^1 sur $[0, +\infty[$, strictement positive telle que $\int_0^\infty \sqrt{q} = +\infty$ et $q' = \underset{+\infty}{o}(q^{3/2})$. Considérons une solution non nulle y de l'équation $y'' + qy = 0$. Le nombre de zéro $N(x)$ de y dans l'intervalle $[0, x]$ satisfait l'équivalent*

$$N(x) \underset{x\to\infty}{\sim} \frac{1}{\pi}\int_0^x \sqrt{q}.$$

Démonstration. 1. Un premier cas inutile pour la suite : q est constant. Dans ce cas il existe des constantes A, B telles que $y(x) = A\sin(\sqrt(q)x + B$, et on peut calculer $N(x)$.

2. Considérons la fonction $\tau(x) = \int_0^x \sqrt{q}$. Puisque q est continue et strictement positive, τ est un C^1-difféomorphisme sur $[0, +\infty[$ (application C^1 strictement croissante de dérivée jamais nulle). Posons $Y = y \circ \tau^{-1}$.

3. L'équation satisfaite par Y. On a $y = Y \circ \tau$, donc $Y' = \tau' Y' \circ \tau = \sqrt{q}Y' \circ \tau$. Puis $Y'' = qY'' \circ \tau + \frac{q'}{2\sqrt{q}}Y' \circ \tau$. Ainsi

$$0 = y'' + qy = qY \circ \tau + Y'' = qY'' \circ \tau + \frac{q'}{2\sqrt{q}}Y' \circ \tau,$$

c'est-à-dire, en posant $\phi = \frac{q' \circ \tau^{-1}}{2q^{3/2} \circ \tau^{-1}} \to 0$,

$$Y'' + \phi Y' + Y = 0.$$

Maintenant Y est affecté de la constante 1, et Y' d'un petit coefficient, ce qui nous ramène presque au point 1.

4. Écriture de Y en coordonnées polaires. Puisque Y et Y' n'ont aucun zéro commun, la fonction $Y' + \mathrm{i}\, Y$ ne s'annule pas, et le théorème du relèvement C^1 garantit qu'elle s'écrit $Y' + \mathrm{i}\, Y = re^{i\theta}$, soit $Y' = r\cos(\theta)$ et $Y = r\sin\theta$. Ainsi

$$Y' = r'\sin\theta + r\theta'\cos\theta = r\cos\theta$$

et

$$Y'' = (r\cos\theta)' = r'\cos\theta - r\theta'\sin\theta = -\phi Y' - Y = -\phi r\cos\theta - r\sin\theta.$$

Ainsi on a

$$\theta' = 1 + \phi\cos\theta\sin\theta.$$

Donc θ' tend vers 1, et par intégration des relations de comparaison, $\theta(t) \sim t$.

4. Compter les zéros de Y. Puisque $Y = r\sin\theta$, le nombre de zéros $M(t)$ de Y sur $[0,t]$ est le nombre de fois où $\sin\theta(t)$ s'annule. En fait comme θ' tend vers 1, elle est strictement positive sur $[t_0,+\infty[$ et θ est strictement croissante sur $[t_0,+\infty[$ et tend vers $+\infty$.

$$M(t) \sim \#\{u \in [t_0,t] \,:\, \sin\theta(u) = 0\} = \#\{v \in [\theta(t_0),\theta(t)] \,:\, \sin v = 0\} \sim \frac{\theta(t)}{\pi} \sim \frac{t}{\pi}.$$

Enfin $N(x) = M \circ \tau(x) \sim \frac{\tau(x)}{\pi}$. □

54. Sous-espaces de $C(\mathbf{R},\mathbf{R})$ stables par translation

Référence Beck, Malick et Peyré *Objectif Agrégation.*

Leçons

- 151. Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications
- 221. Equations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications
- 228. Continuité et dérivabilité des fonctions réelles d'une variable réelle. Exemples et contre-exemples

Théorème 1. *Soit G un sous-espace vectoriel de $C(\mathbf{R},\mathbf{R})$ de dimension finie et stable par translation : pour tout $f\in G$ et $a\in\mathbf{R}$, $f(\cdot+a)\in G$. Il existe une équation différentielle scalaire d'ordre $\dim G$ dont G soit précisément l'espace des solutions.*

Démonstration. Notons n la dimension de G et considérons en une base $f_1,\dots,f_n$. Posons enfin pour $1\leqslant j\leqslant n$,

$$F_j : x\mapsto \int_0^x f_j(t)\,\mathrm{d}t.$$

La famille (f_j) étant libre, la famille (F_j) l'est aussi. Comme G est invariant par translation, il existe pour tout $a\in\mathbf{R}$ des réels $(b_{i,j}(a))$, uniques, tels que pour tout $1\leqslant i\leqslant n$,

$$f_i(\cdot+a)=\sum_{i=1}^{n} b_{i,j}(a)f_j. \tag{10}$$

Établissons qu'il existe des points $x_1,\dots,x_n\in\mathbf{R}$ tels que la matrice $A=(F_j(x_i))$ soit inversible. Posons $H=\mathrm{Vect}(F_1,\dots,F_n)$. Introduisons les formes linéaires sur H

$$\delta_x : f\mapsto f(x).$$

Clairement $\bigcap_{x\in\mathbf{R}}\ker\delta_x=\{0\}$, ce qui signifie que notant $\Delta=\mathrm{Vect}(\delta_x,x\in\mathbf{R})$, $\Delta^\perp=0$, puis, avec le théorème du rang, que $\Delta=H^*$, c'est-à-dire que $(\delta_x,x\in\mathbf{R})$ est une famille génératrice de l'espace H^* qui est de dimension n. Extrayons-en une base $(\delta_{x_1},\dots,\delta_{x_n})$. Si la matrice $A=(F_j(x_i))$ n'était pas inversible, il existerait des réels $\lambda_1,\dots,\lambda_n$ tels que pour tout j, $\sum_i\lambda_iF_i(x_j)=0$, c'est-à-dire $\delta_{x_j}\left(\sum_i\lambda_iF_i\right)=0$, ce qui contredit le fait que $(\delta_{x_1},\dots,\delta_{x_n})$ soit génératrice, ou que $(F_1,\dots,F_n)$ soit libre. La matrice $(F_i(x_j))$ est finalement inversible.

Soit $C(a)=(F_i(x_j+a)-F_i(x_j))$. Les fonctions F_i étant de classe C^1, l'application $a\mapsto C(a)$ l'est aussi. Or pour tout a,

$$C(a)=B(a)A.$$

Aussi l'application $a\mapsto B(a)=C(a)A^{-1}$ est-elle de classe C^1. Dérivant l'égalité (10), on obtient que les fonctions f_i sont de classe C^1 elles aussi, et que G est stable par dérivation.

Introduisons l'endomorphisme de dérivation sur $C^1(\mathbf{R})$, noté D. Le polynôme minimal de $D_{|G}$, noté π satisfait $\deg\pi\leqslant\dim G=n$, et $\pi(D_{|G})=0$. Autrement dit $G\subset\ker\pi(D)$. Mais le théorème de Cauchy linéaire donne $\dim\ker\pi(D)=\deg\pi$. Finalement $\deg\pi=n$ et $G=\ker\pi(D)$. □

Couplages

55. Couplages d'algèbre

101. Groupe opérant sur un ensemble. Exemples et applications.

— Théorème de la base de Burnside

— Sous-groupes finis de $\mathrm{SO}(\mathbf{R}^3)$

— Loi de réciprocité quadratique et formes quadratiques

102. Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications.

— Un théorème de Kronecker

— Théorème de structure des groupes abéliens par la théorie des caractères

— Théorème de Gauss–Wantzel

103. Exemples et applications des notions de sous-groupes distingués et de groupes quotients. Applications.

— Théorème de la base de Burnside

— Simplicité du groupe spécial orthogonal $\mathrm{SO}_n(\mathbf{R})$

104. Groupes finis. Exemples et applications.

— Théorème de la base de Burnside

— Théorème de structure des groupes abéliens par la théorie des caractères

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

— Théorème de Frobenius–Zolotarev

— Sous-groupes finis de $\mathrm{SO}(\mathbf{R}^3)$

— Automorphismes de $\mathfrak{S}_n$

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

— Sous-groupes compacts de $\mathrm{GL}(E)$

— Théorème de Frobenius–Zolotarev

— Sous-groupes finis de $\mathrm{SO}(\mathbf{R}^3)$

— Théorème de Lie–Kolchin

107. Représentations et caractères d'un groupe fini sur un C-espace vectoriel.

— Théorème de structure des groupes abéliens par la théorie des caractères

— Table de caractères de $\mathfrak{S}_4$

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

— Théorème de la base de Burnside

— Automorphismes de $\mathfrak{S}_n$

109. Représentations de groupes finis de petit cardinal.

— Théorème de structure des groupes abéliens par la théorie des caractères

— Table de caractères de $\mathfrak{S}_4$

110. Caractères d'un groupe abélien fini et transformée de Fourier discrète. Applications.

— Théorème de structure des groupes abéliens par la théorie des caractères

— **??**

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

— Théorème de structure des groupes abéliens par la théorie des caractères

— Théorèmes de Chevalley-Warning et de Erdös-Ginzburg-Ziv

— Théorème de Frobenius–Zolotarev

121. Nombres premiers. Applications.

— Théorèmes de Chevalley-Warning et de Erdös-Ginzburg-Ziv

— Loi de réciprocité quadratique et formes quadratiques

122. Anneaux principaux. Applications.

— Automorphismes de $k(X)$

— Invariants de Smith

123. Corps finis. Applications.

— Algorithme de Berlekamp

— Théorèmes de Chevalley-Warning et de Erdös-Ginzburg-Ziv

124. Anneau des séries formelles. applications.

— Théorème de Cauchy–Kowalevski

— Fractions rationnelles et Séries formelles

125. Extensions de corps. Exemples et applications.

— Théorème de Gauss–Wantzel

— Théorème de l'élément primitif

126. Exemples d'équations diophantiennes.

— Théorèmes de Chevalley-Warning et de Erdös-Ginzburg-Ziv

— Théorème de Carathéodory et équations diophantiennes

— Invariants de Smith

127. Droite projective et birapport.

140. Corps des fractions rationnelles à une indéterminée sur un corps commutatif. Applications.

— Automorphismes de $k(X)$

— Fractions rationnelles et Séries formelles

141. Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

— Algorithme de Berlekamp

— Théorème de Gauss–Wantzel

— Automorphismes de $k(X)$

142. Algèbre des polynômes à plusieurs indéterminées. Applications.

— Théorèmes de Chevalley-Warning et de Erdös-Ginzburg-Ziv

— Théorème de la borne de Bezout

143. Résultant. Applications.

— Un théorème de Kronecker

— Théorème de la borne de Bezout

144. Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.

— Méthode de Newton pour les polynômes

— Un théorème de Kronecker

150. Exemples d'actions de groupes sur les espaces de matrices.

— Sous-groupes compacts de $\mathrm{GL}(E)$

— Invariants de Smith

151. Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.

— Théorème de la base de Burnside

— Théorème de Carathéodory et équations diophantiennes

152. Déterminant. Exemples et applications.

— Théorème de Frobenius–Zolotarev

— Fractions rationnelles et Séries formelles

— Théorème de la borne de Bezout

153. Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.

— Décomposition effective de Dunford

— Réduction de Frobenius

— Adhérence des matrices codiagonalisables

154. Sous-espaces stables par un endomorphisme ou une famille d'endomorphismes d'un espace vectoriel de dimension finie. Applications.

— Théorème de Lie–Kolchin

— Réduction de Frobenius

— Adhérence des matrices codiagonalisables

155. Endomorphismes diagonalisables en dimension finie.

— Décomposition effective de Dunford

— Adhérence des matrices codiagonalisables

156. Exponentielle de matrices. Applications.

— Exponentielle d'une somme et application

— Étude topologique de $O(p,q)$

157. Endomorphismes trigonalisables. Endomorphismes nilpotents.

— Décomposition effective de Dunford

— Exponentielle d'une somme et application

— Théorème de Lie–Kolchin

158. Matrices symétriques réelles, matrices hermitiennes.

— Étude topologique de $O(p,q)$

— Convergence des méthodes de Jacobi et de Gauss-Seidel

159. Formes linéaires et hyperplans en dimension finie. Exemples et applications.

— Extrema liés, billard convexe.

— Réduction de Frobenius

160. Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie).

— Simplicité du groupe spécial orthogonal $\mathrm{SO}_n(\mathbf{R})$

— Sous-groupes compacts de $\mathrm{GL}(E)$

161. Isométries d'un espace affine euclidien de dimension finie. Applications en dimension 2 et 3.

— Simplicité du groupe spécial orthogonal $\mathrm{SO}_n(\mathbf{R})$

— Sous-groupes finis de $\mathrm{SO}(\mathbf{R}^3)$

162. Systèmes d'équations linéaires ; opérations, aspects algorithmiques et conséquences théoriques.

— Invariants de Smith

— Convergence des méthodes de Jacobi et de Gauss-Seidel

170. Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.

— Loi de réciprocité quadratique et formes quadratiques

— Ellipsoide de John-Lowner

171. Formes quadratiques réelles. Exemples et applications.

— Étude topologique de $O(p,q)$

— Ellipsoide de John-Lowner

180. Coniques. Applications.

181. Barycentres dans un espace affine réel de dimension finie, convexité. Applications.

— Sous-groupes compacts de $\mathrm{GL}(E)$

— Théorème de Carathéodory et équations diophantiennes

182. Applications des nombres complexes à la géométrie.

— Théorème de Gauss–Wantzel

183. Utilisation des groupes en géométrie.

— Théorème de Gauss–Wantzel

— Sous-groupes finis de $\mathrm{SO}(\mathbf{R}^3)$

190. Méthodes combinatoires, problèmes de dénombrement.

— Un théorème de Kronecker

— Sous-groupes finis de $\mathrm{SO}(\mathbf{R}^3)$

— Loi de réciprocité quadratique et formes quadratiques

56. Couplages d'analyse

201. Espaces de fonctions. Exemples et applications.

— Théorème de Prokhorov

— Construction du pré-mouvement brownien

202. Exemples de parties denses et applications.

— Espérance conditionnelle et convergence L^p

— Théorème de Prokhorov

203. Utilisation de la notion de compacité.

— Théorème de Prokhorov

— Théorème de Brouwer

— Existence de géodésiques.

— Sous-groupes compacts de $\mathrm{GL}(E)$

204. Connexité. Exemples et applications.

— Théorème de Brouwer

— Simplicité du groupe spécial orthogonal $\mathrm{SO}_n(\mathbf{R})$

205. Espaces complets. Exemples et applications.

— Théorème de Prokhorov

— Théorèmes de l'application ouverte et du graphe fermé.

206. Théorèmes de point fixe. Exemples et applications.

— Sous-groupes compacts de $\mathrm{GL}(E)$

— Théorème de Brouwer

207 Prolongement de fonctions. Exemples et applications

— Théorème de Steinhaus

— Théorème de Joris

208. Espaces vectoriels normés, applications linéaires continues. Exemples.

— Sous-groupes compacts de $\mathrm{GL}(E)$

— Théorèmes de l'application ouverte et du graphe fermé.

209. Approximation d'une fonction par des polynômes et des polynômes trigonométriques. Exemples et applications.

— Polynômes de Bernstein

— Principe de localisation

— Équation de la chaleur sur le cercle

213. Espaces de Hilbert. Bases hilbertiennes. Exemples et applications.

— Construction du pré-mouvement brownien

— Équation de la chaleur sur le cercle

214. Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications.

— Théorème de Brouwer

— Extrema liés, billard convexe.

215. Applications différentiables définies sur un ouvert de $\mathbf{R}^n$. Exemples et applications.

— Théorème de Brouwer

— Extrema liés, billard convexe.

217. Sous-variétés de $\mathbf{R}^n$. Exemples.

— Extrema liés, billard convexe.

— Simplicité du groupe spécial orthogonal $\mathrm{SO}_n(\mathbf{R})$

218. Applications des formules de Taylor.

— Méthode de Newton pour les polynômes

— Théorème de Joris

219. Extremums : existence, caractérisation, recherche. Exemples et applications.

— Existence de géodésiques.

— Extrema liés, billard convexe.

220. Équations différentielles $X' = f(t, X)$. Exemples d'étude des solutions en dimension 1 et 2.

— Théorème de Cauchy–Kowalevski

— Nombre de zéros d'une équation différentielle

221. Equations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications.

— Nombre de zéros d'une équation différentielle

— Sous-espaces de $C(\mathbf{R}, \mathbf{R})$ stables par translation

222. Exemples d'équations aux dérivées partielles linéaires

— Équation de la chaleur sur le cercle

— **??**

223. Suites numériques. Convergence, valeurs d'adhérence. Exemples et applications.

— Théorème de Sarkowski

— Méthode de Newton pour les polynômes

— Processus de branchement critique

224. Exemples de développements asymptotiques de suites et de fonctions.

— Méthode de Newton pour les polynômes

— Nombre de zéros d'une équation différentielle

226. Suites vectorielles et réelles définies par une relation de récurrence $u_{n+1} = f(u_n)$. Exemples et applications.

— Processus de branchement critique

— Nombre de zéros d'une équation différentielle

228. Continuité et dérivabilité des fonctions réelles d'une variable réelle. Exemples et contre-exemples.

— Théorème de Sarkowski

— Polynômes de Bernstein

— Théorème de Joris

229. Fonctions monotones. Fonctions convexes. Exemples et applications.

— Processus de branchement critique

— Lemme d'Artin, $\int_0^1 \log \Gamma$ et formules de multiplication.

230. Séries de nombres réels ou complexes. Comportement des restes ou des sommes partielles des séries numériques. Exemples.

— Inégalité de Carleman et une application.

— Théorème taubérien fort de Hardy et Littlewood

232. Méthodes d'approximation des solutions d'une équation $F(X) = 0$. Exemples.

— Méthode de Newton pour les polynômes

— Méthode QR

233. Analyse numérique matricielle : résolution approchée de systèmes linéaires, recherche de vecteurs propres, exemples.

— Méthode QR

— Convergence des méthodes de Jacobi et de Gauss-Seidel

234. Espaces L^p, $1 \leqslant p \leqslant +\infty$.

— Construction du pré-mouvement brownien

— Espérance conditionnelle et convergence L^p

235. Problèmes d'interversion de limites et d'intégrales.

— Inégalité de Gross

— Espérance conditionnelle et convergence L^p

— Équation de la chaleur sur le cercle

— ((Principe de localisation))

— ((Théorèmes de Morera, de Weierstrass et d'Osgood))

236. Illustrer par des exemples quelques méthodes de calcul d'intégrales de fonctions d'une ou plusieurs variables réelles.

— Lemme d'Artin, $\int_0^1 \log\Gamma$ et formules de multiplication.

— Un calcul d'intégrale

239. Fonctions définies par une intégrale dépendant d'un paramètre. Exemples et applications.

— Inégalité de Hoeffding

— Équation de la chaleur sur le cercle

— ((Lemme d'Artin, $\int_0^1 \log\Gamma$ et formules de multiplication.))

240. Produit de convolution, transformation de Fourier. Applications.

— Théorème de Lévy

241. Suites et séries de fonctions. Exemples et contre-exemples.

— Théorème de Steinhaus

— Construction du pré-mouvement brownien

— Processus de branchement critique

— Théorèmes de Morera, de Weierstrass et d'Osgood

243. Convergence des séries entières, propriétés de la somme. Exemples et applications.

— Théorème de Steinhaus

— Processus de branchement critique

— Théorème taubérien fort de Hardy et Littlewood

— Théorème de Cauchy–Kowalevski

244. Fonctions développables en série entière, fonctions analytiques. Exemples.

— Théorème de Steinhaus

— Théorème de Cauchy–Kowalevski

245. Fonctions holomorphes sur un ouvert de C. Exemples et applications.

— Théorème de Steinhaus

— Un calcul d'intégrale

— Théorèmes de Morera, de Weierstrass et d'Osgood

246. Séries de Fourier. Exemples et applications.

— Principe de localisation

— Équation de la chaleur sur le cercle

247. Exemples de problèmes d'interversion de limites.

— Théorème taubérien fort de Hardy et Littlewood

— Équation de la chaleur sur le cercle

— Théorèmes de Morera, de Weierstrass et d'Osgood

249. Suites de variables de Bernoulli indépendantes.

— Polynômes de Bernstein

— Inégalité de Gross

253. Utilisation de la notion de convexité en analyse.

— Théorème de Brouwer

— Sous-groupes compacts de $\mathrm{GL}(E)$

254. Espaces de Schwartz $S(\mathbf{R}^d)$ et distributions tempérées. Transformation de Fourier dans $S(\mathbf{R}^d)$ et $S'(\mathbf{R}^d)$.

260. Espérance, variance et moments d'une variable aléatoire.

— Inégalité de Gross

— Processus de branchement critique

261. Fonction caractéristique et transformée de Laplace d'une variable aléatoire. Exemples et applications.

— Processus de branchement critique

— Théorème de Lévy

262. Modes de convergence d'une suite de variables aléatoires. Exemples et applications.

— Théorème de Prokhorov ou Théorème de Lévy

— Processus de branchement critique

— Construction du pré-mouvement brownien

263. Variables aléatoire à densité. Exemples et applications.

— Théorème de Steinhaus

— Construction du pré-mouvement brownien

— Inégalité de Gross

264. Variables aléatoire discrètes. Exemples et applications.

— Polynômes de Bernstein

— Processus de branchement critique

— Inégalité de Gross