
Couplages agrégation 2023

Geoffrey Deperle

Algèbre - Géométrie

- **101 : Groupe opérant sur un ensemble. Exemples et applications.**
 - Automorphismes de S_n
 - Décomposition de Bruhat
- **102 : Groupe des nombres complexes de module 1. Racines de l'unité. Applications.**
 - Théorème de Dirichlet faible
 - Morphismes continus de S^1 dans $GL_n(\mathbb{R})$
- **103 : Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications.**
 - SO_3 et les quaternions
 - Automorphismes de S_n
- **104 : Groupes finis. Exemples et applications.**
 - Isométries du cube et coloriage
 - Automorphismes de S_n
- **105 : Groupe des permutations d'un ensemble fini. Applications.**
 - Décomposition de Bruhat
 - Automorphismes de S_n
- **106 : Groupe linéaire d'un espace vectoriel de dimension finie E , sous-groupes de $GL(E)$. Applications.**
 - Décomposition de Bruhat
 - Morphismes continus de (S^1, \times) dans $(GL_n(\mathbb{R}), \times)$
- **108 : Exemples de parties génératrices d'un groupe. Applications.**
 - SO_3 et les quaternions
 - Automorphismes de S_n
- **120 : Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.**
 - Théorème de Dirichlet faible
 - Théorème chinois : cas général
- **121 : Nombres premiers. Applications.**
 - Théorème de Dirichlet faible
 - Nombres premiers de forme $p = x^2 + 3y^2$
- **122 : Anneaux principaux. Exemples et applications.**
 - Nombres premiers de forme $p = x^2 + 3y^2$
 - Forme normale de Smith
- **123 : Corps finis. Applications.**
 - Lemme de Fitting et cardinal du cône nilpotent
 - Dénombrement des polynômes irréductibles sur \mathbb{F}_q
- **125 : Extensions de corps. Exemples et applications.**
 - Théorème de Springer
 - Dénombrement des polynômes irréductibles sur \mathbb{F}_q
- **126 : Exemples d'équations en arithmétique.**
 - Nombres premiers de forme $p = x^2 + 3y^2$
 - Théorème chinois : cas général
- **141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.**
 - Dénombrement des polynômes irréductibles sur \mathbb{F}_q
 - Théorème de Springer
- **142 : PGCD et PPCM, algorithmes de calcul. Applications.**

- Forme normale de Smith
- Théorème chinois : cas général
- **144 : Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.**
 - Dénombrement des polynômes irréductibles sur \mathbb{F}_q
 - Formes de Hankel
- **148 : Exemples de décomposition de matrices. Applications.**
 - Homéomorphisme $\exp : S_n(\mathbb{R}) \rightarrow S_n^{++}(\mathbb{R})$ et décomposition polaire
 - Décomposition de Bruhat
- **149 : Valeurs propres, vecteurs propres. Calculs exacts ou approchés d'éléments propres. Applications.**
 - Déterminant circulant et suite de polygones
 - Morphismes continus de (S^1, \times) dans $(GL_n(\mathbb{R}), \times)$
- **151 : Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.**
 - Formes de Hankel
 - Réduction de Jordan par la dualité
- **152 : Déterminant. Exemples et applications.**
 - Théorème de Sylvester
 - Déterminant circulant et suite de polygones
- **153 : Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.**
 - Lemme de Fitting et cardinal du cône nilpotent
 - Déterminant circulant et suite de polygones
- **154 : Sous-espaces stables par un endomorphisme ou une famille d'endomorphisme en dimension finie. Applications.**
 - Lemme de Fitting et cardinal du cône nilpotent
 - Réduction de Jordan par la dualité
- **155 : Endomorphismes diagonalisables en dimension finie.**
 - Déterminant circulant et suite de polygones
 - Morphismes continus de (S^1, \times) dans $(GL_n(\mathbb{R}), \times)$
- **156 : Exponentielle de matrices. Applications.**
 - Homéomorphisme $\exp : S_n(\mathbb{R}) \rightarrow S_n^{++}(\mathbb{R})$ et décomposition polaire
 - Morphismes continus de (S^1, \times) dans $(GL_n(\mathbb{R}), \times)$
- **157 : Endomorphismes trigonalisables. Endomorphismes nilpotents.**
 - Lemme de Fitting et cardinal du cône nilpotent
 - Réduction de Jordan par la dualité
- **158 : Matrices symétriques réelles, matrices hermitiennes.**
 - Homéomorphisme $\exp : S_n(\mathbb{R}) \rightarrow S_n^{++}(\mathbb{R})$ et décomposition polaire
 - Théorème de Sylvester
- **159 : Formes linéaires et dualité en dimension finie. Exemples et applications.**
 - Formes de Hankel
 - Réduction de Jordan par la dualité
- **160 : Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie).**
 - Homéomorphisme $\exp : S_n(\mathbb{R}) \rightarrow S_n^{++}(\mathbb{R})$ et décomposition polaire
 - SO_3 et les quaternions
- **161 : Distances dans un espace affine euclidien. Isométries.**
 - SO_3 et les quaternions

- Isométries du cube et coloriage
- **162 : Systèmes d'équations linéaires ; opérations élémentaires, aspects algorithmiques et conséquences théoriques.**
 - Décomposition de Bruhat
 - Forme normale de Smith
- **170 : Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie.**
 - Théorème de Springer
 - Formes de Hankel
- **171 : Formes quadratiques réelles. Coniques. Exemples et applications.**
 - Théorème de Sylvester
 - Formes de Hankel
- **181 : Barycentres dans un espace affine réel de dimension finie, convexité. Applications.**
 -
 -
- **190 : Méthodes combinatoires, problèmes de dénombrement.**
 - Automorphismes de S_n
 - Dénombrement des polynômes irréductibles sur \mathbb{F}_q
- **191 : Exemples d'utilisation de techniques d'algèbre en géométrie.**
 - SO_3 et les quaternions
 - Déterminant circulant et suite de polygones

Analyse

- **201 : Espaces de fonctions. Exemples et applications.**
 - Représentation des fonctions lipschitziennes
 - Théorème de Riesz-Fréchet-Kolmogorov
- **203 : Utilisation de la notion de compacité.**
 - Théorème du point fixe de Brouwer
 - Théorème de Riesz-Fréchet-Kolmogorov
- **204 : Connexité. Exemples et applications.**
 - Théorème du point fixe de Brouwer
 - Théorème d'Hadamard-Lévy
- **205 : Espaces complets. Exemples et applications.**
 - Représentation des fonctions lipschitziennes
 - Théorème de Stampacchia
- **206 : Exemples d'utilisation de la notion de dimension finie en analyse.**
 - Théorème du point fixe de Brouwer
 - Théorème de Korovkin
- **208 : Espaces vectoriels normés, applications linéaires continues. Exemples**
 - Représentation des fonctions lipschitziennes
 - Théorème de Stampacchia
- **209 : Approximation d'une fonction par des fonctions régulières. Exemples et applications.**
 - Théorème de Korovkin
 - Théorème de Riesz-Fréchet-Kolmogorov
- **213 : Espaces de Hilbert. Bases hilbertiennes. Exemples et applications.**
 - Optimisation dans un Hilbert

- Théorème de Stampacchia
- **214 : Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications en analyse et en géométrie.**
 - Théorème d'Hadamard-Lévy
 - Théorème du point fixe de Brouwer
- **215 : Applications différentiables définies sur un ouvert de \mathbb{R}^N . Exemples et applications.**
 - Algorithme de descente de gradient
 - Théorème du point fixe de Brouwer
- **219 : Extremums : existence, caractérisation, recherche. Exemples et applications.**
 - Optimisation dans un Hilbert
 - Algorithme de descente de gradient
- **220 : Équations différentielles ordinaires. Exemples de résolution et d'études de solutions en dimension 1 et 2.**
 - Théorème d'Hadamard-Lévy
 - Équation de Bessel
- **221 : Équations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications.**
 - Résolution de $-u'' + u = f$ sur le cercle
 - Équation de Bessel
- **223 : Suites numériques. Convergence, valeurs d'adhérence. Exemples et applications.**
 - Équivalent d'une suite définie par récurrence
 - Méthode de Newton pour les polynômes
- **224 : Exemples de développements asymptotiques de suites et de fonctions.**
 - Équivalent d'une suite définie par récurrence
 - Méthode de Newton pour les polynômes
- **226 : Suites vectorielles et réelles définies par une relation de récurrence $u_{n+1} = f(u_n)$. Exemples. Applications à la résolution approchée d'équations.**
 - Méthode de Newton pour les polynômes
 - Algorithme de descente de gradient
- **228 : Continuité, dérivabilité des fonctions réelles d'une variable réelle. Exemples et applications.**
 - Représentation des fonctions lipschitziennes
 - Méthode de Newton pour les polynômes
- **229 : Fonctions monotones. Fonctions convexes. Exemples et applications.**
 - Optimisation dans un Hilbert
 - Algorithme de descente de gradient
- **230 : Séries de nombres réels ou complexes. Comportement des restes ou des sommes partielles des séries numériques. Exemples**
 - Équivalent d'une suite définie par récurrence
 - Méthode de Newton pour les polynômes
- **234 : Fonctions et espaces de fonctions Lebesgue-intégrables**
 - Théorème de Riesz-Fréchet-Kolmogorov
 - Représentation des fonctions lipschitziennes
- **235 : Problèmes d'interversion en analyse.**
 - Prolongement de la fonction Gamma et formule de Weierstrass
 - Calcul de l'intégrale de Dirichlet
- **236 : Illustrer par des exemples quelques méthodes de calcul d'intégrales de fonc-**

- tions d'une ou plusieurs variables.**
- Prolongement de la fonction Gamma et formule de Weierstrass
- Calcul de l'intégrale de Dirichlet
- **239 : Fonctions définies par une intégrale dépendant d'un paramètre. Exemples et applications.**
- Prolongement de la fonction Gamma et formule de Weierstrass
- Calcul de l'intégrale de Dirichlet
- **241 : Suites et séries de fonctions. Exemples et contre-exemples**
- Théorème de Korovkin
- Formule sommatoire de Poisson et formule de Shannon
- **243 : Séries entières, propriétés de la somme. Exemples et applications.**
- Indécomposabilité de la loi de Poisson
- Équation de Bessel
- **245 : Fonctions d'une variable complexe. Exemples et applications.**
- Prolongement de la fonction Gamma et formule de Weierstrass
- Indécomposabilité de la loi de Poisson
- **246 : Séries de Fourier. Exemples et applications.**
- Formule sommatoire de Poisson et formule de Shannon
- Résolution de $-u'' + u = f$ sur le cercle
- **250 : Transformation de Fourier. Applications.**
- Formule sommatoire de Poisson et formule de Shannon
- Théorème de Lévy et TCL
- **253 : Utilisation de la notion de convexité en analyse.**
- Optimisation dans un Hilbert
- Algorithme de descente de gradient
- **261 : Loi d'une variable aléatoire : caractérisations, exemples, applications.**
- Inégalité de Hoeffding et applications
- Théorème de Lévy et TCL
- **262 : Convergences d'une suite de variables aléatoires. Théorèmes limite. Exemples et applications.**
- Inégalité de Hoeffding et applications
- Théorème de Lévy et TCL
- **264 : Variables aléatoires discrètes. Exemples et applications.**
- Inégalité de Hoeffding et applications
- Indécomposabilité de la loi de Poisson
- **265 : Exemples d'études et d'applications de fonctions usuelles et spéciales.**
- Prolongement de la fonction Gamma et formule de Weierstrass
- Équation de Bessel
- **266 : Illustration de la notion d'indépendance en probabilités.**
- Inégalité de Hoeffding et applications
- Indécomposabilité de la loi de Poisson
- **267 : Exemples d'utilisation de courbes en dimension 2 ou supérieure.**
-
-

Automorphisme de S_n

Geoffrey Deperle

Leçons associées :

- 101 : Groupe opérant sur un ensemble. Exemples et applications.
- 103 : Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients.
- 104 : Groupes finis. Exemples et applications.
- 105 : Groupes de permutation d'un ensemble fini.
- 108 : Exemples de parties génératrices d'un groupe.
- 190 : Méthodes combinatoires, problème de dénombrement.

Le but de ce développement est de montrer le théorème suivant :

Théorème. *Pour $n \neq 6$, tout automorphisme de S_n est intérieur.*

Idee générale : Un automorphisme de S_n préserve seulement les propriétés algébriques (ordre d'un élément, commutation) mais pas forcément les propriétés géométriques liées à l'action naturelle sur $\{1, \dots, n\}$. Pour des raisons de cardinal, quand $n \neq 6$, les propriétés géométriques seront également conservées.

Lemme 1. *Soit $\varphi \in \text{Aut}(S_n)$, si φ transforme toute transposition en transposition alors φ est intérieur.*

Preuve du lemme : Soit φ un tel automorphisme,

S_n est engendré par les transpositions $(\tau_i)_{i \in \llbracket 2, n \rrbracket}$ avec pour tout $i \geq 2$, $\tau_i = (1\ i)$. Comme les τ_i ne commutent pas, il en va de même pour les $\varphi(\tau_i)$ donc le support des transpositions $\varphi(\tau_i)$ ne sont pas deux à deux disjoints.

Notons $\varphi(\tau_2) = (\alpha_1\ \alpha_2)$, alors $\varphi(\tau_3)$ est de la forme $\varphi(\tau_3) = (\alpha_1\ \alpha_3)$ et de même pour $i \geq 3$, $\varphi(\tau_i)$ ne commute pas avec les $\varphi(\tau_j)$ pour $j < i$ donc $\varphi(\tau_i)$ est de la forme $\varphi(\tau_i) = (\alpha_1\ \alpha_i)$. Les α_i sont deux à deux disjoints donc $\{\alpha_1, \dots, \alpha_n\} = \llbracket 1, n \rrbracket$ et $\alpha : i \mapsto \alpha_i$ est une permutation vérifiant pour tout $i \in \llbracket 1, n \rrbracket$, $\alpha\tau_i\alpha^{-1} = (\alpha_1\ \alpha_i) = \varphi(\tau_i)$ donc φ est un automorphisme intérieur. \square

Soit φ un automorphisme de S_n , il envoie les classes de conjugaison sur des classes de conjugaison donc il envoie les transpositions sur une classe de conjugaison constitué d'éléments d'ordre 2. Dénombrons le cardinal de chaque classe de conjugaison :

Lemme 2. Soit Ω une classe de conjugaison de S_n et $\sigma \in \Omega$, supposons que la décomposition en cycle à support disjoint de σ possède k_i cycle de longueur i , alors

$$\text{Card}(\Omega) = \frac{n!}{\prod_{i=1}^n k_i! i^{k_i}}$$

Preuve du lemme : Le groupe S_n agit transitivement sur Ω par conjugaison donc

$$\text{Card}(\Omega) = \frac{\text{Card}(S_n)}{\text{Card}(\text{Stab}(\sigma))}$$

Or, comme $\tau(a_1 \dots a_i) \tau^{-1} = (\tau(a_1) \dots \tau(a_i))$, $\tau \in \text{Stab}(\sigma)$ si et seulement si

- τ permute les cycles de même longueur : $k_i!$ possibilités.
- τ réalise une permutation cyclique sur chaque cycle donc il y a : $\underbrace{i \times \dots \times i}_{k_i \text{ fois}} = i^{k_i}$ possibilités

Donc $\text{Card}(\text{Stab}(\sigma)) = \prod_{i=1}^n k_i! i^{k_i}$ d'où le résultat. □

Preuve du théorème : Les classes de conjugaison constituées d'éléments d'ordre 2 sont les classes de conjugaison de produit de k transpositions.

Par l'absurde, si φ est un automorphisme non intérieur, il existe $k \geq 2$ tel que le cardinal de l'ensemble des transpositions est égal au cardinal de l'ensemble des produits de k transpositions. D'où d'après le lemme 2 :

$$\binom{n}{2} = \frac{n!}{2^k k! (n-2k)!}$$

Or,

$$\begin{aligned} \frac{n!}{2(n-2)!} = \frac{n!}{2^k k! (n-2k)!} &\iff \frac{(n-2)!}{2^{k-1} k! (n-2k)!} = 1 \\ &\iff \frac{\binom{n-2}{2k-2} (2k-2)!}{2^{k-1} k!} = 1 \\ &\iff \frac{\binom{n-2}{2k-2} (2k-3)(2k-5)}{k} = 1 \end{aligned}$$

- Si $k > 3$, on a $2k-3 > k$ donc absurde.
- Si $k = 2$, on a $\frac{1}{2} \binom{n-2}{2} \iff (n-2)(n-3) = 4$ ce qui est absurde car deux entiers consécutifs ne peuvent être pairs tous les deux.
- Si $k = 3$, $\binom{n-2}{4} = 1$ donc $n = 6$.

□

Remarque 1. On peut montrer qu'il existe bien des automorphismes non intérieurs dans S_6 .

Critère de Sylvester pour la signature

Geoffrey Deperle

Leçons associées :

- 152 : Déterminant. Exemples et applications.
- 158 : Matrices symétriques réelles, matrices hermitiennes.
- 171 : Formes quadratiques réelles. Coniques. Exemples et applications.

Le but de ce développement est de montrer le théorème suivant :

Théorème. Soit A une matrice symétrique (de mineurs non nuls) de taille n . Notons Δ_k le mineur principal de taille k de M .

(i) M est définie positive $\iff \forall k \in \llbracket 1, n \rrbracket, \Delta_k > 0$

(ii) En posant

— $\varepsilon_k = \frac{\Delta_k}{|\Delta_k|}$ (signe de Δ_k)

— $\sigma_k = \frac{\varepsilon_k}{\varepsilon_{k-1}} \in \{\pm 1\}$ (changement de signe entre Δ_{k-1} et Δ_k)

La signature de M est (r, s) où r est le nombre de 1 et s est le nombre de -1 de la suite (σ_k) .

Preuve :

(i) On note (e_1, \dots, e_n) la base canonique de \mathbb{R}^n et q la forme quadratique associée à M : on a pour tout $X \in \mathbb{R}^n, q_M(X) = {}^t X M X$.

(\Leftarrow) Si q est définie positive, il en est de même que $q|_{\text{Vect}(e_1, \dots, e_k)}$ pour tout $k \in \llbracket 1, n \rrbracket$. Or, la matrice extraite M_k obtenue en extrayant les k premières lignes et les k premières colonnes est la matrice de cette restriction, donc $\Delta_k > 0$.

(\Rightarrow) : On procède par récurrence sur n ,

— Le résultat est vrai pour $n = 1$,

— Supposons $n \geq 2$, tel que $\forall k \in \llbracket 1, n \rrbracket, \Delta_k > 0$, par hypothèse de récurrence, $q|_{\text{Vect}(e_1, \dots, e_{n-1})}$ est définie positive.

Soit $G = F^\perp$,

Comme q est non dégénérée (car $\det M = \Delta_n > 0$), sa dimension est 1.

Si $x \in F \cap G$, x est isotrope donc nul car q est définie positive sur F , d'où $\mathbb{R}^n = F \oplus G$.

Soit (e'_1, \dots, e'_{n-1}) une base orthonormale de F pour q et ε_n un vecteur non nul de G . En notant P la matrice de passage des e_i aux ε_i , matrice de q_M dans $(\varepsilon_1, \dots, \varepsilon_n)$,

$${}^t P M P = \begin{pmatrix} 1 & & (0) \\ & \ddots & \\ & & 1 \\ (0) & & & \alpha \end{pmatrix}$$

En appliquant le déterminant à cette relation, on a $\alpha = (\det P)^2(\det M) = (\det P)\Delta_n > 0$ donc q_A est définie positive donc M est définie positive.

(ii) On procède par récurrence sur n ,

— Pour $n = 1$, on a $M = (\Delta_1)$ donc $\sigma_1 = \text{signe}(\Delta_1)$ d'où $\text{sgn}(M) = (1, 0)$ ou $\text{sgn}(M) = (0, 1)$ selon le signe de M .

— Soit $n \in \mathbb{N}$, supposons le résultat vrai jusqu'à l'ordre $n - 1$,

La sous-matrice M_{n-1} est symétrique de signature (r_{n-1}, s_{n-1}) . Considérons $H = \text{Vect}(e_1, \dots, e_{n-1})$,

Il existe $P_{n-1} \in \text{GL}_{n-1}(\mathbb{R})$ telle que ${}^t P_{n-1} M_{n-1} P_{n-1} = \begin{pmatrix} I_{r_{n-1}} & 0 \\ 0 & -I_{s_{n-1}} \end{pmatrix}$ et donc on a

$\varepsilon_{n-1} = (-1)^{s_{n-1}}$.

Avec (e'_1, \dots, e'_{n-1}) la base orthonormalisée de H , comme Δ_{n-1} est non nul, $q|_H$ est non dégénérée d'où $\mathbb{R}^n = H \oplus \mathbb{R}e'_n$ d'où la matrice de q dans la base (e'_1, \dots, e'_n) est de la forme :

$$\begin{pmatrix} I_{r_{n-1}} & & \\ & -I_{s_{n-1}} & \\ & & q(e'_n) \end{pmatrix} = {}^t Q \begin{pmatrix} I_{r_{n-1}} & & \\ & -I_{s_{n-1}} & \\ & & \xi_n \end{pmatrix} Q$$

avec $Q = \begin{pmatrix} I_{r_{n-1}} & & \\ & I_{s_{n-1}} & \\ & & \sqrt{\xi_n q(e'_n)} \end{pmatrix}$ et avec ξ_n le signe de $q(e'_n)$ (non nul).

Ainsi la matrice est congruente à $\begin{pmatrix} I_{r_{n-1}} & & \\ & -I_{s_{n-1}} & \\ & & \xi_n \end{pmatrix}$ de Sylvester donc de déterminant de

même signe que Δ_n :

$$(-1)^{s_{n-1}} \xi_n = \varepsilon_n$$

d'où $\varepsilon_{n-1} \xi_n = \varepsilon_n$ et $\xi_n = \delta_n$ d'où le résultat. □

Application. $S_n^{++}(\mathbb{R})$ est un ouvert de $S_n(\mathbb{R})$

Preuve : On a $S_n^{++}(\mathbb{R}) = \bigcap_{k=1}^r \Delta_k^{-1}(\mathbb{R}^{+*})$ avec Δ_k l'application donnant mineur de taille k qui est continue par continuité du déterminant. Ainsi, $S_n^{++}(\mathbb{R})$ est un ouvert de $S_n(\mathbb{R})$ en tant qu'intersection finie d'ouverts de $S_n(\mathbb{R})$ □

Décomposition de Bruhat

Geoffrey Deperle

Leçons associées :

- 101 : Groupe opérant sur un ensemble. Exemples et applications.
- 105 : Groupe de permutations d'un ensemble fini. Applications.
- 106 : Groupe linéaire d'un espace vectoriel de dimension finie E , sous-groupes de $GL(E)$. Applications.
- Système d'équations linéaires ; opérations élémentaires, aspects algorithmiques et conséquences théoriques.

Le but de ce développement est de montrer le théorème suivant :

Théorème. Soit $A \in GL_n(\mathbb{K})$, il existe T_1, T_2 triangulaires supérieures et un unique $\sigma \in S_n$ tel que $A = T_1 P_\sigma T_2$.

Preuve :

Existence de la décomposition de Bruhat

Notons (E_{ij}) la base canonique, \mathcal{T}_S l'ensemble des matrices triangulaire supérieures de $\mathcal{M}_n(\mathbb{K})$.

Pour tout $i < j$ dans $\llbracket 1, n \rrbracket$, $\lambda \in \mathbb{K}$, $\alpha \neq 0$ on définit :

- $T_{ij}(\lambda) = I_n + \lambda E_{ij} \in \mathcal{T}_S$
- $D_i(\alpha) = I_n + (\alpha - 1)E_{ii} \in \mathcal{T}_S$

Soit $A \in GL_n(\mathbb{K})$,

Soit $i_1 = \max\{k \in \llbracket 1, n \rrbracket \mid a_{k,i} \neq 0\}$ (existe car $A \in GL_n(\mathbb{K})$).

(i) $\forall k < i_1$, on multiplie à gauche par

$$T_{k,i_1} \left(-\frac{a_{k,1}}{a_{i_1,1}} \right) \left(L_k \leftarrow L_k - \frac{a_{k,1}}{a_{i_1,1}} L_{i_1} \right) \begin{pmatrix} 0 \\ \vdots \\ 0 \\ a_{i_1,1} \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad (*)$$

(ii) On multiplie à gauche par

$$D_{i_1} \left(\frac{1}{a_{i_1,1}} \right) \quad (L_{i_1} \leftarrow \frac{1}{a_{i_1,1}} L_{i_1}) \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad (*)$$

(iii) $\forall k \in \llbracket 2, n \rrbracket$, on multiplie à droite par

$$T_{i,k}(-a_{i_1,k}) \quad (C_k \leftarrow C_k - a_{i_1,k} C_1) \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

On itère cet algorithme aux autres colonnes et on construit alors une suite (i_1, \dots, i_n) avec $j \mapsto i_j$ injective de $\llbracket 1, n \rrbracket$ dans $\llbracket 1, n \rrbracket$ donc bijective.

Soit $\sigma \in S_n$ la permutation telle que $\forall k \in \llbracket 1, n \rrbracket, \sigma(k) = i_k$ et on lui associe la matrice de permutation P_σ . On a donc par construction $P_\sigma = T_1 A T_2$ d'où l'existence.

Unicité de la décomposition

Soit $A = T_1 P_\sigma T_2 = T'_1 P_\tau T'_2$ avec σ, τ deux permutations de S_n et $T_1, T_2, T'_1, T'_2 \in \mathcal{T}_S$.

On a

$$P_\tau^{-1} \underbrace{(T'_1 T_1)}_{:=T} P_\sigma = \underbrace{T'_2 T_2^{-1}}_{:=\tilde{T}}$$

Par l'absurde si $\sigma \neq \tau$, il existe $i \in \llbracket 1, n \rrbracket$ tel que $\sigma(i) < \tau(i)$,

La $\sigma(i)$ -ème colonne de T est alors $\begin{pmatrix} (*) \\ T_{\sigma(i),\sigma(i)} \\ 0 \\ \vdots \\ 0 \\ T_{\tau(i),\sigma(i)} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ donc $0 \neq \tilde{T}_{ii} = T_{\tau(i),\sigma(i)} = 0$.

Absurde, donc $\sigma = \tau$.

□

Application. Soit $A \in \text{GL}_n(\mathbb{K})$ et $d = (F_0, \dots, F_n)$ un drapeau de \mathbb{K}^n .

Alors $A \cdot d := (A(F_0), \dots, A(F_n))$ est également un drapeau et définit une action de $\text{GL}_n(\mathbb{K})$ sur l'ensemble \mathcal{D} des drapeaux. On peut définir de même une action de A sur les couples de drapeau par $A \cdot (d, d') = (A \cdot d, A \cdot d')$.

Le nombre d'orbite de l'action sur les couples de drapeau est $n!$.

Étape 1 : Montrons que $\mathcal{D} \simeq \text{GL}_n(\mathbb{K})/T_S$

Montrons que cette action est transitive,

Soit (e_1, \dots, e_n) la base canonique de \mathbb{K}^n et δ le drapeau formé des $(\text{Vect}(e_1, \dots, e_k))_{k \in [0, n]}$.

Pour $d = (F_0, \dots, F_n)$ un drapeau quelconque, on peut trouver une base (f_1, \dots, f_n) de \mathbb{K}^n telle que $\forall k \in [1, n], (f_1, \dots, f_k)$ est une base de F_k .

L'unique matrice A vérifiant $Ae_i = f_i$ est inversible et vérifie $A \cdot \delta = d$.

Comme l'action est transitive, \mathcal{D} est en bijection avec $\text{GL}_n(\mathbb{K})/G_\delta$ avec G_δ le stabilisateur de δ .

Or, on a pour $A \in \text{GL}_n(\mathbb{K})$ $A \cdot \delta = \delta \iff A$ est triangulaire supérieure, d'où $G_\delta = T_S$ et $\mathcal{D} \simeq \text{GL}_n(\mathbb{K})/T_S$.

Étape 2 : Identifions une action de $\text{GL}_n(\mathbb{K})$ sur $\text{GL}_n(\mathbb{K})/T_S \times \text{GL}_n(\mathbb{K})/T_S$

Pour $d \in \mathcal{D}$, $B \in \text{GL}_n(\mathbb{K})$, tel que $d = B \cdot \delta$, en identifiant d avec \overline{B} de G/T_S , pour $A \in \text{GL}_n(\mathbb{K})$, on a $A \cdot \overline{B} = \overline{AB}$ qui s'identifie à $AB \cdot \delta = A \cdot d$. On définit une action de $\text{GL}_n(\mathbb{K})$ sur $\text{GL}_n(\mathbb{K})/T_S \times \text{GL}_n(\mathbb{K})/T_S$ se traduit sur les couples de drapeaux par l'action $A \cdot (d, d') = (A \cdot d, A \cdot d')$.

Étape 3 : Dénombrons le nombre d'orbite en montrant que chaque orbite contient un unique élément de la forme $(\overline{I_n}, \overline{P_\sigma})$

Soit $X, Y \in \text{GL}_n(\mathbb{K})$, on a $(\overline{X}, \overline{Y}) = X(\overline{I_n}, \overline{X^{-1}Y})$.

Donc en considérant la décomposition de Bruhat de $X^{-1}Y$ on a $X^{-1}Y = T_1 P_\sigma T_2$ et comme $T_1, T_2 \in \mathcal{T}_S$ on a :

$$(\overline{I_n}, \overline{X^{-1}Y}) = T_1(\overline{T_1^{-1}}, \overline{P_\sigma T_2}) = T_1(\overline{I_n}, \overline{P_\sigma})$$

D'où $(\overline{X}, \overline{Y}) = X T_1(\overline{I_n}, \overline{P_\sigma})$. Toute orbite contient donc un élément de la forme $(\overline{I_n}, \overline{P_\sigma})$ avec σ défini de manière unique car s'il existe $A \in \text{GL}_n(\mathbb{K})$ tel que $(\overline{I_n}, \overline{P_\sigma}) = A(\overline{I_n}, \overline{P_\tau}) = (\overline{A}, \overline{AP_\tau})$ donc $A \in \mathcal{T}_S$ et il existe $T \in \mathcal{T}_S$ tel que $AP_\tau = P_\sigma T$ d'où $\sigma = \tau$ par unicité de la décomposition de Bruhat.

Il y a donc autant d'orbite que d'éléments de S_n donc il y a $n!$ orbites.

Dénombrement des polynômes irréductibles sur \mathbb{F}_q

Geoffrey Deperle

Leçons associées :

- 123 : Corps finis. Applications.
- 125 : Extension de corps. Exemples et applications.
- 141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.
- 144 : Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.
- 190 : Méthodes combinatoires, problèmes de dénombrement.

Le but de ce développement est de montrer le théorème suivant :

Théorème. On note $\mathcal{P}_q(d)$ l'ensemble des polynômes irréductibles de degré d sur \mathbb{F}_q ($q = p^\alpha$ est une puissance d'un nombre premier). Si $I(q, d)$ désigne le cardinal de $\mathcal{P}_q(d)$, on a pour $n \in \mathbb{N}^*$,

$$I(q, d) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$$

Preuve :

Lemme 3. Pour $n \in \mathbb{N}^*$, $X^{q^n} - X = \prod_{d|n} \prod_{P \in \mathcal{P}_q(d)} P(X)$.

Preuve : Soit $P \in \mathcal{P}_q(d)$, l'anneau $K = \mathbb{F}_q[X]/(P)$ est un corps (car $\mathbb{F}_q[X]$ est principal) de cardinal q^d donc isomorphe à \mathbb{F}_{q^d} , ainsi $\forall x \in K, x^{q^d} = x$.

Or, si $n = dk$, on a $x^{q^n} = x^{q^{dk}} = (x^{q^d})^{q^d \times \dots \times q^d}$ donc par récurrence $x^{q^n} = x$ donc $\overline{X^{q^n} - X} = 0$ et P divise $X^{q^n} - X$ dans $\mathbb{F}_q[X]$. Comme les éléments de $\mathcal{P}_q(d)$ sont irréductibles, le produit $\prod_{d|n} \prod_{P \in \mathcal{P}_q(d)} P(X)$

divise $X^{q^n} - X$.

Réciproquement, soit P un facteur irréductible de degré d de $X^{q^n} - X$ dans $\mathbb{F}_q[X]$,

Comme \mathbb{F}_{q^n} est un corps de décomposition de $X^{q^n} - X$, P est scindé sur \mathbb{F}_{q^n} ,

Si x est une racine de P , on a $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, par multiplicativité des degrés, $[\mathbb{F}_{q^n} : \mathbb{F}_q(x)][\mathbb{F}_q(x) : \mathbb{F}_q] = n$. Or, comme P est irréductible, $\mathbb{F}_q(x)$ est un corps de rupture de P de degré d sur \mathbb{F}_q donc $d|n$.

Montrons que $X^{q^n} - X$ n'admet pas de facteur double (ou plus), s'il existe un tel facteur, alors $X^{q^n} - X$ admet une racine double dans un corps de décomposition.

Or, $(X^{q^n} - X)' = q^n X^{q^n-1} - 1 = -1$ car K (car caractéristique p) donc $X^{q^n} - X$ n'a pas de racine double dans un corps de décomposition. \square

Lemme 4 (Inversion de Möbius). Soit $g : \mathbb{N}^* \rightarrow \mathbb{C}$, soit $G(n) = \sum_{d|n} g(d)$, on a

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

où μ est la fonction de Möbius

Preuve : Soit $n \geq 2$,

Soit p_1, \dots, p_r les diviseurs de n , (on a $r \geq 2$),

$$\sum_{d|n} \mu(d) = \sum_{I \subset [1,r]} (-1)^{|I|} = \sum_{s=0}^r \binom{r}{s} (-1)^s = (1-1)^r = 0$$

Donc

$$\sum_{d|n} \mu(d) = \begin{cases} 0 & \text{si } n \geq 2 \\ 1 & \text{si } n = 1 \end{cases}$$

Si $n \in \mathbb{N}^*$, $d|n$ et $d'|\frac{n}{d} \iff d'|n$ et $d|\frac{n}{d'}$, donc

$$\begin{aligned} \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} g(d') = \sum_{d|n} \sum_{d'|\frac{n}{d}} \mu(d) g(d') \\ &= \sum_{d'|n} \sum_{d|\frac{n}{d'}} \mu(d) g(d') \\ &= \sum_{d'|n} g(d') \underbrace{\sum_{d|\frac{n}{d'}} \mu(d)}_{=0 \text{ sauf pour } d'=n} = g(n) \end{aligned}$$

□

Passons à la preuve du théorème, on a

$$\deg(X^{q^n} - X) = q^n = \sum_{d|n} \sum_{P \in \mathcal{P}_q(d)} \deg(P) = \sum_{d|n} dI(q, d)$$

D'où par inversion de Möbius,

$$I(q, d) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$$

□

Annexe

Application. On a $I(q, n) \underset{n \rightarrow +\infty}{\sim} \frac{q^n}{n}$

Preuve : En posant $r_n = \sum_{\substack{d|n \\ d < n}} \mu\left(\frac{n}{d}\right) q^d$, on a

$$\begin{aligned} |r_n| &\leq \sum_{\substack{d|n \\ d < n}} q^d \leq \sum_{d=0}^{\lfloor \frac{n}{2} \rfloor} q^d \\ &= \frac{q^{\lfloor \frac{n}{2} \rfloor + 1} - 1}{q - 1} \end{aligned}$$

Donc $r_n = O(q^{\lfloor \frac{n}{2} \rfloor})$, comme $I(q, d) = \frac{q^n + r_n}{n}$ on a le résultat. \square

Application. Pour tout $n \in \mathbb{N}^*$, il existe un polynôme irréductible sur \mathbb{F}_q de degré n .

Preuve : Comme $q^n = \sum_{d|n} dI(q, d)$,

Donc pour tout $d \in \mathbb{N}^*$, $q^d \geq dI(q, d)$ d'où

$$\begin{aligned} nI(q, n) &= q^n - \sum_{\substack{d|n \\ d \neq n}} dI(q, d) \\ &\geq q^n - \sum_{\substack{d|n \\ d \neq n}} q^d \\ &\geq q^n - \sum_{d=1}^{n-1} q^d = q^n - q \frac{q^{n-1} - 1}{q - 1} > 0 \end{aligned}$$

\square

Quelques polynômes irréductibles

- Sur \mathbb{F}_2 , on a
 - $\mathcal{P}_2(1) = \{X, X + 1\} \rightarrow I(2, 1) = 2$
 - $\mathcal{P}_2(2) = \{X^2 + X + 1\} \rightarrow I(2, 2) = 1$
 - $\mathcal{P}_2(3) = \{X^3 + X + 1, X^3 + X^2 + 1\} \rightarrow I(2, 3) = 2$
- Sur \mathbb{F}_3 , on a
 - $\mathcal{P}_3(1) = \{X, X + 1, X + 2\} \rightarrow I(3, 1) = 3$
 - $\mathcal{P}_3(2) = \{X^2 + 1, X^2 + X + 2, X^2 + 2X + 2\} \rightarrow I(3, 2) = 3$

Déterminant circulant et suite de polygônes

Geoffrey Deperle

Leçons associées :

- 102 : Groupe des nombres complexes de module 1. Racines de l'unité. Applications.
- 149 : Valeurs propres, vecteurs propres. Calculs exacts ou approchés d'éléments propres. Applications.
- 152 : Déterminant. Exemples et applications.
- 153 : Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.
- 155 : Endomorphismes diagonalisables en dimension finie.
- 181 : Barycentre dans un espace affine réel de dimension finie, convexité. Applications.

Le but de ce développement est de montrer le théorème suivant :

Théorème. Soit $a_0, \dots, a_{n-1} \in \mathbb{C}^n$ et $\omega = e^{i\frac{2i\pi}{n}}$, alors

$$\begin{vmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & a_0 & \ddots & a_{n-2} \\ \vdots & & \ddots & \vdots \\ a_1 & a_2 & \dots & a_0 \end{vmatrix} = \prod_{j=0}^{n-1} \sum_{k=0}^{n-1} a_k \omega^{jk}$$

Preuve : Soit $\mathcal{B} = (e_1, \dots, e_n)$ la base canonique de \mathbb{C}^n , J la matrice de l'unique endomorphisme qui à e_i associe à e_{i-1} si $i \geq 2$ et qui associe e_1 à e_n . On a

$$J = \begin{pmatrix} 0 & 1 & & (0) \\ \vdots & \ddots & \ddots & \\ 0 & & \ddots & 1 \\ 1 & 0 & \dots & 0 \end{pmatrix} \text{ et } \forall k \in \mathbb{N}, J^k = \begin{pmatrix} 0 & \overset{0 \text{ apparait } k \text{ fois}}{\ddots} & 0 & 1 & 0 & \dots & 0 \\ \vdots & & & & \ddots & & \vdots \\ \vdots & & & & & \ddots & 0 \\ 0 & & & & & & 1 \\ 1 & & & (0) & & & \\ & \ddots & & & & & \\ (0) & & & & 1 & & \end{pmatrix}$$

donc en notant A la matrice dont on cherche le déterminant, on a $A = \sum_{k=0}^{n-1} a_k J^k$.

Diagonalisons A en diagonalisant J .

Comme $A = P(J)$ avec $P = \sum_{i=0}^{n-1} a_i X^i$, si $Q \in \mathbb{C}[X]$ tel que $Q \neq 0$ et $\deg Q < n$, $Q(J) \neq 0$ (par

lecture des coefficients sur la matrice).

Donc le polynôme minimal de J vérifie $\deg \pi_J \geq n$. Or, $J^n - I_n = 0$ donc $\pi_J = X^n - 1$.

Or, π_J divise le polynôme caractéristique χ_J de J donc $\chi_J = X^n - 1 = \prod_{k=0}^{n-1} (X - \omega^k)$.

Donc J est diagonalisable et il existe $Q \in \text{GL}_n(\mathbb{C})$ telle que

$$Q^{-1}JQ = \begin{pmatrix} 1 & & & (0) \\ & \omega & & \\ & & \ddots & \\ (0) & & & \omega^{n-1} \end{pmatrix}$$

$$\text{D'où } Q^{-1}JQ = P(Q^{-1}JQ) = \begin{pmatrix} P(1) & & & (0) \\ & P(\omega) & & \\ & & \ddots & \\ (0) & & & P(\omega^{n-1}) \end{pmatrix}.$$

D'où

$$\det(A) = \prod_{i=0}^{n-1} P(\omega^i) = \prod_{i=0}^{n-1} \left(\sum_{k=0}^{n-1} a_k \omega^{jk} \right)$$

□

Application. Soit P un polygone du plan complexe dont les sommets sont $\{z_1, \dots, z_n\}$. On définit par récurrence la suite de polygone $(P_k)_{k \in \mathbb{N}}$ avec $P_0 = P$ et pour tout $k \in \mathbb{N}$, les sommets de P_{k+1} sont les milieux des arêtes de P_k .

La suite (P_k) converge vers l'isobarycentre de $\{z_1, \dots, z_n\}$.

Preuve :

Étape 1 : Montrons la convergence de la suite (P_k)

On représente le polygone P_k par le vecteur $Z_k = \begin{pmatrix} z_1^k \\ \vdots \\ z_n^k \end{pmatrix}$, la relation de récurrence s'écrit alors

$$Z_{k+1} = \begin{pmatrix} \frac{z_1^k + z_2^k}{2} \\ \vdots \\ \frac{z_n^k + z_1^k}{2} \end{pmatrix} = AZ_k \text{ avec } A = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & & \ddots & & \frac{1}{2} \\ \frac{1}{2} & 0 & \dots & 0 & \frac{1}{2} \end{pmatrix} \text{ et } Z_0 = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}.$$

Ainsi, on a $\forall k \in \mathbb{N}, Z_k = A^k Z_0$. Il suffit de montrer que la suite (A^k) converge pour n'importe quelle norme. On a

$$\chi_A(X) = \begin{vmatrix} X - \frac{1}{2} & -\frac{1}{2} & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & & \ddots & & -\frac{1}{2} \\ -\frac{1}{2} & 0 & \dots & 0 & X - \frac{1}{2} \end{vmatrix}$$

Par calcul du déterminant circulant, on a

$$\chi_A(X) = \prod_{j=0}^{n-1} \left(X - \frac{1 + \omega^j}{2} \right)$$

Puisque les $\frac{1+\omega^j}{2}$ sont distincts deux à deux, χ_A est scindé à racines simples donc A est diagonalisable. Il existe $Q \in \text{GL}_n(\mathbb{C})$ tel que $A = QDQ^{-1}$ avec $D = \text{diag}(\lambda_0, \dots, \lambda_{n-1})$ avec pour tout $j \in \llbracket 0, n-1 \rrbracket$, $\lambda_j = \frac{1+\omega^j}{2}$.

Or, $\forall j \in \llbracket 1, n-1 \rrbracket$, $\left| \frac{1+\omega^j}{2} \right| = \left| e^{\frac{ij\pi}{2}} \frac{e^{\frac{ij\pi}{2}} + e^{-\frac{ij\pi}{2}}}{2} \right| = \left| \cos\left(\frac{j\pi}{n}\right) \right| < 1$.

Ainsi, pour tout $j \in \llbracket 0, n-1 \rrbracket$, $\lambda_j^k \xrightarrow{k \rightarrow +\infty} 0$.

Par conséquent, la suite (A^k) converge vers $B := Q \text{diag}(1, 0, \dots, 0) Q^{-1}$.

Posons $Z_\infty = BZ_0$, on a $Z_k \xrightarrow{k \rightarrow +\infty} Z_\infty$ (on a $Z_\infty = AZ_\infty$). Or, l'espace propre associé à 1 contient

le vecteur $\begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$ et est de dimension 1 (car χ_A possède n racines distinctes).

Donc il existe $a \in \mathbb{C}$ tel que $Z_\infty = a \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$ c'est-à-dire (P_k) converge vers a .

Étape 2 : Montrons que la limite est l'isobarycentre de P

Montrons que les P_k ont même isobarycentre.

Soit g_k l'isobarycentre de P_k , on a pour $k \in \mathbb{N}$,

$$g_{k+1} = \frac{1}{n} \sum_{i=1}^n z_i^{k+1} = \frac{1}{n} \left(\sum_{i=1}^{n-1} \frac{z_i^k + z_i^{k+1}}{2} + \frac{z_n^k + z_1^{k+1}}{2} \right) = \frac{1}{n} \sum_{i=1}^n z_i^k = g_k$$

Ainsi, par continuité de la fonction qui à n points du plan associe son isobarycentre, (g_k) converge vers l'isobarycentre du polygone $\{a, \dots, a\}$ qui est a . \square

Forme normale de Smith

Geoffrey Deperle

Leçons associées :

- 122 : Anneaux principaux. Exemples et applications.
- 142 : PGCD et PPCM, algorithmes de calcul. Applications.
- 162 : Systèmes d'équations linéaires, opérations élémentaires, aspects algorithmiques et conséquences théoriques.

Le but de ce développement est de montrer le théorème suivant :

Théorème. Soit A un anneau euclidien, δ un stathme euclidien de A et $m, n \in \mathbb{N}^*$ et $M \in \mathcal{M}_{m,n}(A)$.

$$\exists (P, Q) \in \text{GL}_m(A) \times \text{GL}_n(A) / PMQ = \begin{pmatrix} f_1 & & & & (0) \\ & \ddots & & & \\ & & f_r & & \\ & & & 0 & \\ (0) & & & & \ddots \\ & & & & & 0 \end{pmatrix}$$

avec $f_1, \dots, f_r \in A$ tels que $f_1 | \dots | f_r$ avec unicité modulo les inversibles de A .

Preuve :

Étape 1 : Montrons qu'il existe $f_1 \in A$ et P, Q tel que $PMQ = \begin{pmatrix} f_1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & & \\ 0 & & & v \end{pmatrix}$ tel que pour tout $(i, j) \in \llbracket 1, m-1 \rrbracket \times \llbracket 1, n-1 \rrbracket$, $f_1 | v_{ij}$

Si $M = 0$, alors $f_1 = 0$ convient.

Sinon, considérons X la classe des matrices équivalentes à M et considérons

$$f_1 = \{\text{pgcd}(M_{ij}), (i, j) \in \llbracket 1, m \rrbracket \times \llbracket 1, n \rrbracket, M \in X\}$$

On a alors $\delta(f_1) < \delta(u_{ij})$ pour tout $(i, j) \in \llbracket 1, m \rrbracket \times \llbracket 1, n \rrbracket$, $M \in X$. Considérons la matrice M tel que f_1 est un coefficient de M . Quitte à permuter les colonnes et les lignes, on peut supposer que f_1 se situe en haut à gauche de M :

$$M = \begin{pmatrix} f_1 & u_{12} & \dots & u_{1n} \\ u_{21} & & & \vdots \\ \vdots & & & \vdots \\ u_{n1} & \dots & \dots & u_{nn} \end{pmatrix}$$

On effectue la division euclidienne pour C_1 :
 $\forall i \in \llbracket 2, m \rrbracket, \exists q_i, r_i \in A/u_{i1} = q_i f_1 + r_i$ avec $\delta(r_i) < \delta(f_1)$

$$(L_i \leftarrow L_i - q_i L_1) \begin{pmatrix} f_1 & & & \\ r_2 & (*) & & \\ \vdots & & & \\ r_m & & & \end{pmatrix}$$

Par minimalité de f_1 , on a $r_2 = \dots = r_m = 0$.

De même pour L_1 :
 $\forall j \in \llbracket 2, n \rrbracket, \exists q_j, r_j \in A/u_{1j} = q_j f_1 + r_j$ avec $\delta(r_j) < \delta(f_1)$

$$(C_j \leftarrow C_j - q_j C_1) \begin{pmatrix} f_1 & r_2 & & r_n \\ 0 & (*) & & \\ \vdots & & & \\ 0 & & & \end{pmatrix}$$

Par minimalité de f_1 , on a $r_2 = \dots = r_n = 0$. Donc M est équivalente à $\begin{pmatrix} f_1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & V & \\ 0 & & & \end{pmatrix}$.

Montrons alors que $\forall i, j, f_1 | V_{ij}$.

Pour $i \in \llbracket 2, m \rrbracket$, on effectue $L_1 \leftarrow L_1 + L_i$ $\begin{pmatrix} f_1 & V_{i2} & & V_{in} \\ 0 & (*) & & \\ \vdots & & & \\ 0 & & & \end{pmatrix}$.

On réalise la division euclidienne pour L_1 ,
 $\forall j \in \llbracket 2, n \rrbracket, \exists q_j, r_j \in A/V_{ij} = q_j f_1 + r_j$ avec $\delta(r_j) < \delta(f_1)$ et de même par minimalité de f_1 :
 $r_2 = \dots = r_k = 0$ donc $\forall j \in \llbracket 2, n \rrbracket, V_{ij} = q_j f_1$ d'où $\forall i, j, f_1 | V_{ij}$.

Étape 2 : Montrons le théorème par récurrence sur $m + n \in \mathbb{N} \setminus \{0, 1\}$

- Initialisation : Pour $m + n = 2, M \in \mathcal{M}_{1,1}(A)$ ok
- Hérédité : Soit $n, m \in \mathbb{N}^*$ tels que $m + n \geq 3$. Supposons le résultat vrai pour tout $p, q \in \mathbb{N}^*$

tel que $p + q = m + n - 1$ pour tout $N \in \mathcal{M}_{p,q}(A)$, N est équivalente à $\begin{pmatrix} h_1 & & & \\ & \ddots & & \\ & & h_s & 0 \\ & & & \ddots & 0 \end{pmatrix}$ avec

$h_1 | \dots | h_s$.

Si $m = n = 1$, le résultat est acquis.

Sinon, par ce qui précède, M est équivalente à $\begin{pmatrix} f_1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & f_1 M' & \\ 0 & & & \end{pmatrix}$ et par hypothèse de récurrence

M' est équivalente à $\begin{pmatrix} f'_2 & & & \\ & \ddots & & \\ & & f'_r & 0 \\ & & & \ddots & 0 \end{pmatrix}$ avec $f'_2 | \dots | f'_r$.

Annexe

Lemme 5 (*). Soit $M \in \mathcal{M}_{m,n}(A)$, $P \in \text{GL}_m(A)$, les mineurs de taille k de PM sont combinaisons linéaires des mineurs de taille k de M à coefficients dans A .

Preuve : Soit M_{IJ} la matrice extraite de M en gardant $I = \{i_1, \dots, i_k\}$ lignes de M et $J = \{j_1, \dots, j_k\}$ colonnes de M .

Notons (C_i) les colonnes de M , $M = (C_1 \ \dots \ C_n)$ et $M_{IJ} = (C_{I,j_1} \ \dots \ C_{I,j_s})$.

Si $P = (p_{ij})_{(i,j) \in \llbracket 1, n \rrbracket^2}$, on a $MP = \left(\sum_{i=1}^n p_{i1} C_i \ \dots \ \sum_{i=1}^n p_{in} C_i \right)$. D'où :

$$(MP)_{IJ} = \left(\sum_{i=1}^n p_{i1} C_{I,j_1} \ \dots \ \sum_{i=1}^n p_{in} C_{I,j_k} \right)$$

Par multilinéarité du déterminant, on a $\det((MP)_{I,J})$ est combinaison linéaire des mineurs $M_{I,J}$ où J est un ensemble de k -indice.

□

Formes de Hankel

Geoffrey Deperle

Leçons associées :

- 144 : Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.
- 151 : Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.
- 159 : Formes linéaires et dualité en dimension finie. Exemples et applications.
- 171 : Formes quadratiques réelles. Coniques. Exemples et application.

Le but de ce développement est de montrer le théorème suivant :

Théorème. Soit P un polynôme réel de degré n unitaire, soit x_1, \dots, x_t ses racines distinctes avec x_k de multiplicité $m_k \in \mathbb{N}$. En notant $s_k = m_1 x_1^k + \dots + m_t x_t^k$ les sommes de Newton. La forme quadratique $\sigma : (z_0, \dots, z_{n-1}) \mapsto \sum_{0 \leq i, j \leq n-1} s_{i+j} z_i z_j$ définit une forme quadratique sur \mathbb{R}

de signature $\left(\frac{t+r}{2}, \frac{t-r}{2}\right)$ avec

- r le nombre de racines réelles de P
- t le nombre de racines distinctes de P

Ainsi en notant $\text{sgn}(\sigma_{\mathbb{R}}) = (p, q)$, on a $r = p - q$.

Preuve : $\sigma_{\mathbb{C}}$ est un polynôme homogène de degré 2 sur \mathbb{C} donc définit une forme quadratique sur \mathbb{C} . De plus, les s_k sont des polynômes symétriques en les n -racines (avec multiplicité) de P donc ce sont des combinaisons \mathbb{Z} -linéaires des fonctions symétriques élémentaires en les racines. Or, comme P est unitaire, les fonctions symétriques élémentaires sont au signe près les coefficients de P sont réelles.

Ainsi, $\sigma_{\mathbb{C}}$ définit une forme quadratique $\sigma_{\mathbb{R}}$ sur \mathbb{R}^n . Notons (p, q) sa signature.

Étape 1 : Montrons que le rang de $\sigma_{\mathbb{R}}$ est t , le nombre de racines distinctes de P .

Décomposons $\sigma_{\mathbb{R}}$ selon une base bien choisie.

Soit φ_k la forme linéaire sur \mathbb{C}^n donnée par :

$$\varphi_k(z_0, \dots, z_{n-1}) = z_0 + x_k z_1 + x_k^2 z_2 + \dots + x_k^{n-1} z_{n-1}$$

Montrons que les $(\varphi_k)_{k \in [1, t]}$ sont libres sur \mathbb{C} :

On a $\varphi_k = e_0^* + x_k e_1^* + \dots + x_k^{n-1} e_{n-1}^*$. Donc la matrice des φ_k dans la base duale $(e_0^*, \dots, e_{n-1}^*)$ est

$$\begin{pmatrix} 1 & \dots & \dots & 1 \\ x_0 & & & x_t \\ \vdots & & & \vdots \\ x_0^{n-1} & \dots & \dots & x_t^{n-1} \end{pmatrix}$$

C'est une matrice extraite d'une matrice de Vandermonde inversible car les x_k sont distincts donc elle est de rang t donc les φ_k sont libres.

De plus, le coefficient de $z_i z_j$ dans $\sum_{k=1}^t m_k \varphi_k^2$ vaut
$$\begin{cases} \sum_{k=1}^t 2m_k x_k^i x_k^j = \sum_{k=1}^t 2m_k m_k^{i+j} = 2s_{i+j} & \text{si } i \neq j \\ \sum_{k=1}^t m_k x_k^{2i} = s_{i+j} & \text{si } i = j \end{cases}$$

D'où

$$\sigma = \sum_{k=1}^t m_k \varphi_k^2$$

Ainsi, $\text{rg}_{\mathbb{C}} \sigma = t$ car les φ_k sont indépendants. Or, par invariance du rang par extension de corps, le rang de la matrice (complexe) de σ est le même rang que la matrice (réelle) de $\sigma_{\mathbb{R}}$ donc $\text{rg}_{\mathbb{R}} \sigma = t = p + q$.

Étape 2 : Calculons la signature $\sigma_{\mathbb{R}}$

En décomposant selon les racines réelles et non réelles :

$$\sigma = \sum_{k \in R} m_k \varphi_k^2 + \sum_{k \in I} m_k \varphi_k^2$$

avec $R = \{k \in \llbracket 1, t \rrbracket, x_k \in \mathbb{R}\}$ et $I = \llbracket 1, t \rrbracket \setminus R$.

Or, si x_k est racine de P non réelle, \bar{x}_k est racine de P avec la même multiplicité donc si J est une partie de I tel que $|J| = \frac{|I|}{2}$,

$$\sigma = \sum_{k \in R} m_k \varphi_k^2 + \left(\sum_{k \in J} m_k \varphi_k^2 + \sum_{k \in J} m_k \bar{\varphi}_k^2 \right)$$

Or, $\forall z \in \mathbb{C}, z^2 + \bar{z}^2 = 2\text{Re}(z)^2 - 2\text{Im}(z)^2$,

$$\sigma = \sum_{k \in R} m_k \varphi_k^2 + 2 \sum_{k \in J} m_k (\text{Re}(\varphi_k)^2 + \text{Im}(\varphi_k)^2)$$

Cette décomposition constitue une décomposition de $\sigma_{\mathbb{R}}$ comme combinaison linéaire des carrés de t formes réelles $\varphi_k, k \in R, \text{Re}(\varphi_k), \text{Im}(\varphi_k), k \in J$. Montrons que ces formes linéaires sont indépendantes. Quitte à ré-ordonner, supposons x_1, \dots, x_r les racines réelles de P et x_{r+1}, \dots, x_{r+s} les racines non réelles de P . La matrice de la famille $(\varphi_k, k \in R, \text{Re}(\varphi_k), \text{Im}(\varphi_k), k \in J)$ dans la base duale est

$$\begin{pmatrix} 1 & \dots & 1 & 1 & \dots & 1 & 0 & \dots & 0 \\ x_1 & \dots & x_r & \text{Re}(x_{r+1}) & \dots & \text{Re}(x_{r+s}) & \text{Im}(x_{r+1}) & \dots & \text{Im}(x_{r+s}) \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ x_1^{n-1} & & x_r^{n-1} & \text{Re}(x_{r+1}^{n-1}) & \dots & \text{Re}(x_{r+s}^{n-1}) & \text{Im}(x_{r+1}^{n-1}) & \dots & \text{Im}(x_{r+s}^{n-1}) \end{pmatrix}$$

Donc en effectuant pour tout $j \in \llbracket r+1, r+s \rrbracket, C_j \leftarrow C_j + iC_{j+s}$, on obtient la matrice

$$\begin{pmatrix} 1 & \dots & 1 & 1 & \dots & 1 & 0 & \dots & 0 \\ x_1 & \dots & x_r & x_{r+1} & \dots & x_t & \text{Im}(x_{r+1}) & \dots & \text{Im}(x_{r+s}) \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ x_1^{n-1} & & x_r^{n-1} & x_{r+1}^{n-1} & \dots & x_t^{n-1} & \text{Im}(x_{r+1}^{n-1}) & \dots & \text{Im}(x_{r+s}^{n-1}) \end{pmatrix}$$

La matrice extraite en extrayant les t premières colonnes et les t premières lignes est une matrice extraite d'une matrice de Vandermonde associée à la famille x_1, \dots, x_t distincts donc le rang (complexe) de cette famille est t donc par invariance du rang par extension de corps, la famille $(\varphi_k, k \in R, \text{Re}(\varphi_k), \text{Im}(\varphi_k), k \in J)$ est de rang t donc indépendante.

Comme les m_k sont strictement positifs, $\text{sgn}(\sigma_{\mathbb{R}}) = (|R| + |J|, |J|)$. Comme $|J| = \frac{t-r}{2}$, on obtient le résultat. \square

Annexe

Pour mettre en pratique cette méthode de dénombrement de racines :

- On calcule les sommes de Newton algorithmiquement grâce à la formule les reliant aux fonction symétriques élémentaires donc aux coefficients de P (sans avoir à calculer les racines).
- On dispose de deux méthodes pour calculer la signature : l'algorithme de Gauss et le critère de Sylvester.

Application pour les polynômes de degré 2

Soit $P = aX^2 + bX + c = a(X^2 + \frac{b}{a}X + \frac{c}{a})$ de racines complexes α_1, α_2 .

On a $s_0 = 1 + 1, s_1 = \alpha_1 + \alpha_2 = \frac{-b}{a}, s_2 = \alpha_1^2 + \alpha_2^2 = (\alpha_1 + \alpha_2)^2 - 2\alpha_1\alpha_2 = \frac{b^2 - 2ac}{a^2}$.

Donc la matrice de la forme quadratique est $H = \begin{pmatrix} 2 & \frac{-b}{a} \\ \frac{-b}{a} & \frac{b^2 - 2ac}{a^2} \end{pmatrix}$.

On peut calculer la signature avec le critère de Sylvester. En notant Δ_1 et Δ_2 les deux mineurs principaux de H , on a : $\Delta_1 = 2, \Delta_2 = 2\frac{b^2 - 2ac}{a^2} - \frac{b^2}{a^2} = \frac{b^2 - 4ac}{a^2}$.

$$\text{D'où } \text{sgn}(H) = \begin{cases} (2, 0) & \iff b^2 - 4ac > 0 \\ (1, 1) & \iff b^2 - 4ac < 0. \\ (1, 0) & \iff b^2 - 4ac = 0 \end{cases}$$

Groupe d'isométries du cube et coloriage

Geoffrey Deperle

Leçons associées :

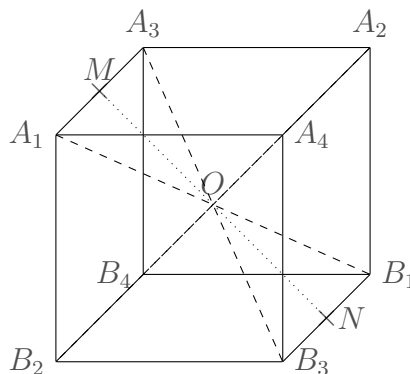
- 101 : Groupe opérant sur un ensemble. Exemples et applications.
- 104 : Groupes finis. Exemples et applications.
- 105 : Groupe des permutations d'un ensemble fini. Applications.
- 161 : Distances dans un espace affine euclidien. Isométries.
- 191 : Exemples d'utilisation de techniques d'algèbre en géométrie.

Le but de ce développement est de montrer le théorème suivant :

Théorème. *Les groupes d'isométrie du cube sont*

$$\text{Isom}^+(C_6) \simeq S_4 \quad \text{Isom}(C_6) \simeq S_4 \times \mathbb{Z}/2\mathbb{Z}$$

Preuve : On considère l'ensemble des 4 grandes diagonales du cube $\mathcal{D} = (D_1, D_2, D_3, D_4)$, elles sont conservées par les isométries (car ce sont les plus grandes distances entre deux points du cube).



On fait agir $\text{Isom}^+(C_6)$ sur \mathcal{D} avec

$$\begin{array}{ccc} \varphi : \text{Isom}^+(C_6) & \rightarrow & S(\mathcal{D}) \simeq S_4 \\ g & \mapsto & g|_{\mathcal{D}} \end{array}$$

Surjectivité :

Soit M le milieu de $[A_1, A_2]$ et N le milieu de $[B_1, B_2]$, la transposition $(D_1 D_2)$ est réalisée par le retournement d'axe (MN) . Donc $(D_1 D_2) \in \text{Im}\varphi$. De même toutes les transpositions appartiennent à $\text{Im}\varphi$. Comme les transpositions engendrent S_4 , φ est surjective.

Injectivité :

Soit $g \in \text{Isom}^+(C_6)$ tel que $\varphi(g) = \text{id}_{\mathcal{D}}$. On a l'alternative suivante :

$$\forall i \in \llbracket 1, 4 \rrbracket, \begin{cases} g(A_i) = A_i \\ g(B_i) = B_i \\ (*) \end{cases} \text{ ou } \begin{cases} g(A_i) = B_i \\ g(B_i) = A_i \\ (**) \end{cases}$$

Supposons qu'il existe $i \in \llbracket 1, 4 \rrbracket$ tel que (**).

Sans perte de généralité, supposons $g(A_1) = B_1$.

Comme g conserve les distances et $\begin{cases} g(A_2) \in \{A_2, B_2\} \\ g(A_1)g(A_2) = A_1A_2 \end{cases}$ on a nécessairement $g(A_2) = B_2$ donc de

même on a (**) pour tout $i \in \llbracket 1, 4 \rrbracket$ donc g coïncide avec s_O sur un repère affine donc $\varphi = s_O$.

Absurde car $g \in \text{Isom}^+(C_6)$.

D'où $\forall i \in \llbracket 1, 4 \rrbracket, g(A_i) = A_i$ et $g(B_i) = B_i$ donc $g = \text{id}$ car coïncide avec id sur un repère affine.

Ainsi, $\text{Isom}^+(C_6) \simeq S_4$, comme $[\text{Isom}(C_6) : \text{Isom}^+(C_6)] = 2$ on a par théorème d'isomorphisme la suite exacte

$$1 \rightarrow \text{Isom}^+(C_6) \rightarrow \text{Isom}(C_6) \rightarrow \{\text{id}, s_O\} \rightarrow 1$$

D'où $\text{Isom}(C_6) \simeq S_4 \times \mathbb{Z}/2\mathbb{Z}$. Or, s_O est central car commute avec toutes les transpositions donc $\{\text{id}, s_O\} \triangleleft \text{Isom}(C_6)$ donc le produit est direct :

$$\text{Isom}(C_6) \simeq S_4 \times \mathbb{Z}/2\mathbb{Z}$$

□

Application. Il y a 57 manières de colorier un cube avec au plus 3 couleurs.

Preuve : Soit ϕ l'ensemble des faces du cube,

Soit C un ensemble de couleurs (notons n son cardinal),

Un coloriage est une fonction $f \in \mathcal{F}(\phi, C)$,

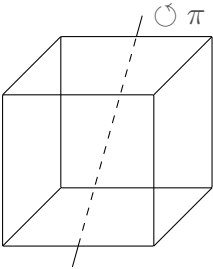
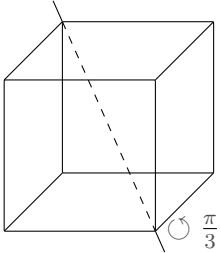
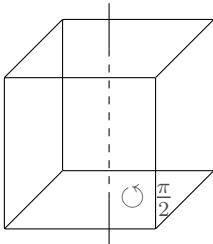
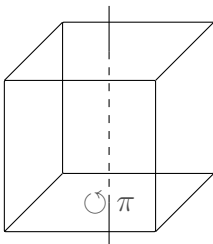
On fait agir le groupe d'isométrie direct G sur $\mathcal{F}(\phi, C)$ par $(g, f) \mapsto (x \mapsto f(g^{-1}x))$ et on s'intéresse aux orbites de cette action.

D'après la formule de Burnside, le nombre d'orbite est :

$$k = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|$$

Or, $f \in \text{Fix}(g) \iff \forall x \in \phi, f(g^{-1}x) = f(x)$ (f est invariant par g).

Dénombrant alors les coloriages invariant sous l'action de g . Il est clair que ce nombre est constant sur la classe de conjugaison de g . Nous allons donc dénombrer $|\text{Fix}(g)|$ pour g dans chaque classe de conjugaison.

<p>Transpositions (6 éléments) : Il s'agit d'une rotation d'angle π d'axe la droite passant par le milieu des arêtes reliant les diagonales.</p>		<p>Il suffit de choisir une couleur pour chaque face latéral, une couleur pour la face de devant et la face de dessous et une couleur pour la face du dessus et la face opposée. Il y a n^4 possibilités.</p>
<p>3-cycle (8 éléments) : Il s'agit d'une rotation autour de la diagonale D_i qui n'intervient pas dans</p>		<p>Il faut et il suffit que les trois faces qui s'intersectent soient de la même couleur. Il y a n^2 possibilités.</p>
<p>4-cycle (6 éléments) : Il s'agit d'une rotation d'angle $\frac{\pi}{2}$ autour de l'axe passant par le centre de deux faces opposées.</p>		<p>Il faut et il suffit choisir une couleur pour la face du haut, une couleur sur la face du bas et une couleur pour les faces latérales. Il y a n^3 possibilités.</p>
<p>Double transpositions (3 éléments) : Il s'agit d'une rotation d'angle π autour de l'axe passant par le centre de deux faces opposées.</p>		<p>Il faut et il suffit choisir une couleur pour la face du haut, la face du bas et une couleur pour la face latéral avant et la face latéral arrière, et une couleur pour les faces latérales des côtes. Il y a n^4 possibilités.</p>

D'où le nombre de coloriage est $k = \frac{1}{24}(n^6 + 6n^4 + 8n^2 + 6n^3 + 3n^4)$. Pour $n = 3$, on obtient $k = 57$. □

Conseil de présentation 1. Lors d'une présentation à l'oral en 15 minutes, on pourra au préalable retenir le nombre d'éléments dans chaque de conjugaison (colonne 1) et expliquer à l'oral uniquement avec des dessins comment obtenir $|\text{Fix}(g)|$ pour g dans chaque classe de conjugaison (colonne 3).

Homéomorphisme $\exp : S_n(\mathbb{R}) \rightarrow S_n^{++}(\mathbb{R})$ et décomposition polaire

Geoffrey Deperle

Leçons associées :

- 156 : Exponentielle de matrices. Applications.
- 158 : Matrices symétriques réelles, matrices hermitiennes.
- 160 : Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie).

Le but de ce développement est de montrer le théorème suivant :

Théorème. *L'application*

$$\begin{array}{ccc} \exp : S_n(\mathbb{R}) & \rightarrow & S_n^{++}(\mathbb{R}) \\ S & \mapsto & e^S \end{array}$$

est un homéomorphisme

Preuve : Soit $S \in S_n(\mathbb{R})$,

Par théorème spectrale, il existe $\lambda_1, \dots, \lambda_n \in \mathbb{R}$ tel que $S = P \text{diag}(\lambda_1, \dots, \lambda_n) P^{-1}$ avec $P \in O_n(\mathbb{R})$.
D'où $\exp(S) = P \text{diag}(e^{\lambda_1}, \dots, e^{\lambda_n}) P^{-1} \in S_n^{++}(\mathbb{R})$ car $\forall i \in \llbracket 1, n \rrbracket, e^{\lambda_i} > 0$.

Étape 1 : Montrons la surjectivité de \exp

Soit $B \in S_n^{++}(\mathbb{R})$, on a $B = P \text{diag}(\mu_1, \dots, \mu_n) P^{-1}$ avec $\mu_i > 0$.

Donc $B = \exp(S)$ avec $S = P \text{diag}(\ln(\mu_1), \dots, \ln(\mu_n)) P^{-1}$ qui est symétrique, d'où la surjectivité.

Étape 2 : Montrons l'injectivité de \exp

Soit $A, A' \in S_n(\mathbb{R})$ tel que $\exp(A) = \exp(A')$.

Soit Q un polynôme interpolateur de Lagrange tel que $\forall i \in \llbracket 1, n \rrbracket, Q(e^{\lambda_i}) = \lambda_i$. On a $Q(\exp(A)) = A$.
 A' commute avec $Q(\exp(A')) = Q(\exp(A)) = A$ donc comme A' et A sont diagonalisables, A et A' sont co-diagonalisables.

En notant $\lambda'_1, \dots, \lambda'_n$ les valeurs propres de A' , il existe $P \in O_n(\mathbb{R})$ tel que

$$\begin{aligned} P \text{diag}(e^{\lambda'_1}, \dots, e^{\lambda'_n}) P^{-1} &= P \text{diag}(e^{\lambda_1}, \dots, e^{\lambda_n}) P^{-1} \\ \iff \text{diag}(e^{\lambda'_1}, \dots, e^{\lambda'_n}) &= \text{diag}(e^{\lambda_1}, \dots, e^{\lambda_n}) \\ \iff \forall i \in \llbracket 1, n \rrbracket, \lambda_i &= \lambda'_i \text{ par injectivité de } \exp_{\mathbb{R}} \end{aligned}$$

donc $A = A'$.

Étape 3 : Montrons la bicontinuité de \exp

L'application \exp est continue, montrons la continuité de la réciproque.

Soit $(B_p)_{p \in \mathbb{N}} = (\exp(A_p))_{p \in \mathbb{N}}$ une suite de $S_n^{++}(\mathbb{R})$ qui converge vers $B = \exp(A) \in S_n^{++}(\mathbb{R})$. Montrons que (A_p) converge vers A .

Comme (B_p) converge, (B_p) est bornée pour $\|\cdot\|_2$.

Donc par continuité de $A \mapsto A^{-1}$, on a $B_p^{-1} \xrightarrow{p \rightarrow +\infty} B^{-1}$ car B est inversible donc est également borné pour $\|\cdot\|_2$.

Or, pour $M \in S_n^{++}(\mathbb{R})$,

$$\begin{aligned} \|\|M\|\|_2 &= \sqrt{\rho({}^t M M)} \\ &= \sqrt{\rho(M^2)} \\ &= \rho(M) \end{aligned}$$

Donc le spectre des B_p est majoré par une constante C et de même le spectre des B_p^{-1} sont majoré par une constante $\frac{1}{C}$. Ainsi, toutes les valeurs propres de B_p sont contenues dans le compact $K = [C', C] \subset]0, +\infty[$.

Donc les valeurs propres des A_p sont incluses dans $[\ln C', \ln C]$. Donc (A_p) est bornés pour $\|\cdot\|_2$.

Or, la suite (A_p) possède une unique valeur d'adhérence,

En effet, soit (A_{p_k}) une sous-suite de (A_p) qui converge vers A' alors $\exp(A_{p_k}) = B_{p_k} \xrightarrow{n \rightarrow +\infty} B$ on a $\exp(A') = B = \exp(A)$ d'où $A = A'$ par injectivité de \exp sur $S_n(\mathbb{R})$.

Ainsi, comme dans un espace vectoriel de dimension finie, une suite bornée qui n'a qu'une seule valeur d'adhérence converge vers cette valeur d'adhérence, la suite (A_p) converge vers A . \square

Corollaire 1. *L'application*

$$\begin{array}{ccc} : S_n^{++}(\mathbb{R}) & \rightarrow & S_n^{++}(\mathbb{R}) \\ S & \mapsto & S^{\frac{1}{2}} \end{array}$$

est un homéomorphisme

Preuve : On a pour $S \in S_n^{++}(\mathbb{R})$,

$$\begin{aligned} (S^{\frac{1}{2}})^2 &= S \\ \exp^{-1}((S^{\frac{1}{2}})^2) &= \exp^{-1}(S) \\ S^{\frac{1}{2}} &= \exp\left(\frac{1}{2} \exp^{-1}(S)\right) \end{aligned}$$

Donc $S \mapsto S^{\frac{1}{2}}$ est un homéomorphisme par composition. \square

Corollaire 2 (Décomposition polaire). *Les applications suivantes :*

$$\begin{array}{ccc} \varphi : O_n(\mathbb{R}) \times S_n^{++}(\mathbb{R}) & \rightarrow & \text{GL}_n(\mathbb{R}) \\ (O, S) & \mapsto & OS \end{array} \quad \text{et} \quad \begin{array}{ccc} \psi : \text{GL}_n(\mathbb{R}) & \rightarrow & O_n(\mathbb{R}) \times S_n^{++}(\mathbb{R}) \\ M & \mapsto & (M({}^t M M)^{-\frac{1}{2}}, ({}^t M M)^{\frac{1}{2}}) \end{array}$$

sont des homéomorphismes inverses l'un de l'autre.

Preuve : φ est bien définie et est continue.

Pour $M \in \text{GL}_n(\mathbb{R})$, on a ${}^t M M \in S_n^{++}(\mathbb{R})$ et

$$M({}^t M M)^{-\frac{1}{2}t} (M({}^t M M)^{-\frac{1}{2}}) = M({}^t M M)^{-\frac{1}{2}} ({}^t M M)^{-\frac{1}{2}t} M = M({}^t M M)^{-1t} M = M M^{-1t} M^{-1t} M = I_n$$

Donc $M({}^tMM)^{-\frac{1}{2}} \in O_n(\mathbb{R})$.

De plus, pour $M \in GL_n(\mathbb{R})$, $M({}^tMM)^{-\frac{1}{2}}({}^tMM)^{\frac{1}{2}} = M$ donc $\varphi(\psi(M)) = M$

Pour $(O, S) \in O_n(\mathbb{R}) \times S_n^{++}(\mathbb{R})$, $(({}^tOS)OS)^{\frac{1}{2}} = (S{}^tOOS)^{\frac{1}{2}} = S$ donc $\psi(\varphi(O, S)) = (O, S)$.

φ et ψ sont donc réciproques l'une de l'autre. □

Lemme de Fitting et cardinal du cône nilpotent

Geoffrey Deperle

Leçons associées :

- 123 : Corps finis. Applications.
- 151 : Dimension d'un espace vectoriel. Rang. Exemples et applications.
- 153 : Polynômes d'endomorphismes en dimension finie. Réduction d'un endomorphisme en dimension finie.
- 154 : Sous-espaces stables par un endomorphisme en dimension finie. Applications.
- 157 : Endomorphismes trigonalisables. Endomorphismes nilpotents.

Le but de ce développement est de montrer le théorème suivant :

Théorème. Soit E un espace vectoriel de dimension n et $u \in \mathcal{L}(E)$, il existe $p \in \mathbb{N}$ tel que

$$E = \text{Ker}u^p \oplus \text{Im}u^p$$

Preuve : Soit P un polynôme annulateur de u et p la multiplicité de 0 comme racine de P . Notons Q le polynôme tel que $Q(0) \neq 0$ et $P(X) = X^p Q(X)$. D'après le lemme des noyaux : $E = \text{Ker}u^p \oplus \text{Im}u^p$.

Montrons que $\text{Ker}Q(u) = \text{Im}u^p$,
Comme $\text{Ker}Q(u)$ est stable par u^p et $\text{Ker}u^p \cap \text{Ker}Q(u) = \{0\}$, l'endomorphisme induit $u^p_{\text{Ker}Q(u)}$ est injectif donc réalise un isomorphisme de $\text{Ker}Q(u)$ dans $\text{Ker}Q(u)$.
D'où $\text{Ker}Q(u) = u^p(\text{Ker}Q(u)) \subset \text{Im}u^p$ et par théorème du rang, $\dim \text{Im}u^p = \dim E - \dim \text{Ker}u^p = \dim \text{Ker}Q(u)$.
D'où $\text{Ker}Q(u) = \text{Im}u^p$. □

Corollaire 3. Toute matrice M de $\mathcal{M}_n(\mathbb{K})$ est semblable à une matrice de la forme $\begin{pmatrix} N & 0 \\ 0 & C \end{pmatrix}$ où N est une matrice nilpotente et C est une matrice carrée inversible.

Preuve : Soit u l'endomorphisme canoniquement associé à $M \in \mathcal{M}_n(\mathbb{K})$, on a

$$\mathbb{K}^n = \text{Ker}u^p \oplus \text{Im}u^p$$

Comme les espaces $\text{Ker}u^p$ et $\text{Im}u^p$ sont stables par u (car pour $x \in \text{Ker}u^p$, $u(x) \in \text{Ker}u^{p+1} \subset \text{Ker}u^p$ et si $y \in \text{Im}u^p$, alors il existe $x \in \mathbb{K}^n$ tel que $y = u^p(x)$ donc $u(y) = u^p(u(x)) \in \text{Im}u^p$).

La matrice de u dans la base obtenue par concaténation d'une base de $\text{Ker}u^p$ et $\text{Im}u^p$ est de la forme

$$\begin{pmatrix} N & 0 \\ 0 & C \end{pmatrix}$$

Avec

- $u_{\text{Ker}u^p}$ est nilpotente d'indice p donc N est nilpotente.
- $u_{\text{Im}u^p}(\text{Im}u^p) = \text{Im}u^p$ donc $u_{\text{Im}u^p}$ est surjective donc bijective donc C est inversible.

□

Application. Soit n_d le cardinal de l'ensemble des matrices nilpotente de taille d sur \mathbb{F}_q alors

$$n_d = q^{d(d-1)}$$

Preuve : D'après le théorème de décomposition de Fitting, à chaque endomorphisme $u \in \mathcal{L}(E)$, on peut associer la donnée $((F, G), v, w)$ avec

- $(F, G) = (\text{Ker}u^{n_0}, \text{Im}u^{n_0})$ est un couple de sous-espaces vectoriels supplémentaires dans E .
- $v = u_{\text{Ker}u^{n_0}}$ est un endomorphisme nilpotent de $\text{Ker}u^{n_0}$
- $w = u_{\text{Im}u^{n_0}}$ un automorphisme de $\text{Im}u^{n_0}$.

Réciproquement, on peut montrer qu'une telle donnée détermine un élément de $\mathcal{L}(E)$.

Notons $m_{k,d}$ le nombre de couples de sous-espaces (F, G) de \mathbb{K}^d tel que $\dim F = k$ et $\dim F \oplus G = \mathbb{K}^d$, notons n_k le nombre de matrices nilpotentes sur \mathbb{F}_q et $g_k = |\text{GL}_k(\mathbb{F}_q)|$. On a

$$|\mathcal{L}(E)| = \sum_{k=0}^d m_{k,d} n_k g_{d-k}$$

$\underbrace{\hspace{1.5cm}}_{=q^{d^2}}$

Or, comme $\text{GL}_n(\mathbb{K})$ agit transitivement sur les (F, G) tel que $F \oplus G = \mathbb{F}_q^n$ avec

$$\text{Stab}((F, G)) \simeq \text{GL}_k(\mathbb{F}_q) \times \text{GL}_{n-k}(\mathbb{F}_q)$$

Par transitivité, $m_{k,d} = \frac{|\text{GL}_d(\mathbb{F}_q)|}{|\text{GL}_k(\mathbb{F}_q) \times \text{GL}_{d-k}(\mathbb{F}_q)|} = \frac{g_d}{g_k g_{d-k}}$.

D'où $q^{d^2} = \sum_{k=0}^d \frac{g_d}{g_k g_{d-k}} n_k g_{d-k}$ d'où $\frac{q^{d^2}}{g_d} = \sum_{k=0}^d \frac{n_k}{g_k}$.

Donc en soustrayant l'égalité entre d et $d-1$, $\frac{q^{d^2}}{g_d} - \frac{q^{(d-1)^2}}{g_{d-1}} = \frac{n_d}{g_d}$ d'où $n_d = q^{d^2} - \frac{g_d}{g_{d-1}} q^{(d-1)^2}$.

Or, comme $g_d = q^{\frac{d(d-1)}{2}} \prod_{i=1}^d (q^i - 1)$, on a $\frac{g_d}{g_{d-1}} = q^{d-1} (q^d - 1)$ d'où

$$\begin{aligned} n_d &= q^{d^2} - q^{d-1} (q^d - 1) q^{(d-1)^2} \\ &= q^{d^2} - q^{d^2 - 2d + 1 + d - 1} (q^d - 1) \\ &= q^{d^2} - q^{d(d-1)} (q^d - 1) \\ &= q^{d(d-1)} \end{aligned}$$

□

Morphismes continus de (S^1, \times) dans $(GL_n(\mathbb{R}), \times)$

Geoffrey Deperle

Leçons associées :

- 102 : Groupe des nombres complexes de module 1. Racine de l'unité. Applications.
- 149 : Valeurs propres, vecteurs propres. Calculs exacts ou approchés d'éléments propres. Applications.
- 155 : Endomorphismes diagonalisables en dimension finie.
- 156 : Exponentielle de matrices. Applications.
- 157 : Endomorphismes trigonalisables. Endomorphismes nilpotents.

Le but de ce développement est de montrer le théorème suivant :

Théorème. *Les morphismes continus φ de (S^1, \times) vers $(GL_n(\mathbb{R}), \times)$ sont de la forme*

$$\varphi : e^{it} \mapsto Q \begin{pmatrix} R_{tk_1} & & & & \\ & \ddots & & & \\ & & R_{tk_r} & & \\ & & & 1 & \\ & & & & \ddots \\ & & & & & 1 \end{pmatrix} Q^{-1}$$

avec $Q \in GL_n(\mathbb{R})$, $r \in \mathbb{N}$, $k_1, \dots, k_r \in \mathbb{Z}^*$ et $\forall \theta \in \mathbb{R}$, $R_\theta = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$.

Preuve :

Analyse :

Soit $\varphi : S^1 \rightarrow GL_n(\mathbb{R})$ un morphisme de groupe continu.

Étape 1 : Montrons qu'il existe $A \in GL_n(\mathbb{R})$ tel que $\forall t \in \mathbb{R}$, $\varphi(e^{it}) = e^{tA}$ (relèvement)

Soit $\psi : t \mapsto \varphi(e^{it})$, ψ est un morphisme de groupe continu de $(\mathbb{R}, +)$ dans $(GL_n(\mathbb{R}), \times)$.

Montrons que ψ est dérivable.

Soit $F : x \mapsto \int_0^x \psi(t) dt$, $F \in C^1(\mathbb{R})$ car ψ est continue et $F'(0) = I_n$ d'où $\frac{1}{t}F(t) \xrightarrow{t \rightarrow 0} I_n$.

Comme $GL_n(\mathbb{R})$ est ouvert, $\frac{1}{t}F(t)$ est inversible pour t assez petit. Soit $a > 0$ tel que $\frac{1}{a}F(a) \in GL_n(\mathbb{R})$ on a $F(a) \in GL_n(\mathbb{R})$. En intégrant la relation $\psi(x+t) \stackrel{(*)}{=} \psi(x)\psi(t)$ on a

$$\int_0^a \psi(x+t) dt = \psi(x) \int_0^a \psi(t) dt \text{ d'où } \psi(x) = F(a)^{-1} \int_x^{x+a} \psi(t) dt$$

Nombres premiers de forme $p = x^2 + 3y^2$

Geoffrey Deperle

Leçons associées :

- 121 : Nombres premiers. Applications.
- 122 : Anneaux principaux. Exemples et applications.
- 126 : Exemples d'équations en arithmétique.

Le but de ce développement est de montrer le théorème suivant :

Théorème. *Un nombre premier p se décompose sous la forme $p = x^2 + 3y^2$ avec $x, y \in \mathbb{Z}$ si et seulement si $p = 3$ ou $p \equiv 1[3]$*

Preuve :

(\Leftarrow) Si $p = x^2 + 3y^2$ alors p est un carré modulo 3.

Or les carrés modulo 3 sont 0 et 1 donc $p \equiv 1[3]$ ou $3|p$ d'où $p = 3$ car p premier.

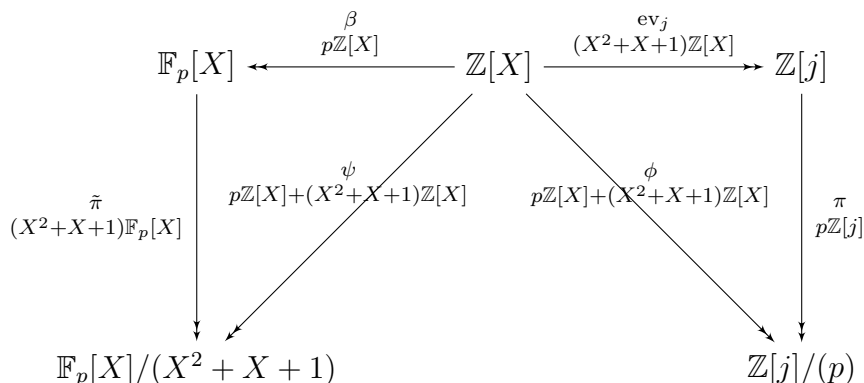
(\Rightarrow) Si $p = 3$, alors le couple $(0, 1)$ convient.

Supposons maintenant $p \equiv 1[3]$,

Étape 1 : Montrons que $X^3 - 1$ est scindé dans $\mathbb{F}_p \iff p = 3$ ou $p \equiv 1[3]$

Comme 0 n'est pas racine de $X^3 - 1$, on se ramène à l'équation dans \mathbb{F}_p^* cyclique et donc isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$. Cela revient à résoudre l'équation $3x = 0$ dans $\mathbb{Z}/(p-1)\mathbb{Z}$. Or, comme $p \equiv 1[3]$, les entiers $0, \frac{p-1}{3}, \frac{2(p-1)}{3}$ sont trois solutions distinctes et il n'y a pas d'autre (question de degré).

Étape 2 : Montrons que l'on a $\mathbb{Z}[j]/(p) \simeq \mathbb{F}_p[X]/(X^2 + X + 1)$ avec $j = \frac{-1+i\sqrt{3}}{2}$



On construit les différents morphismes du diagramme (dont on note les noyaux respectifs en dessous)

Tous les morphismes sont surjectifs de noyau :

— $\text{Ker}(\text{ev}_j) = (X^2 + X + 1)$

— $\text{Ker}(\pi) = p\mathbb{Z}[j]$

Calculons $\text{Ker}(\phi)$,

Soit $P \in \mathbb{Z}[X]$, on effectue la division euclidienne de P par le polynôme unitaire $X^2 + X + 1$: il existe $A, B \in \mathbb{Z}[X]$ tel que $P = (X^2 + X + 1)A(X) + B(X)$.

$$\begin{aligned} P \in \text{Ker}(\phi) &\iff \pi(\text{ev}_j(P)) = 0 \\ &\iff \pi(B(j)) = 0 \\ &\iff p|B(j) \\ &\iff B \in p\mathbb{Z}[X] \end{aligned}$$

donc $\text{Ker}(\phi) = p\mathbb{Z}[X] + (X^2 + X + 1)\mathbb{Z}[X]$.

De même,

— $\text{Ker}(\beta) = p\mathbb{Z}[X]$

— $\text{Ker}(\tilde{\pi}) = (X^2 + X + 1)\mathbb{F}_p[X]$

et de même $\text{Ker}(\psi) = p\mathbb{Z}[X] + (X^2 + X + 1)\mathbb{Z}[X]$.

Comme ψ et ϕ sont surjectifs,

$$\mathbb{F}_p[X]/(X^2 + X + 1) \simeq \mathbb{Z}[X]/\text{Ker}(\psi) = \mathbb{Z}[X]/\text{Ker}(\phi) \simeq \mathbb{Z}[j]/(p)$$

Étape 3 : Montrons qu'il existe un élément $\alpha \in \mathbb{Z}[j]$ de norme p

Ainsi, comme $p \equiv 1[3]$, $X^3 - 1$ possède 3 racines sur \mathbb{F}_p et donc $X^2 + X + 1$ possède deux racines sur \mathbb{F}_p d'où $X^2 + X + 1$ n'est pas irréductible sur \mathbb{F}_p et l'anneau $\mathbb{F}_p[X]/(X^2 + X + 1)$ n'est pas intègre donc l'anneau $\mathbb{Z}[j]/(p)$ n'est pas intègre et p n'est pas premier dans $\mathbb{Z}[j]$.

Comme $\mathbb{Z}[j]$ est factoriel, p est irréductible :

Il existe α, β non inversible (donc de norme > 1) dans $\mathbb{Z}[j]$ tels que $p = \alpha\beta$.

Ainsi, $p^2 = N(\alpha)N(\beta)$ et comme $N(\alpha) \in \mathbb{N}$, $N(\alpha) = p$.

Étape 4 : Montrons qu'en multipliant par un inversible, il existe un élément $\alpha \in \mathbb{Z}[\frac{-1+i\sqrt{3}}{2}]$ de norme p

Montrons qu'il existe un représentant de α modulo les inversibles de $\mathbb{Z}[j]$ se trouvant dans $\mathbb{Z}[i\sqrt{3}]$. $\alpha \in \mathbb{Z}[j]$ donc $\exists a, b \in \mathbb{Z}/\alpha = a + bj$. Comme $j = \frac{-1+i\sqrt{3}}{2}$, on a $\alpha \in \mathbb{Z}[i\sqrt{3}]$ si et seulement si b est pair.

Or, si b est impair :

— Si a est impair, on a $j(a + bj) = aj - b(1 + j) = -b + (a - b)j \in \mathbb{Z}[i\sqrt{3}]$

— Si a est pair, $j^2(a + bj) = b - a(1 + j) = b - a - aj \in \mathbb{Z}[i\sqrt{3}]$

Ainsi, quitte à multiplier par un inversible (de norme 1), on a $\alpha \in \mathbb{Z}[i\sqrt{3}]$.

Donc avec ce $\alpha = x + iy\sqrt{3}$ et $p = N(\alpha) = x^2 + 3y^2$ donnant une décomposition de p sous la forme voulue. □

Réduction de Jordan par la dualité

Geoffrey Deperle

Leçons associées :

- 151 : Dimension d'un espace vectoriel. Rang. Exemples et 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.
- 159 : Formes linéaires et dualité en dimension finie. Exemples et applications.

Le but de ce développement est de montrer le théorème suivant :

Théorème. Soit $u \in \mathcal{L}(E)$ de polynôme caractéristique scindé $\chi_u = \prod_{k=1}^p (X - \lambda_k)^{\alpha_k}$, avec $\alpha_k \geq 1, \lambda_k \in \mathbb{K}$ deux à deux distincts. Il existe une base \mathcal{B} de E dans laquelle la matrice de u est de la forme $\begin{pmatrix} J_1 & & \\ & \ddots & \\ & & J_p \end{pmatrix}$ où

$$\forall k \in \llbracket 1, p \rrbracket, J_k = \begin{pmatrix} \lambda_k & & & (0) \\ \varepsilon_{k,2} & \ddots & & \\ & \ddots & \ddots & \\ (0) & & \varepsilon_{k,\alpha_k} & \lambda_k \end{pmatrix} \in \mathcal{M}_{\alpha_k}(\mathbb{K}) \text{ et } \varepsilon_{k,i} \in \{0, 1\}$$

Lemme 6. Soit $u \in \mathcal{L}(E)$ nilpotent d'indice $q \geq 1$, il existe $\varphi \in E^*, x \in E$ tel que les espaces

- $F = \text{Vect}(x, \dots, u^{q-1}(x))$
- $G = H^\perp$ avec $H = \text{Vect}(\varphi, {}^t u(\varphi), \dots, ({}^t u)^{q-1}(\varphi))$

sont stables par u et $E = F \oplus G$.

Preuve du lemme : Comme $({}^t u)^k = {}^t(u^k)$ pour tout $k \in \mathbb{N}$, l'endomorphisme ${}^t u : E^* \rightarrow E^*$ est nilpotent d'indice q , donc il existe $\varphi \in E^*$ tel que la famille $(\varphi, {}^t u(\varphi), \dots, ({}^t u)^{q-1}(\varphi))$ est libre. Comme $\varphi \circ u^{q-1} \neq 0$, il existe $x \in E$ tel que $\varphi(u^{q-1}(x)) \neq 0$ et $u^{q-1}(x) \neq 0$ donc $(x, u(x), \dots, u^{q-1}(x))$ est libre.

Notons H et F les espaces engendrés et notons $G = H^\perp$.

F est clairement stable par u .

Montrons que G est stable par u :

Soit $y \in G$, montrons que $u(y) \in H^\perp$, or pour $k \in \llbracket 0, q-1 \rrbracket$, $({}^t u)^k(\varphi)(u(y)) = ({}^t u)^{k+1}(\varphi)(y) = 0$ car $y \in G$.

Montrons que $E = F \oplus G$

On a déjà $\dim G + \dim F = n - q + q = n = \dim E$.

Montrons à présent que $F \cap G = \{0\}$,

Soit $y = \sum_{k=0}^{q-1} \lambda_k u^k(x) \in F \cap G$, $u^{q-1}(y) \in G$ car G est stable par u .

D'où $0 = \varphi(u^{q-1}(y)) = \lambda_0 \underbrace{\varphi(u^{q-1}(x))}_{\neq 0}$ donc $\lambda_0 = 0$.

De même, en supposant $\lambda_0 = \dots = \lambda_j = 0$ pour $0 \leq j \leq q-2$, on a $y = \sum_{k=j+1}^{q-1} \lambda_k u^k(x)$ et

$0 = \varphi(u^{q-j-2}(y)) = \lambda_{j+1} \underbrace{\varphi(u^{q-1}(x))}_{\neq 0}$ donc $\lambda_{j+1} = 0$. D'où $E = F \oplus G$. \square

Lemme 7. Soit $u \in \mathcal{L}(E)$ nilpotent d'indice $q \geq 1$, il existe une base $E = \mathcal{B}_1 \cup \dots \cup \mathcal{B}_r$ telle que chaque espace $E_i = \text{Vect}(\mathcal{B}_i)$ sont stables par u et la matrice l'endomorphisme induit par u sur E_i est

$$J_i = \begin{pmatrix} 0 & & & (0) \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ (0) & & 1 & (0) \end{pmatrix} \in \mathcal{M}_{q_i}(\mathbb{K})$$

avec $q_i = \dim(E_i)$

Preuve du lemme : On procède par récurrence sur $n = \dim E$,

— Pour $n = 1$, on a $u = 0$ et le résultat est acquis.

— Soit $n \in \mathbb{N}^*$, supposons le résultat acquis pour les espaces vectoriels de dimension strictement inférieur à n , considérons F et G telle le lemme 1, on a en notant $\mathcal{B}_1 = (x, u(x), \dots, u^{q-1}(x))$,

$$\text{Mat}_{\mathcal{B}_1}(u_F) = \begin{pmatrix} 0 & & & (0) \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ (0) & & 1 & (0) \end{pmatrix} \in \mathcal{M}_q(\mathbb{K})$$

Si $q = n$, le résultat est acquis. Sinon, on complète cette base par une base \mathcal{B}_G une base de G , la matrice de u dans la base $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_G$ est $A = \begin{pmatrix} J_q & 0 \\ 0 & A_{n-q} \end{pmatrix}$ car G est stable par u .

Comme $A_{n-q} \in \mathcal{M}_{n-q}(\mathbb{K})$ est nilpotente d'indice de nilpotence $\leq q$, on applique l'hypothèse de récurrence pour obtenir une base idoine. \square

Passons à présent au cas trigonalisable,

Preuve du théorème : Pour $k \in \{1, 2, \dots, p\}$, notons $N_k = \text{Ker}(u - \lambda_k \text{id})^{\alpha_k}$, on a par théorème de Cayley-Hamilton, $E = \bigoplus_{k=1}^p N_k$.

Chaque N_k est un espace stable de dimension α_k et u_{N_k} a pour unique valeur propre λ_k et $u_{N_k} - \lambda_k \text{id}$ est nilpotente d'indice $\beta_k \leq \alpha_k$.

Donc d'après le lemme 2, il existe une base \mathcal{B}_k de N_k dans laquelle $\text{Mat}(u_{N_k} - \lambda_k \text{id})$ est de la forme

$$\begin{pmatrix} 0 & & & (0) \\ \varepsilon_{k,1} & \ddots & & \\ & \ddots & \ddots & \\ (0) & & \varepsilon_{k,\alpha_k} & 0 \end{pmatrix}$$

Dans la réunion de ces bases, la matrice de u est de la forme indiquée. □

SO₃(ℝ) et les quaternions

Geoffrey Deperle

Leçons associées :

- 103 : Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients.
- 108 : Exemples de parties génératrices d'un groupe. Applications.
- 160 : Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie).
- 161 : Distances dans un espace affine euclidien. Isométries.
- 191 : Exemples d'utilisation de techniques d'algèbre en géométrie.

Le but de ce développement est de montrer le théorème suivant :

Théorème. Soit $H = \{a + ib + jc + kd, (a, b, c, d) \in \mathbb{R}^4\}$ l'algèbre des quaternions sur \mathbb{R} . On identifie H avec \mathbb{R}^4 muni de la topologie euclidienne.

En notant G le sous-groupe de H^* formé des quaternions de norme 1. On a la suite exacte :

$$1 \rightarrow \{\pm 1\} \rightarrow G \rightarrow \text{SO}_3(\mathbb{R}) \rightarrow 1$$

Preuve :

Étape 1 : Construisons un morphisme $\tilde{S} : G \rightarrow \text{O}_3(\mathbb{R})$

Considérons la conjugaison pour $q \in G$:

$$\begin{aligned} S_q &: H \rightarrow H \\ x &\mapsto qxq^{-1} = qx\bar{q} \end{aligned}$$

S_q est une bijection d'inverse $S_{q^{-1}}$. Considérons alors la représentation :

$$\begin{aligned} S &: G \rightarrow \text{GL}(\mathbb{R}^4) \simeq \text{GL}_4(\mathbb{R}) \\ q &\mapsto S_q \end{aligned}$$

Cette application est bien définie car S est un morphisme de groupe et pour tout $q \in G$, S_q est linéaire.

De plus, en notant $\|\cdot\|$ la norme euclidienne de \mathbb{R}^4 , pour tout $q \in G$,

$$\begin{aligned} \|S_q(x)\| &= \|qxq^{-1}\| \\ &= \|q\|\|x\|\|q^{-1}\| \\ &= \|x\| \text{ car } q \in G \end{aligned}$$

donc on a $S : G \rightarrow O(H)$.

Soit $N = \{bi + cj + dk, (b, c, d) \in \mathbb{R}^3\}$ l'espace des quaternions purs, on a $N = (\mathbb{R}.1)^\perp$ l'orthogonal de $\mathbb{R}.1$ dans H .

De plus, pour tout $q \in G, x \in \mathbb{R}, S_q(x) = x$ car \mathbb{R} est central donc $\mathbb{R}.1$ est stable par S_q .

Comme $S_q \in O(H)$, N est stable par S_q .

Notons $\tilde{S}_q = S_{q|_N}$, on a $\tilde{S}_q \in O(N) \simeq O_3(\mathbb{R})$ et notons

$$\begin{aligned} \tilde{S} : G &\rightarrow O_3(\mathbb{R}) \\ q &\mapsto \tilde{S}_{q|_N} \end{aligned}$$

le morphisme associé.

Étape 2 : Calculons $\text{Ker} \tilde{S}$

Soit $q \in G$,

$$\begin{aligned} q \in \text{Ker} \tilde{S} &\iff q \in G \cap Z(N) \\ &\iff q \in G \cap \mathbb{R} \\ &\iff q \in \{\pm 1\} \end{aligned}$$

Étape 3 : Montrons que $\text{Im} \tilde{S} \subset \text{SO}_3(\mathbb{R})$

Les coefficients de \tilde{S}_q sont polynomiales en les coordonnées de q donc \tilde{S} est continue.

Comme $\det : O_3(\mathbb{R}) \rightarrow \{\pm 1\}$ est continue, alors $\det \circ \tilde{S}$ est continue.

De plus, $G \simeq \mathbb{S}^3$ est connexe, on a donc $(\det \circ \tilde{S})(G) \subset \{1\}$ ou $(\det \circ \tilde{S})(G) \subset \{-1\}$.

Or, $\det(\tilde{S}_1) = \det(\text{id}) = 1$ donc on a $\tilde{S}(G) \subset \text{SO}_3(\mathbb{R})$.

Étape 4 : Montrons que $\text{SO}_3(\mathbb{R}) \subset \text{Im} \tilde{S}$

Comme $\text{SO}_3(\mathbb{R})$ est engendré par les retournements, il suffit de montrer que ceux-ci sont atteints.

Soit $p \in N \cap G, \tilde{S}_p(p) = pp\bar{p} = p$ donc \tilde{S}_p fixe p .

De plus, comme $p \in G, \bar{p} = -p$ donc $\tilde{S}_p^2 = \tilde{S}_{p^2} = \tilde{S}_{-1} = \text{id}$ donc \tilde{S}_p est une involution : c'est un retournement d'axe $\text{Vect}(p)$.

Comme ceci est vrai pour tout $p \in G \cap N \simeq \mathbb{S}^2$, tous les renversements de $\text{SO}_3(\mathbb{R})$ sont atteints.

Conclusion

Par théorème d'isomorphisme, on dispose de la factorisation suivante

$$\begin{array}{ccc} G & \xrightarrow{\tilde{S}} & \text{SO}_3(\mathbb{R}) \\ \pi \downarrow & \nearrow \simeq & \\ G/\{\pm 1\} & & \end{array}$$

d'où $\text{SO}_3(\mathbb{R}) \simeq G/\{\pm 1\}$

□

Application.

$$\mathrm{SU}_2(\mathbb{C})/\{\pm I_2\} \simeq \mathrm{SO}_3(\mathbb{R})$$

Preuve : Comme $\mathbb{C} \subset H$, une base de H comme \mathbb{C} -espace vectoriel est donnée par $(1, j)$: un quaternion $q = a + ib + jc + dk$ peut être écrit comme $q = (a + ib) + j(x - ik)$.

On considère l'action de G sur H par multiplication à gauche :

$$q.x := T_q(x) = qx$$

donc le morphisme de groupe $G \rightarrow \mathrm{GL}_2(\mathbb{C})$ à valeurs dans $\mathrm{U}_2(\mathbb{C})$ car q est de norme 1.

Si $q = \lambda + j\mu \in H$, on a $T_q = \begin{pmatrix} \lambda & -\bar{\mu} \\ \mu & \bar{\lambda} \end{pmatrix} \in \mathrm{U}_2(\mathbb{C})$. Or, $1 = \|q\|^2 = |\lambda|^2 + |\mu|^2 = \det(T_q)$ donc $T_q \in \mathrm{SU}_2(\mathbb{C})$.

Donc $G \simeq \mathrm{SU}_2(\mathbb{C})$ (l'application est alors injective et surjective)

□

Théorème chinois : Cas général

Geoffrey Deperle

Leçons associées :

- 120 : Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.
- 142 : PGCD et PPCM, algorithmes de calcul. Applications.

Le but de ce développement est de montrer le théorème suivant :

Théorème. Soit $m, n \in \mathbb{N}$, on dispose de la décomposition

$$\mathbb{Z}/\text{ppcm}(m, n)\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \xrightarrow{\psi} \mathbb{Z}/\text{pgcd}(m, n)\mathbb{Z}$$

avec φ un morphisme injectif et ψ un morphisme surjectif tel que $\text{Im}\phi = \text{Ker}\psi$.

Preuve : Notons pour la suite $\delta = \text{pgcd}(m, n)$ et $\mu = \text{ppcm}(m, n)$.

Étape 1 : Construction de ϕ

Posons $\tilde{\varphi} : \mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, $\tilde{\varphi}$ est un morphisme de groupe de noyau :

$$x \mapsto (\bar{x}_m, \bar{x}_n)$$

$$\text{Ker}\tilde{\varphi} = \{x \in \mathbb{Z} \mid \bar{x}_m = 0 \text{ et } \bar{x}_n = 0\} = \{x \in \mathbb{Z} \mid m|x \text{ et } n|x\}$$

Donc $\text{Ker}\tilde{\varphi} = \text{ppcm}(m, n)\mathbb{Z}$.

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\tilde{\varphi}} & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \pi \downarrow & \nearrow \varphi & \\ \mathbb{Z}/\text{ppcm}(m, n)\mathbb{Z} & & \end{array}$$

En passant au quotient, il existe $\varphi : \mathbb{Z}/\mu\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ tel que

$$\left\{ \begin{array}{l} \varphi \text{ est un morphisme de } \mathbb{Z}/\mu\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \varphi \text{ est injectif} \\ \text{Im}\varphi = \text{Im}\tilde{\varphi} \end{array} \right.$$

Étape 2 : Construction de ψ

Posons $\psi : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/\delta\mathbb{Z}$
 $(\overline{x_m}, \overline{y_n}) \mapsto \overline{x_\delta} - \overline{y_\delta}$. Montrons qu'il s'agit d'un morphisme :

Comme $\delta|m$, $m\mathbb{Z} \subset \delta\mathbb{Z}$ donc par passage au quotient du morphisme de projection $\mathbb{Z} \rightarrow \mathbb{Z}/\delta\mathbb{Z}$ par $m\mathbb{Z}$, on obtient un morphisme $\tilde{\psi} : \mathbb{Z} \rightarrow \mathbb{Z}/\delta\mathbb{Z}$ est bien définie.
 $\tilde{x}_m \mapsto \tilde{x}_\delta$

Ainsi, $\overline{x_\delta}$ est bien définie. De même $\overline{y_\delta}$ est bien définie. Comme les applications $\overline{x_m} \mapsto \overline{x_\delta}$ et $\overline{y_n} \mapsto \overline{y_\delta}$ définissent des morphismes. ψ est bien définie et définie un morphisme d'anneaux.

Montrons la surjectivité de ψ ,

Soit $\overline{x_\delta} \in \mathbb{Z}/\delta\mathbb{Z}$, on a $\psi(\overline{x_m}, 0) = \overline{x_\delta}$ d'où la surjectivité.

Étape 3 : Montrons que $\text{Ker}\psi = \text{Im}\varphi$

Soit $(\overline{x_m}, \overline{x_n}) \in \text{Im}\varphi$ avec $x \in \mathbb{Z}$, alors $\psi(\overline{x_m}, \overline{x_n}) = \overline{x_\delta} - \overline{x_\delta} = 0$. Donc $\text{Im}\varphi \subset \text{Ker}\psi$.
 De plus,

$$\begin{aligned} |\text{Im}\varphi| &= |\mathbb{Z}/\mu\mathbb{Z}| = \text{ppcm}(m, n) = \frac{mn}{\text{pgcd}(m, n)} \\ &= \frac{|\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}|}{|\mathbb{Z}/\delta\mathbb{Z}|} \\ &= |\text{Ker}\psi| \end{aligned}$$

d'où l'égalité entre les ensembles. □

Application. Soit $x, a, b \in \mathbb{Z}$, $m, n \in \mathbb{N}$, en posant $\delta = \text{pgcd}(m, n)$,

Le système $(S) : \begin{cases} x \equiv a [m] \\ x \equiv b [n] \end{cases}$ admet une solution si et seulement si $\overline{a_\delta} = \overline{b_\delta}$

Preuve :

Soit a, b tel que $\overline{a_\delta} \neq \overline{b_\delta}$ alors si (S) admet une solution x , on a $\tilde{\varphi}(x) = (\overline{x_m}, \overline{x_n}) = (\overline{a_m}, \overline{b_n})$ et $(\overline{a_m}, \overline{b_n}) \in \text{Im}\varphi = \text{Ker}\psi$ d'où $\psi((\overline{a_m}, \overline{b_n})) = \overline{a_\delta} - \overline{b_\delta} = 0$. Absurde.

Supposons à présent que a, b est telle que $\overline{a_\delta} = \overline{b_\delta}$, alors il existe $k \in \mathbb{Z}$ tel que $a = b + k\delta$.

Soit $u, v \in \mathbb{Z}$ tel que $um + vn = \delta$, et posons $x_0 = \frac{1}{\delta}(avn + bum) \in \mathbb{Z}$.

On a $x_0 = \frac{1}{\delta}((b + k\delta)vn + bum) = b\frac{vn+um}{\delta} + kvn$.

D'où $x_0 \equiv b [n]$.

De même $x_0 = \frac{1}{\delta}(avn + (a - k\delta)um) = \frac{vn+um}{\delta} - kum$.

D'où $x_0 \equiv a [m]$ donc x_0 est solution.

Soit x une autre solution de (S) , alors $\tilde{\varphi}(x) = \tilde{\varphi}(x_0)$ d'où $x - x_0 \in \text{Ker}\tilde{\varphi} = \text{ppcm}(m, n)\mathbb{Z}$.
 L'ensemble des solution est $\{x_0 + k\text{ppcm}(m, n), k \in \mathbb{Z}\}$. □

Théorème de Dirichlet faible

Geoffrey Deperle

Leçons associées :

- 102 : Groupes des nombres complexes de module 1. Racines de l'unité. Applications.
- 120 : Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.
- 121 : Nombres premiers. Applications.

Le but de ce développement est de montrer le théorème suivant :

Théorème. *Soit $n \geq 1$, un entier fixé. Il existe une infinité de nombres premiers congrus à 1 modulo n .*

Commençons par présenter un lemme qui permet de reformuler le problème.

Lemme 8. *Soit $n \geq 1$, s'il existe $a \in \mathbb{Z}$, p premier tel que*

- $p \mid \phi_n(a)$
- $\forall d < n, d \mid n, p \nmid \phi_d(a)$

avec ϕ_n le n -ième polynôme cyclotomique, alors $p \equiv 1[n]$.

Preuve du lemme : Soit $a \in \mathbb{Z}$, p premier vérifiant les hypothèses,

Comme $\phi_n \mid X^n - 1$, on a $\phi_n(a) \mid a^n - 1$ d'où $p \mid a^n - 1$ donc l'ordre de \bar{a} divise n dans $(\mathbb{Z}/p\mathbb{Z})^*$.

Montrons que l'ordre de \bar{a} est exactement n .

Soit d un diviseur strict de n , d'après la décomposition

$$X^d - 1 = \prod_{d' \mid d} \phi_{d'}$$

On a $\bar{a}^d - 1 = \prod_{d' \mid d} \overline{\phi_{d'}(a)}$.

Pour $d' \in \mathbb{N}$ tel que $d' \mid d$, on a $d' \mid n$ donc par hypothèse, p ne divise aucun $\phi_{d'}(a)$ pour $d' \mid d$ donc $\overline{\phi_{d'}(a)} \neq 0$. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, c'est un anneau intègre donc $\prod_{d' \mid d} \overline{\phi_{d'}(a)} \neq 0$ d'où $\bar{a}^d - 1 \neq 0$.

Ainsi, l'ordre de \bar{a} est n d'où $n \mid p-1$ d'après le théorème de Lagrange donc p est de la forme $p = \lambda n + 1$ avec $\lambda \in \mathbb{Z}$. □

Passons à la preuve du théorème.

Preuve du théorème : Supposons qu'il existe un nombre fini de nombres premiers congrus à 1 modulo n noté $\{p_1, \dots, p_q\}$.

Il faut trouver un entier p premier différent de p_1, \dots, p_q congruent à 1 modulo n .

Nous allons utiliser le lemme avec $N = np_1 \dots p_q$ car si $p \equiv 1[N]$ alors $p \notin \{p_1, \dots, p_q\}$ et $p \equiv 1[n]$.

Soit $B = \prod_{d|N, d < N} \phi_d$, il suffit de trouver $a \in \mathbb{Z}$, p premier tel que $p | \phi_d(a)$ et $p \nmid B(a)$.

B est premier avec ϕ_N dans $\mathbb{C}[X]$ car n'ont pas de racine complexe en commun donc ne sont pas premiers entre eux dans $\mathbb{Q}[X]$ par invariance du pgcd par extension de corps (l'algorithme d'Euclide est le même dans $\mathbb{C}[X]$ et $\mathbb{Q}[X]$).

D'après le théorème de Bézout,

$$\exists(U, V) \in \mathbb{Q}[X]^2 / U\phi_N + VB = 1$$

Soit a un multiple du ppcm des dénominateurs des coefficients de U, V que l'on peut supposer tel que $\phi_N(a) \neq 0$ et $\phi_N(a) \neq \pm 1$ (possible car il y a une infinité de choix pour a).

En posant
$$\begin{cases} \tilde{U} &= aU \in \mathbb{Z}[X] \\ \tilde{V} &= aV \end{cases}$$

La relation de Bézout peut s'écrire $a = \tilde{U}\phi_N + \tilde{V}B$ d'où $a = \tilde{U}(a)\phi_N(a) + \tilde{V}(a)B(a)$.

Soit p un nombre premier divisant $\phi_N(a)$ alors $p | a^d - 1$ car ϕ_N divise $X^N - 1$ dans $\mathbb{Z}[X]$ donc dans $\mathbb{Z}/p\mathbb{Z}$, $\bar{a}^N = 1$ donc \bar{a} est inversible et donc a est premier avec p .

Si p divisait $B(a)$, alors p diviserait a ce qui est exclu.

Ainsi, d'après le lemme $p \equiv 1[N]$ et on a donc construit un nombre premier p tel que $p \notin \{p_1, \dots, p_q\}$ et $p \equiv 1[n]$ d'où la contradiction. \square

Théorème de Springer

Geoffrey Deperle

Leçons associées :

- 125 : Extension de corps. Exemples et applications.
- 141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.
- 170 : Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.

Le but de ce développement est de montrer le théorème suivant :

Théorème. *Soit \mathbb{K} un corps et \mathbb{L} une extension de degré m impair sur \mathbb{K} . Soit q une forme quadratique sur \mathbb{K}^n et on note aussi q son prolongement naturel sur \mathbb{L}^n . Si q possède un vecteur isotrope sur \mathbb{L}^n alors q possède un vecteur isotrope dans \mathbb{K}^n .*

Preuve : On procède par récurrence sur m .

Pour $m = 1$, le résultat est clair.

On fixe $m > 1$ impair et on suppose la propriété vraie jusqu'au rang $m - 2$.

Soit \mathbb{L} une extension de \mathbb{K} , q une forme quadratique sur \mathbb{K}^n et $v \in \mathbb{L}^n$ un vecteur isotrope.

Si \mathbb{L} est une tour d'extension $\mathbb{L} = \mathbb{K}[\alpha_1, \dots, \alpha_k]$ avec chaque étage de degré impair, il suffit de considérer un étage intermédiaire (extension de degré $< m$) et appliquer deux fois l'hypothèse de récurrence.

Supposons alors que \mathbb{L} est une extension monogène $\mathbb{L} = \mathbb{K}[\alpha]$, Soit $\mu \in \mathbb{K}[X]$ le polynôme minimal de α , soit $v = (v_1, \dots, v_n) \in \mathbb{L}^n$ isotrope non nul.

On a pour tout $i \in \llbracket 1, n \rrbracket$, $v_i \in \mathbb{K}[\alpha] = \mathbb{K} + \alpha\mathbb{K} + \dots + \alpha^{m-1}\mathbb{K}$ donc $v_i = g_i(\alpha)$ avec $g_i \in \mathbb{K}_{m-1}[X]$.

Donc $q(g_1(\alpha), \dots, g_n(\alpha)) = 0$ dans $\mathbb{K}[\alpha] \simeq \mathbb{K}[X]/(\mu)$ donc $q(g_1, \dots, g_n) = \mu h$ avec $h \in \mathbb{K}[X]$.

Étape 1 : Montrons que l'on peut supposer les g_i sont premiers entre eux

Supposons que ce n'est pas le cas, soit $\delta = \text{pgcd}(g_1, \dots, g_n)$, on a $\delta^2 q(\frac{g_1}{\delta}, \dots, \frac{g_n}{\delta}) = \mu h$ car q homogène de degré 2 donc $\delta^2 | \mu h$

Or $\mu \not\propto \delta$ car sinon on aurait $(g_1(\alpha), \dots, g_n(\alpha)) = 0$ donc $v = 0$. Absurde car v est supposé non nul.

Ainsi, comme μ est irréductible, par théorème de Gauss on a $\delta^2 | h$.

Ainsi, $q(\frac{g_1}{\delta}, \dots, \frac{g_n}{\delta}) = \mu \frac{h}{\delta^2}$ et les $\frac{g_i}{\delta}$ sont premiers entre eux. Par conséquent, quitte à diviser les g_i par δ , on peut supposer les g_i premiers entre eux.

Étape 2 : Raisonnons sur le degré de h

Supposons $h = 0$

Soit $x \in \mathbb{K}$, il existe $i \in \llbracket 1, n \rrbracket$, $g_i(x) \neq 0$ car sinon $X - x|g_j$ pour tout j et les polynômes ne seraient pas premiers entre eux.

Le vecteur $(g_1(x), \dots, g_n(x)) \in \mathbb{K}^n$ et $q(g_1(x), \dots, g_n(x)) = 0$.

Supposons $h \neq 0$

Comme $q(g_1, \dots, g_n) = \mu h$ et que q est un polynôme homogène de degré 2, $q(g_1, \dots, g_n)$ est de degré pair, comme $\deg(g_i) < m$ pour tout $i \in \llbracket 1, n \rrbracket$, $\deg(q(g_1, \dots, g_n)) < 2m$.

Donc $\deg(\mu h) < 2m$ et par conséquent $\deg h$ est impair et $< m$.

Ainsi, comme $\deg(h)$ est impair et que $\mathbb{K}[X]$ est factoriel, h admet une décomposition en produit d'irréductible et h admet un facteur h_0 de degré impair.

Posons $\mathbb{L}_0 = \mathbb{K}[X]/(h_0) \simeq \mathbb{K}[\beta]$ avec $\beta = \bar{X}$.

Comme $\deg(h_0) \leq \deg(h) < m$, $[\mathbb{L}_0 : \mathbb{K}] < [\mathbb{L} : \mathbb{K}]$ et comme β annule h_0 , on a $q(g_1(\beta), \dots, g_n(\beta)) = 0$.

Il reste alors à montrer que $(g_1(\beta), \dots, g_n(\beta))$ est non nul.

On a $\forall i \in \llbracket 1, n \rrbracket$, $g_i(\beta) = 0 \implies h_0 | g_i$ (polynôme minimal divise le polynôme annulateur).

Or, les g_i sont premiers entre eux. Contradiction.

Étape 3 : Conclusion

Le vecteur $(g_1(\beta), \dots, g_n(\beta))$ est donc un nouveau vecteur isotrope dans une extension de degré strictement inférieur à m impaire (de degré $\deg(h_0)$).

On applique l'hypothèse de récurrence pour obtenir un vecteur isotrope dans \mathbb{K}^n . □

Remarques

Remarque 2. Si l'extension est de degré pair, le résultat n'est plus vrai : $x^2 + y^2$ est anisotrope sur \mathbb{R} mais pas sur \mathbb{C} en prenant le vecteur $(1, i)$.

Remarque 3. Sur un corps fini, en dimension ≥ 3 et caractéristique $\neq 2$, toutes les formes quadratiques sont isotropes car si $q(x) = \sum_{i=1}^n a_i x_i^2$, on a $q(x) = 0 \iff a_1 x_1^2 + a_2 x_2^2 = -\sum_{i=3}^n a_i x_i^2$.

D'où avec $x_3 \neq 0, x_4 = 0, \dots, x_n = 0$, on a $a_1 x_1^2 + a_2 x_2^2 = -a_3$ et cette équation admet une solution.

En dimension 1, s'il existe un vecteur isotrope, alors $q = 0$

En dimension 2, on a deux classes d'équivalences :

- $q((x, y)) = x^2 + y^2$, q est isotrope si et seulement si -1 est un carré.
- $q((x, y)) = x^2 + \alpha y^2$ avec α non carré et la forme quadratique est isotrope si et seulement si $-\alpha$ est un carré.

Calcul de l'intégrale de Dirichlet

Geoffrey Deperle

Leçons associées :

- 235 : Problèmes d'interversion en analyse
- 236 : Illustrer par des exemples quelques méthodes de calcul d'intégrales de fonctions d'une ou plusieurs variables
- 239 : Fonction définies par une intégrale dépendant d'un paramètre. Exemples et applications.

Le but de ce développement est de montrer le théorème suivant :

Théorème.

$$\int_0^{+\infty} \frac{\sin(t)}{t} dt = \frac{\pi}{2}$$

Preuve :

Étape 1 : Justifions la convergence de cette intégrale

On a $\frac{\sin(t)}{t} \xrightarrow[t \rightarrow 0]{} 1$ et pour $X \geq 1$, on a en intégrant par parties,

$$\int_1^X \frac{\sin(t)}{t} dt = \left[-\frac{\cos(t)}{t} \right]_1^X - \int_1^X \frac{\cos(t)}{t^2} dt$$

et $t \mapsto \frac{\cos(t)}{t^2}$ est intégrable sur $[1, +\infty[$ car $\frac{\cos(t)}{t^2} = O_{t \rightarrow +\infty}(\frac{1}{t^2})$ donc l'intégrale entre 1 et X admet une limite finie lorsque $X \rightarrow +\infty$ d'où l'intégrale $\int_1^{+\infty} \frac{\sin(t)}{t} dt = \cos(1) - \int_1^{+\infty} \frac{\cos(t)}{t^2} dt$ est bien définie.

Étape 2 : Étudions la transformée de Laplace de sinc

Introduisons $F : x \mapsto \int_0^{+\infty} e^{-xt} \frac{\sin(t)}{t} dt$ la transformée de Laplace de sinc,

F est bien définie sur \mathbb{R}^{+*} car pour $x > 0$, on a $e^{-xt} \frac{\sin(t)}{t} = O_{t \rightarrow +\infty}(\frac{1}{t^2})$ donc $t \mapsto e^{-xt} \frac{\sin(t)}{t}$ est intégrable pour $x > 0$.

$F(x)$ est définie pour $x > 0$ et est définie pour $x = 0$ d'après précédemment.

Montrons que F est de classe C^1 sur \mathbb{R}^{+*} ,

Soit $f : (x, t) \in \mathbb{R}^+ \times \mathbb{R}^{+*} \mapsto e^{-xt} \frac{\sin(t)}{t}$, f est de classe C^∞ sur $(\mathbb{R}^{+*})^2$ avec $\partial_x f(x, t) = -e^{-xt} \sin(t)$.

Soit $a > 0$, pour tout $x \geq a$ et $t > 0$, $|\partial_x f(x, t)| = e^{-xt} |\sin(t)| \leq e^{-at}$ et $t \mapsto e^{-at}$ est intégrable sur

\mathbb{R}^+ , donc par théorème de dérivation sous le signe somme, F est de classe C^1 sur $]a, +\infty[$ donc sur \mathbb{R}^{+*} avec pour tout $x > 0$,

$$\begin{aligned} F'(x) &= - \int_0^{+\infty} e^{-xt} \sin(t) dt = -\text{Im} \left(\int_0^{+\infty} e^{-(x-i)t} dt \right) \\ &= \text{Im} \left(\frac{1}{i-x} \right) = -\frac{1}{1+x^2} \end{aligned}$$

Donc il existe $c \in \mathbb{R}$ tel que $\forall x > 0, F(x) = c - \arctan(x)$. Or, comme

$$|F(x)| \leq \int_0^{+\infty} e^{-xt} dt = \frac{1}{x} \xrightarrow{x \rightarrow +\infty} 0$$

On a donc $c = \frac{\pi}{2}$ et $\forall x > 0, F(x) = \frac{\pi}{2} - \arctan(x)$.

Pour montrer que $F(0) = 0$, il faut étudier la continuité de F en 0.

Étape 3 : Montrons la continuité de F en 0

Remarque 4. Il n'est pas possible d'utiliser le théorème de continuité sous le signe somme en l'état car $t \mapsto \frac{\sin(t)}{t}$ n'est pas intégrable sur \mathbb{R} .

$$\text{Posons } \begin{cases} F_1(x) = \int_0^1 e^{-xt} \frac{\sin(t)}{t} dt \\ F_2(x) = \int_1^{+\infty} e^{-xt} \frac{\sin(t)}{t} dt \end{cases} \text{ de sorte que } F = F_1 + F_2.$$

La fonction F_1 est de classe C^1 sur \mathbb{R}^+ car on dispose de la domination $|\partial_x f(x, t)| = e^{-xt} |\sin(t)| \leq 1$ et la constante 1 est intégrable sur $]0, 1]$.

Montrons la continuité de $F_2 = \text{Im}G$ avec $G : x \mapsto \int_1^{+\infty} \frac{e^{-(x-i)t}}{t} dt$.

Pour $X \geq 1$,

$$\int_1^X \frac{e^{-(x-i)t}}{t} dt = \left[\frac{1}{i-x} \frac{e^{-(x-i)t}}{t} \right]_1^X + \frac{1}{i-x} \int_1^X \frac{e^{-(x-i)t}}{t^2} dt$$

Comme $\left| \frac{e^{-(x-i)t}}{t^2} \right| \leq \frac{1}{t^2}$, la fonction $t \mapsto \frac{e^{-(x-i)t}}{t^2}$ est intégrable et

$$G(x) = \frac{e^{i-x}}{x-i} + \frac{1}{i-x} \int_1^{+\infty} \frac{e^{-(x-i)t}}{t^2} dt$$

Or, $(x, t) \mapsto \frac{e^{-(x-i)t}}{t^2}$ est continue sur $\mathbb{R}^+ \times [1, +\infty[$ et on dispose de la domination $\left| \frac{e^{-(x-i)t}}{t^2} \right| \leq \frac{1}{t^2}$ donc G est continue sur \mathbb{R}^+ donc F_2 et F le sont.

On a donc $F(0) = \int_0^{+\infty} \frac{\sin(t)}{t} dt$ □

Descente de gradient

Geoffrey Deperle

Leçons associées :

- 215 : Applications différentiables définies sur un ouvert de \mathbb{R}^n . Exemples et applications.
- 223 : Extremums : existence, caractérisation, recherche. Exemples et applications.
- 226 : Suites vectorielles et réelles définies par une relation de récurrence $u_{n+1} = f(u_n)$. Exemples. Applications.
- 229 : Fonctions monotones. Fonctions convexes. Exemples et applications.
- 253 : Utilisation de la notion de convexité en analyse.

Le but de ce développement est de montrer le théorème suivant :

Théorème. Soit $G : \mathbb{R}^n \rightarrow \mathbb{R}$ de classe C^2 et $\alpha > 0$ tels que pour tout $x, y \in \mathbb{R}^n$,

$$G(y) - G(x) \geq \langle \nabla G(x), y - x \rangle + \frac{\alpha}{2} \|y - x\|^2$$

G admet une borne inférieure sur \mathbb{R}^n et la suite (x_k) définie par :

$$\begin{cases} x_0 \in \mathbb{R}^n \\ \forall k \in \mathbb{N}, x_{k+1} = x_k + \lambda_k \nabla G(x_k) \end{cases}$$

où λ_k est tel que $x_k + \lambda_k \nabla G(x_k)$ est un minimum de G sur la droite $x_k + \mathbb{R} \nabla G(x_k)$.
La suite (x_k) converge vers cette borne inférieure.

Preuve :

Étape 1 : Montrons l'existence de $\inf G$

Pour $x = 0$, et $y \in \mathbb{R}^n$, l'hypothèse donne

$$G(y) \geq G(0) + \langle \nabla G(0), y \rangle + \frac{\alpha}{2} \|y\|^2 = \frac{\alpha}{2} \|y\|^2 + O(\|y\|)$$

donc $\lim_{\|y\| \rightarrow +\infty} G(y) = +\infty$ et G est coercive.

Rappelons les arguments justifiant qu'une fonction coercive sur \mathbb{R}^n admet un minimum global :
Il existe $A > 0$ tel que pour $\|x\| > A$, $G(x) > G(0)$. Comme \mathbb{R}^n est de dimension finie, la boule de centre 0 et de rayon A est un compact sur lequel G est continue donc borné et atteint son minimum en un point a .

Pour tout $\|x\| > A$, on a $G(x) > G(0) \geq G(a)$ donc G admet un minimum global sur \mathbb{R}^n en a .
Ce point est nécessairement un point critique donc $\nabla G(a) = 0$. Ainsi, pour $y \neq a$, on a

$$G(y) \geq G(a) + \frac{\alpha}{2} \|y - a\|^2 > G(a)$$

donc G admet son minimum uniquement en a .

Ce minimum est caractérisé par la condition $\nabla G(a) = 0$. En effet, soit $x \in \mathbb{R}^n$ tel que $\nabla G(x) = 0$, alors $G(a) - G(x) \geq \frac{\alpha}{2} \|a - x\|^2$ d'où $G(x) \leq G(a) - \frac{\alpha}{2} \|a - x\|^2$ donc comme le minimum de G est atteint en un unique point a , on a $\|a - x\|^2 = 0$ d'où $x = a$.

Étape 2 : Montrons que $\forall x \in \mathbb{R}^n$, $t \mapsto G(x + t\nabla G(x))$ atteint son minimum en un unique point

Soit $\varphi_x : t \mapsto G(x + t\nabla G(x))$, φ_x est C^1 et par composition des limites, $\varphi_x(t) \xrightarrow{t \rightarrow +\infty} +\infty$ donc φ_x possède un minimum en un point τ vérifiant $\varphi'_x(\tau) = 0$.

Or,

$$\varphi'_x(\tau) = dG(x + \tau\nabla G(x)) \cdot \nabla G(x) = \langle \nabla G(x + \tau\nabla G(x)), \nabla G(x) \rangle$$

donc $\nabla G(x + \tau\nabla G(x)) \perp \nabla G(x)$ car $\varphi'_x(\tau) = 0$.

Montrons l'unicité, soit $t \in \mathbb{R}^n$, si $t \neq \tau$, on a

$$\begin{aligned} \varphi_x(t) = G(x + t\nabla G(x)) &\geq G(x + \tau\nabla G(x)) + \langle \nabla G(x + t\nabla G(x)), (\tau - t)\nabla G(x) \rangle + \frac{\alpha}{2} |\tau - t|^2 \|\nabla G(x)\|^2 \\ &> \varphi_x(\tau) \end{aligned}$$

donc φ_x atteint son minimum en un unique point.

Étape 3 : Montrons la convergence de (x_k)

On a $\forall k \in \mathbb{N}$, $\nabla G(x_k) \perp \nabla G(x_{k+1})$.

Si l'un des $x_k = a$, alors la suite est stationnaire et est égale à a donc le résultat est acquis.

Sinon, la suite $(G(x_k))$ est décroissante par construction et minorée par $G(a)$ donc elle converge vers un réel l donc en particulier $G(x_k) - G(x_{k+1}) \xrightarrow{k \rightarrow +\infty} 0$. De plus,

$$\begin{aligned} G(x_k) - G(x_{k+1}) &\geq \langle \nabla G(x_{k+1}), x_k - x_{k+1} \rangle + \frac{\alpha}{2} \|x_k - x_{k+1}\|^2 \\ &= \lambda_k \langle \nabla G(x_{k+1}), \nabla G(x_k) \rangle + \frac{\alpha}{2} \|x_k - x_{k+1}\|^2 \\ &= \frac{\alpha}{2} \|x_k - x_{k+1}\|^2 \end{aligned}$$

donc $(x_k - x_{k+1})$ converge également vers 0 par théorème d'encadrement.

Comme il existe $A > 0$ tel que si $\|x\| > A$, $G(x) > G(x_0)$, par décroissance de $(G(x_k))$, on a nécessairement pour tout $k \in \mathbb{N}$, $x_k \in B(0, A)$.

Ainsi, comme (x_k) est une suite définie sur un espace de dimension finie, d'après le théorème de Bolzano-Weierstrass, (x_k) possède une valeur d'adhérence : il existe $\phi : \mathbb{N} \rightarrow \mathbb{N}$ strictement croissante et $x \in \mathbb{R}^n$ tel que $\lim_{k \rightarrow +\infty} x_{\phi(k)} = x$ et par continuité de ∇G , on a $\nabla G(x_{\phi(k)}) \xrightarrow{k \rightarrow +\infty} \nabla G(x)$.

Or, $(x_{\phi(k)+1})$ converge vers x car $\|x_{\phi(k)+1} - x_{\phi(k)}\| \leq \frac{2}{\alpha} (G(x_{\phi(k)+1}) - G(x_{\phi(k)}))$.

D'où

$$0 = \langle G(x_{\phi(k)+1}), G(x_{\phi(k)}) \rangle \xrightarrow{k \rightarrow +\infty} \|\nabla G(x)\|^2$$

d'où $\nabla G(x) = 0$ et $x = a$.

Donc la suite (x_k) admet une unique valeur d'adhérence, donc la suite (x_k) converge vers a . \square

Équation de Bessel

Geoffrey Deperle

Leçons associées :

- 220 : Équations différentielles ordinaires. Exemples de résolution et d'études de solutions en dimension 1 et 2.
- 221 : Équations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications.
- 241 : Suites et séries de fonctions. Exemples et contre-exemples.
- 243 : Séries entières, propriétés de la somme. Exemples et applications.
- 265 : Exemples d'études et d'applications de fonctions usuelles et spéciales.

Le but de ce développement est de montrer le théorème suivant :

Théorème. La fonction $J_0 : x \mapsto \sum_{n=0}^{+\infty} \frac{(-1)^n}{4^n n!^2} x^{2n}$ est bien définie sur \mathbb{R} et est l'unique solution de l'équation différentielle

$$(E) : xy'' + y' + xy = 0$$

développable en série entière vérifiant $J_0(0) = 1$

Preuve : Procédons par analyse-synthèse :

Analyse :

Soit f une solution développable en série entière au voisinage de 0, Il existe une suite $(a_n)_{n \in \mathbb{N}}$ et $R > 0$ tel que pour tout $x \in]-R, R[$, $f(x) = \sum_{n=0}^{+\infty} a_n x^n$. On a

$$\begin{cases} xf(x) &= \sum_{n=0}^{+\infty} a_n x^{n+1} = \sum_{n=1}^{+\infty} a_{n-1} x^n \\ xf''(x) &= \sum_{n=0}^{+\infty} n(n-1)a_n x^{n-1} = \sum_{n=1}^{+\infty} n(n+1)a_{n+1} x^n \end{cases}$$

D'où $(E) \iff \sum_{n=0}^{+\infty} (n+1)^2 a_{n+1} x^n + \sum_{n=1}^{+\infty} a_{n-1} x^n = 0$.

Par unicité du développement en série entière, on a

$$\begin{cases} a_1 = 0 \\ \forall n \in \mathbb{N}^*, (n+1)^2 a_{n+1} = -a_{n-1} \end{cases}$$

d'où $\forall n \in \mathbb{N}, a_{2n+1} = 0$ et $a_{2n} = \frac{(-1)^n a_0}{(2n)^2(2n-2)^2 \dots 2^2} = \frac{(-1)^n}{4^n n!^2} a_0$. Donc

$$\forall x \in]-R, R[, f(x) = a_0 \sum_{n=0}^{+\infty} \frac{(-1)^n}{4^n n!^2} x^{2n}$$

Synthèse :

La série ainsi obtenue a un rayon de convergence infini . En effet, d'après le critère de d'Alembert,

$$\forall x \in \mathbb{R}, \left| \frac{(-1)^{n+1} 4^n n!^2}{(-1)^n 4^{n+1} (n+1)!^2} x^2 \right| = \frac{x^2}{4(n+1)^2} \xrightarrow{n \rightarrow +\infty} 0$$

donc f définit une fonction développable en série entière dont les coefficients vérifient la récurrence établie : f est donc solution de l'équation différentielle.

Comme $f(0) = a_0$, il existe une unique solution développable en série entière et vérifiant $f(0) = 1$

définie par $f(x) = \sum_{n=0}^{+\infty} \frac{(-1)^n}{4^n n!^2} x^{2n}$ □

Lemme 9. Soit J_0 la solution développable en série entière tel que $J_0(0) = 1$ et f une solution de l'équation sur un intervalle $]0, a[$, (f, J_0) est libre si et seulement si f n'est pas borné au voisinage de 0.

Preuve du lemme : Si (f, J_0) est liée, comme J_0 est bornée au voisinage de 0, f est bornée au voisinage de 0.

Supposons (f, J_0) libre, sur $]0, a[$, l'ensemble des solutions de (E) est un espace vectoriel de dimension 2 dont (f, J_0) est une base. Considérons le Wronskien $W = fJ_0' - J_0f'$ de la famille (f, J_0) . On a $\forall x \in]0, a[, W'(x) = -\frac{1}{x}W(x)$ donc

$$\exists C \in \mathbb{R}, \forall x \in]0, a[, W(x) = Ce^{-\ln(x)} = \frac{C}{x}$$

Comme (f, J_0) est libre, on a $C \neq 0$, donc $\forall x \in]0, a[, f(x)J_0'(x) - J_0(x)f'(x) = \frac{C}{x}$.

Si f est borné au voisinage de 0, comme $\begin{cases} J_0(x) \xrightarrow{x \rightarrow 0} 1 \\ J_0'(x) \xrightarrow{x \rightarrow 0} 0 \end{cases}$. On a $f'(x) \underset{x \rightarrow 0}{\sim} -\frac{C}{x}$ donc pour $b \in]0, a[$,

comme $x \mapsto -\frac{C}{x}$ garde un signe constant sur $]0, b[$ et n'est pas intégrable sur $]0, b[$, par intégration des relations de comparaison

$$f(x) - f(b) = \int_b^x f'(t) dt \sim -C \int_b^x \frac{dt}{t} = -C(\ln(x) - \ln(b))$$

d'où $f(x) \underset{x \rightarrow 0}{\sim} -C \ln(x)$ d'où $\lim_{x \rightarrow 0} f(x) = +\infty$ ce qui contredit l'hypothèse f borné. D'où l'équivalence,

□

Application.

$$\forall x \in \mathbb{R}, \frac{1}{\pi} \int_0^\pi \cos(x \sin \theta) d\theta = \sum_{n=0}^{+\infty} \frac{(-1)^n}{4^n n!} x^{2n}$$

Preuve : La fonction $(x, \theta) \mapsto \frac{1}{\pi} \cos(x \sin(\theta))$ est de classe C^∞ donc en posant $g : x \mapsto \frac{1}{\pi} \int_0^\pi \cos(x \sin \theta) d\theta$, par dérivation sous le signe somme :

$$\begin{aligned} \forall x \in \mathbb{R}, g'(x) &= -\frac{1}{\pi} \int_0^\pi \sin(x \sin \theta) \sin \theta d\theta \\ g''(x) &= -\frac{1}{\pi} \int_0^\pi \cos(x \sin \theta) \sin^2 \theta d\theta \end{aligned}$$

donc

$$\begin{aligned} xg''(x) + g'(x) + xg(x) &= \frac{1}{\pi} \int_0^\pi [(x \cos(x \sin \theta) \cos^2 \theta) - \sin(x \sin \theta) \sin \theta] d\theta \\ &= \frac{1}{\pi} [\sin(x \sin \theta) \cos \theta]_0^\pi \end{aligned}$$

Donc g est solution de (E) et est bornée sur \mathbb{R} donc (J_0, g) est liée sur $]0, +\infty[$, comme $J_0(0) = g(0)$, il y a égalité sur \mathbb{R}^+ et sur \mathbb{R} par parité. \square

Équivalent d'une suite définie par récurrence

Geoffrey Deperle

Leçons associées :

- 223 : Suites numériques. Convergence, valeurs d'adhérence. Exemples et applications.
- 224 : Exemples de développements asymptotiques de suites et de fonctions.
- 226 : Suites vectorielles et réelles définies par une relation de récurrence $u_{n+1} = f(u_n)$. Exemples. Applications à la résolution approchée d'équations.
- 230 : Séries de nombres réels ou complexes. Comportement des restes ou de sommes partielles des séries numériques. Exemples.

Le but de ce développement est de montrer le théorème suivant :

Théorème. Soit $c > 0$ et $f : [0, c] \rightarrow [0, c]$ une fonction continue, admettant en 0 un développement asymptotique de la forme $f(x) = x - ax^\alpha + o(x^\alpha)$ où $a > 0$ et $\alpha > 1$.

Pour u_0 assez petit, la suite (u_n) définie par $u_{n+1} = f(u_n)$ pour tout $n \in \mathbb{N}$ converge vers 0 et on a

$$u_n \underset{n \rightarrow \infty}{\sim} (na(\alpha - 1))^{\frac{1}{1-\alpha}}$$

Preuve :

Étape 1 : Montrons la convergence de (u_n)

Par continuité de f , on a $f(0) = 0$ et avec le développement asymptotique, il existe $\eta > 0$ tel que pour tout $x \in]0, \eta]$, $f(x) < x$. Si $u_0 \in]0, \eta]$, la suite (u_n) est décroissante et positive donc par théorème de convergence monotone, la suite (u_n) converge vers l'unique point fixe sur $[0, c]$ donc converge vers 0.

Étape 2 : Montrons l'équivalence de (u_n)

Déterminons β tel que $(u_{n+1}^\beta - u_n^\beta)$ ait une limite non nulle. Comme $\alpha > 1$, on a

$$\begin{aligned} f(x)^\beta - x^\beta &= (x - ax^\alpha + o_{x \rightarrow 0}(x^\alpha))^\beta - x^\beta \\ &= x^\beta [1 - x^{\alpha-\beta} + o_{x \rightarrow 0}(x^{\alpha-\beta})]^\beta - x^\beta \\ &= x^\beta [-a\beta x^{\alpha-1} + o_{x \rightarrow 0}(x^{\alpha-1})] \underset{x \rightarrow 0}{\sim} -a\beta x^{\alpha+\beta-1} \end{aligned}$$

En prenant $\beta = 1 - \alpha$, on a $f(x)^\beta - x^\beta \xrightarrow{x \rightarrow 0} a(\alpha - 1)$.

En particulier, comme la suite (u_n) converge vers 0, on a $u_{n+1}^{1-\alpha} - u_n^{1-\alpha} \xrightarrow{n \rightarrow +\infty} a(\alpha - 1)$.

Par théorème de Cesaro, on a $u_n^{1-\alpha} \underset{n \rightarrow +\infty}{\sim} u_n^{1-\alpha} - u_n^{1-\alpha} \underset{n \rightarrow +\infty}{\sim} na(\alpha - 1)$. D'où

$$u_n \underset{n \rightarrow +\infty}{\sim} (na(\alpha - 1))^{\frac{1}{1-\alpha}}$$

□

Application. Soit (u_n) la suite définie par $u_0 > 0$ et pour tout $n \in \mathbb{N}$, $u_{n+1} = \ln(1 + u_n)$. On a

$$u_n = \frac{2}{n} + \frac{2 \ln(n)}{3n^2} + \underset{n \rightarrow +\infty}{o} \left(\frac{\ln(n)}{n^2} \right)$$

Preuve : Comme $\ln(1 + x) = x - \frac{x^2}{2} + \underset{x \rightarrow 0}{o}(x^2)$ donc en appliquant le théorème précédent avec $\alpha = 2$ et $a = -\frac{1}{2}$ on a $u_n \underset{n \rightarrow +\infty}{\sim} \frac{2}{n}$.

Pour aller plus loin, poussons le développement asymptotique :

$$\begin{aligned} u_{n+1}^{-1} - u_n^{-1} &= \left(u_n - \frac{1}{2}u_n^2 + \frac{1}{3}u_n^3 + \underset{n \rightarrow +\infty}{o}(u_n^3) \right)^{-1} - u_n^{-1} \\ &= u_n^{-1} \left(\left(1 - \frac{1}{2}u_n + \frac{1}{3}u_n^2 + \underset{n \rightarrow +\infty}{o}(u_n^2) \right)^{-1} - 1 \right) \\ &= u_n^{-1} \left(\frac{1}{2}u_n - \frac{1}{3}u_n^2 + \frac{1}{4}u_n^2 + \underset{n \rightarrow +\infty}{o}(u_n^2) \right) \\ &= \frac{1}{2} - \frac{1}{3}u_n + \frac{1}{4}u_n + \underset{n \rightarrow +\infty}{o}(u_n) = \frac{1}{2} - \frac{1}{12}u_n + \underset{n \rightarrow +\infty}{o}(u_n) \end{aligned}$$

Donc en posant $x_n = u_{n+1}^{-1} - u_n^{-1} - \frac{1}{2}$, on a $x_n \underset{n \rightarrow +\infty}{\sim} -\frac{1}{12}u_n \underset{n \rightarrow +\infty}{\sim} -\frac{1}{6n}$.

Comme $\left\{ \begin{array}{l} \sum \frac{1}{6n} \text{ diverge} \\ \left(\frac{1}{6n} \right) \text{ est de signe constant} \end{array} \right.$, on a par sommation des relations de comparaison,

$$\sum_{k=1}^n x_k \underset{n \rightarrow +\infty}{\sim} -\frac{1}{6} \sum_{k=1}^n \frac{1}{k} \underset{n \rightarrow +\infty}{\sim} -\frac{1}{6} \ln(n)$$

D'où

$$u_n^{-1} - u_1^{-1} = \sum_{k=1}^{n-1} u_{k+1}^{-1} - u_k^{-1} = \frac{n}{2} + \sum_{k=0}^{n-1} x_k = \frac{n}{2} - \frac{1}{6} \ln(n) + \underset{n \rightarrow +\infty}{o}(\ln(n))$$

D'où

$$\begin{aligned} u_n &= \left(\frac{n}{2} - \frac{1}{6} \ln(n) + \underset{n \rightarrow +\infty}{o}(\ln(n)) \right)^{-1} \\ &= \frac{2}{n} \left(1 - \frac{\ln(n)}{3} + \underset{n \rightarrow +\infty}{o} \left(\frac{\ln(n)}{n} \right) \right)^{-1} \\ &= \frac{2}{n} + \frac{2 \ln(n)}{3n^2} + \underset{n \rightarrow +\infty}{o} \left(\frac{\ln(n)}{n^2} \right) \end{aligned}$$

□

Formule sommatoire de Poisson et formule de Shannon

Geoffrey Deperle

Leçons associées :

- 241 : Suites et séries de fonctions. Exemples et contre-exemples.
- 246 : Séries de Fourier. Exemples et applications.
- 250 : Transformation de Fourier. Applications.

Le but de ce développement est de montrer le théorème suivant :

Théorème. Soit $f \in \mathcal{S}(\mathbb{R})$ alors pour tout réel t , on a

$$\sum_{k \in \mathbb{Z}} f(t + 2k\pi) = \frac{1}{2\pi} \sum_{n \in \mathbb{Z}} \hat{f}(n) e^{inx}$$

Preuve :

Étape 1 : Montrons la convergence de $\varphi : x \mapsto \sum_{k \in \mathbb{Z}} f(x + 2k\pi)$ et de sa dérivée sur tout compact

Soit K un compact de \mathbb{R} inclus dans un intervalle de la forme $[-\alpha, \alpha]$, $\alpha > 0$.

Comme $x^2 f(x) \xrightarrow{x \rightarrow \pm\infty} 0$, il existe $a > 0$ tel que $|x^2 f(x)| \leq 1$ pour $|x| \geq a$, pour $|x| \leq \alpha$ et $k \in \mathbb{Z}$, on a $|x + 2k\pi| \geq |2k\pi| - |x| \geq 2|k|\pi - \alpha$ d'où $|x + 2k\pi| \geq a$ si $|k| \geq \frac{\alpha+a}{2\pi}$.

Pour $|k| \geq \frac{\alpha+a}{2\pi}$, $f(x + 2k\pi) \leq \frac{1}{(x+2k\pi)^2} \leq \frac{1}{(2|k|\pi - \alpha)^2}$.

Comme $\sum \frac{1}{(2|k|\pi - \alpha)^2}$ est convergente, la série $\sum f(\cdot + 2k\pi)$ converge uniformément sur $[-\alpha, \alpha]$.

De plus, f' vérifie la même hypothèse que f d'où $\sum f'(\cdot + 2k\pi)$ converge uniformément sur tout intervalle $[-\alpha, \alpha]$.

Par théorème de dérivation des série de fonctions, $\varphi : x \mapsto \sum_{k \in \mathbb{Z}} f(x + 2k\pi)$ est de classe C^1 sur $[-\alpha, \alpha]$.

Étape 2 : Développons φ en série de Fourier

Comme φ est 2π -périodique, notons $c_n(\varphi)$ ses coefficients de Fourier, on a pour tout $n \in \mathbb{N}$;

$$\begin{aligned} c_n(\varphi) &= \frac{1}{2\pi} \int_0^{2\pi} \varphi(x) e^{-inx} dx \\ &= \frac{1}{2\pi} \sum_{n \in \mathbb{Z}} \int_0^{2\pi} f(x + 2k\pi) e^{-inx} dx \quad \text{par convergence uniforme} \\ &= \frac{1}{2\pi} \sum_{n \in \mathbb{Z}} \int_{2k\pi}^{2(k+1)\pi} f(x) e^{-inx} \\ &= \frac{1}{2\pi} \int_{\mathbb{R}} f(x) e^{-inx} \quad \text{l'intégrale a un sens car } |f(x) e^{-inx}| = |f(x)| = o\left(\frac{1}{x^2}\right) \text{ au voisinage de } \pm\infty \end{aligned}$$

Comme φ est \mathcal{C}^1 est 2π -périodique, le théorème de convergence normale de Dirichlet assure que pour tout réel x ,

$$\varphi(x) = \sum_{n \in \mathbb{Z}} c_n(\varphi) e^{inx} = \sum_{n \in \mathbb{Z}} \left(\frac{1}{2\pi} \int_{\mathbb{R}} f(t) e^{-int} dt \right) e^{inx} = \sum_{n \in \mathbb{Z}} \hat{f}(n) e^{inx}$$

□

Théorème. *Supposons que le support de \hat{f} est inclus dans $[-F, F]$ avec $F \in \mathbb{R}^{+*}$.
Si $0 \leq F \leq \pi$, alors pour tout $t \in \mathbb{R}$,*

$$f(t) = \sum_{n \in \mathbb{Z}} f(n) \frac{\sin((n-t)\pi)}{(n-t)\pi}$$

Preuve : En appliquant la formule sommatoire de Poisson à $\hat{f} \in S(\mathbb{R})$ (car $f \in S(\mathbb{R})$), on a

$$\forall \xi \in \mathbb{R}, \sum_{k \in \mathbb{Z}} \hat{f}(\xi + 2k\pi) = \frac{1}{2\pi} \sum_{n \in \mathbb{Z}} \hat{f}(n) e^{in\xi}$$

Or, par formule d'inversion de Fourier, $\hat{f}(n) = 2\pi f(-n)$. D'où

$$\forall \xi \in \mathbb{R}, \sum_{k \in \mathbb{Z}} \hat{f}(\xi + 2k\pi) = \sum_{n \in \mathbb{Z}} f(-n) e^{in\xi}$$

Comme $2F \leq 2\pi$, on a pour tout k non nul, $\hat{f}(2k\pi + \cdot)$ est nul en dehors de $[-\pi, \pi]$ donc :

$$\hat{f} = \mathbf{1}_{[-\pi, \pi]} \sum_{k \in \mathbb{Z}} \hat{f}(2k\pi + \cdot) = \mathbf{1}_{[-\pi, \pi]} \sum_{n \in \mathbb{Z}} f(-n) e^{in\bullet}$$

Et en ré-applicant la formule d'inversion de Fourier, on a

$$\begin{aligned} f(t) &= \frac{1}{2\pi} \int_{\mathbb{R}} \left(\mathbf{1}_{[-\pi, \pi]}(\xi) \sum_{n \in \mathbb{Z}} f(-n) e^{in\xi} \right) e^{i\xi t} d\xi \\ &= \frac{1}{2\pi} \int_{-\pi}^{\pi} \left(\sum_{n=-\infty}^{+\infty} f(-n) e^{i\xi(t+n)} \right) d\xi \\ &= \frac{1}{2\pi} \int_{-\pi}^{\pi} \sum_{n=-\infty}^{+\infty} f(m) e^{i\xi(t-m)} d\xi \end{aligned}$$

Or, la série $\sum_{m \in \mathbb{Z}} f(m) e^{i\xi(t-m)}$ converge absolument donc uniformément sur $[-\pi, \pi]$ car

$$\forall m \in \mathbb{Z}, \|f(m) e^{i(t-m)}\|_{\infty} = |f(m)| \text{ et } \sum |f(m)| \text{ converge}$$

D'où

$$\begin{aligned} f(t) &= \sum_{m \in \mathbb{Z}} f(m) \times \frac{1}{2\pi} \int_{-\pi}^{\pi} e^{i\xi(t-m)} d\xi \\ &= \sum_{m \in \mathbb{Z}} f(m) \times \frac{1}{2\pi} \left[\frac{e^{i\xi(t-m)}}{i(t-m)} \right]_{-\pi}^{\pi} \\ &= \sum_{m \in \mathbb{Z}} f(m) \times \frac{1}{2\pi} \frac{\sin(\pi(t-m))}{i(t-m)} \\ &= \sum_{n \in \mathbb{Z}} f(n) \frac{\sin((n-t)\pi)}{(n-t)\pi} \end{aligned}$$

□

Application (Équation fonctionnelle de Θ). Soit Θ la fonction de Jacobi définie par

$$\begin{aligned} \Theta :]0, +\infty[&\rightarrow \mathbb{R} \\ x &\mapsto \sum_{n \in \mathbb{Z}} e^{-\pi n^2 x} \end{aligned}$$

On a

$$\forall x > 0, \Theta(x) = \frac{1}{\sqrt{x}} \Theta\left(\frac{1}{x}\right)$$

Preuve : En appliquant la formule sommatoire de Poisson à $f : t \mapsto e^{-\alpha t^2} \in S(\mathbb{R})$ de transformée de Fourier $\hat{f} : t \mapsto \sqrt{\frac{\pi}{\alpha}} e^{-\frac{t^2}{4\alpha}}$. On a :

$$\sum_{k \in \mathbb{Z}} e^{-\alpha(t+2k\pi)^2} = \frac{1}{2\pi} \sum_{k \in \mathbb{Z}} \sqrt{\frac{\pi}{\alpha}} e^{-\frac{t^2}{4\alpha}} e^{int}$$

Donc en évaluant en 0,

$$\sum_{k \in \mathbb{Z}} e^{-4k^2\pi^2\alpha} = \frac{1}{2\pi} \sum_{k \in \mathbb{Z}} \sqrt{\frac{\pi}{\alpha}} e^{-\frac{k^2}{4\alpha}}$$

Avec $x = 2\alpha\pi$, on a

$$\sum_{k \in \mathbb{Z}} e^{-\pi k^2 x} = \frac{1}{\sqrt{x}} \sum_{k \in \mathbb{Z}} e^{-\frac{\pi k^2}{x}}$$

D'où le résultat. □

Indécomposabilité de la loi de Poisson

Geoffrey Deperle

Leçons associées :

- 243 : Séries entières, propriétés de la somme. Exemples et applications.
- 245 : Fonctions d'une variable complexe. Exemples et applications.
- 261 : Loi d'une variable aléatoire : caractérisations, exemples, applications.
- 264 : Variables aléatoires discrètes. Exemples et applications.
- 266 : Illustration de la notion d'indépendance.

Le but de ce développement est de montrer le théorème suivant :

Théorème. *Soit Z une variable aléatoire suivant une loi de poisson de paramètre $\lambda > 0$ et soient X et Y deux variables indépendantes à valeurs dans \mathbb{N} telles que $Z = X + Y$ alors X et Y suivent des loi de Poisson.*

Preuve : Soit G_Z , (resp. G_X, G_Y) la série génératrice de Z (resp. X, Y). On a par indépendance de X et Y , la décomposition $\forall |z| < 1, G_Z(z) = G_X(z)G_Y(z)$.

On a pour tout $s \in \mathbb{C}$,

$$\begin{aligned} G_Z(s) &= \sum_{n=0}^{+\infty} \mathbb{P}(Z = n) s^n \\ &= \sum_{n=0}^{+\infty} e^{-\lambda} \frac{\lambda^n}{n!} s^n = e^{-\lambda} \sum_{n=0}^{+\infty} \frac{(\lambda s)^n}{n!} = e^{\lambda(s-1)} \end{aligned}$$

Nous allons identifier la loi de X et Y en identifiant les fonctions génératrices G_X et G_Y .

Étape 1 : Montrons qu'il existe F, G des fonctions entières tel que $G_X = e^F$ et $G_Y = e^G$.

G_X et G_Y se développent en série entière à coefficients positifs.

On a par indépendance de X et Y , $\forall n \in \mathbb{N}, \mathbb{P}(X = n)\mathbb{P}(Y = 0) \leq \mathbb{P}(Z = n) = e^{-\lambda} \frac{\lambda^n}{n!}$ avec de plus $\mathbb{P}(X = 0)\mathbb{P}(Y = 0) = \mathbb{P}(Z = 0) \neq 0$, donc $\mathbb{P}(Y = 0) \neq 0$ donc $\mathbb{P}(X = n) \leq \frac{e^{-\lambda}}{\mathbb{P}(Y = 0)} \frac{\lambda^n}{n!}$.

Donc, par comparaison, G_X (et de même G_Y) est somme de série entière de rayon de convergence infini.

Par le principe du prolongement analytique, l'identité valable pour $|z| \leq 1$, se prolonge sur \mathbb{C} :

$$\forall z \in \mathbb{C}, G_X(z)G_Y(z) = e^{\lambda(z-1)}$$

Ainsi, G_X et G_Y ne s'annulent pas, donc il existe F, G analytique sur \mathbb{C} tel que $\begin{cases} G_X = e^F \\ G_Y = e^G \end{cases}$.

Étape 2 : Identifions F et G .

Si $|z| = r \geq 1$, alors $|G_X(z)| \leq G_X(|z|) = G_X(r)$ car les coefficients de la série entière définissant G_X sont positifs.

De plus, $\mathbb{P}(Y = 0)G_X(r) \leq G_X(r)G_Y(r) = e^{\lambda(r-1)}$.

Donc, $|G_X(z)| = \underbrace{|\exp(F(z))|}_{=\exp(\operatorname{Re}(F(z)))} \leq Ce^{\lambda(r-1)}$ avec $C = \frac{G_Y(r)}{\mathbb{P}(Y=0)}$.

Donc, $\operatorname{Re}(F(z)) \leq \ln C + \lambda(|z| - 1)$.

Afin de conclure, nous allons utiliser le lemme suivant.

Lemme 10. Soit $f = u + iv$, $f(z) = \sum_{n=0}^{+\infty} a_n z^n$ une fonction entière, alors si $A(r) = \sup_{|z|=r} \operatorname{Re} f(z)$,
on a

1. $\forall n \geq 1, r > 0, |a_n| \leq 2 \frac{A(r) - u(0)}{r^n}$.

2. Si $d \geq 0$ et $A(r) = O(r^d)$ alors f est une fonction polynomiale de degré $\leq d$.

Preuve : Soit $r > 0$, la série $\theta \mapsto \sum_{n=0}^{+\infty} a_n r^n e^{in\theta}$ converge uniformément vers $\theta \mapsto f(re^{i\theta})$ donc

$$\begin{cases} a_n r^n &= \frac{1}{2\pi} \int_0^{2\pi} f(re^{i\theta}) e^{-in\theta} d\theta & L_1 \\ 0 &= \frac{1}{2\pi} \int_0^{2\pi} f(re^{i\theta}) e^{in\theta} d\theta & L_2 \end{cases} . \text{ Donc en effectuant } L_1 + \overline{L_2}, \text{ on a}$$

$$\begin{aligned} a_n r^n &= \frac{1}{\pi} \int_0^{2\pi} u(re^{i\theta}) e^{-in\theta} d\theta \\ &= \frac{1}{\pi} \int_0^{2\pi} (u(re^{i\theta}) - A(r)) e^{-in\theta} d\theta + \underbrace{\frac{1}{\pi} \int_0^{2\pi} A(r) e^{-in\theta} d\theta}_{=0} \end{aligned}$$

D'où $|a_n r^n| = |a_n| r^n \leq \frac{1}{\pi} \int_0^{2\pi} (A(r) - u(re^{i\theta})) d\theta$.

Or, $a_0 r^0 = \frac{1}{2\pi} \int_0^{2\pi} f(re^{i\theta}) d\theta = f(0)$ donc $u(0) = \frac{1}{2\pi} \int_0^{2\pi} u(re^{i\theta}) d\theta$ d'où l'inégalité $|a_n| \leq 2 \frac{A(r) - u(0)}{r^n}$.

De plus, si $A(r) = O(r^d)$, alors en passant à la limite $n \rightarrow +\infty$ dans l'inégalité, on a $a_n = 0$ pour $n > d$ donc f est une fonction polynomiale de degré $\leq d$. \square

Le lemme s'applique à la fonction F et $d = 1$, F est donc de la forme $F(z) = \alpha z + a$.

Or, $G_X(1) = 1$ donc $e^{\alpha} e^a = 1$ donc $G_X(z) = e^{\alpha(z-1)}$.

Comme $G'_X(z) = \alpha e^{\alpha(z-1)}$, on a $G'_X(1) = \alpha$. Comme $G'_X(1) = \sum_{n=0}^{+\infty} n \mathbb{P}(X = n) \geq 1$, on a $\alpha \in \mathbb{R}^+$.

Donc $X \sim \mathcal{P}(\alpha)$.

De même, Y suit une loi de Poisson de paramètre $\beta \in \mathbb{R}^+$ tel que $\alpha + \beta = \lambda$. \square

Inégalité de Hoeffding et applications

Geoffrey Deperle

Leçons associées :

- 261 : Loi d'une variable aléatoire : caractérisations, exemples, applications.
- 262 : Convergences d'une suite de variables aléatoires. Théorèmes limite. Exemples et applications.
- 264 : Variables aléatoires discrètes. Exemples et applications.
- 266 : Illustration de la notion d'indépendance en probabilités.

Le but de ce développement est de montrer le théorème suivant :

Lemme 11. *Soit X une variable réelle, centrée, bornée par 1 presque sûrement alors*

$$\forall t \in \mathbb{R}^{+*}, \mathbb{E}[\exp(tX)] \leq \exp\left(\frac{t^2}{2}\right)$$

Preuve : Pour $x \in [-1, 1]$ et $t \in \mathbb{R}$, on a $\left\{ \begin{array}{l} \frac{1-x}{2} + \frac{1+x}{2} = 1 \\ \frac{1-x}{2} \in [0, 1] \end{array} \right.$ donc $\frac{1-x}{2}(-t) + \frac{1+x}{2}t = tx$ est une combinaison convexe de $-t$ et t .

Par convexité de \exp ,

$$\forall t \in \mathbb{R}, \exp(tx) \leq \frac{1-x}{2} \exp(-t) + \frac{1+x}{2} \exp(t)$$

Pour $u \in \mathbb{R}$, uX est bornée p.s. donc $\exp(uX)$ est bornée p.s. donc intégrable. Donc pour $t \in \mathbb{R}$,

$$\begin{aligned} L_X(t) &:= \mathbb{E}[\exp(tX)] \\ &\leq \frac{1}{2} \mathbb{E}[(1-X) \exp(-t)] + \frac{1}{2} \mathbb{E}[(1+X) \exp(t)] \\ &\leq \frac{1}{2} (\exp(-t) + \exp(t)) \quad \text{car } \mathbb{E}[X] = 0 \\ &\leq \cosh(t) \end{aligned}$$

Or, comme $\forall k \in \mathbb{N}^*, 2^k k! = 2 \times 4 \times 6 \times \cdots \times 2(k-1) \times 2k \leq (2k)!$.

Donc pour tout $t \in \mathbb{R}$,

$$\cosh(t) = \sum_{k=0}^{+\infty} \frac{t^{2k}}{(2k)!} \leq \sum_{k=0}^{+\infty} \frac{t^{2k}}{2^k k!} = \exp\left(\frac{t^2}{2}\right)$$

d'où le résultat. □

Théorème. Soit $(X_n)_{n \in \mathbb{N}}$ une suite de variable aléatoires réelles indépendantes, centrées, bornées p.s. : $\forall n \in \mathbb{N}, \exists c_n > 0 / |X_n| \leq c_n$.

Soit $S_n = \sum_{k=1}^n X_k$, alors

$$\forall n \in \mathbb{N}, \varepsilon > 0, \mathbb{P}(|S_n| \geq \varepsilon) \leq 2 \exp\left(\frac{\varepsilon^2}{2 \sum_{k=1}^n c_k^2}\right)$$

Preuve : Soit $n \in \mathbb{N}, t \in \mathbb{R}^{+*}$,

Étape 1 : Donnons une majoration de $\mathbb{E}[\exp(tS_n)]$

La variable aléatoire $\frac{X_n}{c_n}$ est bornée p.s. par 1 et centrée, donc d'après le lemme

$$\forall t' \in \mathbb{R}^{+*}, \mathbb{E}[\exp\left(t' \frac{X_n}{c_n}\right)] \leq \exp\left(\frac{t'^2}{2}\right)$$

Avec $t' = tc_n$, on a donc $\mathbb{E}[\exp(tX_n)] \leq \exp\left(\frac{t^2 c_n^2}{2}\right)$. Ainsi,

$$\begin{aligned} \mathbb{E}[\exp(tS_n)] &= \prod_{k=1}^n \mathbb{E}[\exp(tX_k)] \quad \text{car les } \exp(tX_k) \text{ sont indépendantes} \\ &\leq \prod_{k=1}^n \exp\left(\frac{t^2 c_k^2}{2}\right) \\ &\leq \exp\left(\frac{t^2}{2} \sum_{k=1}^n c_k^2\right) \end{aligned}$$

Étape 2 : Établissons l'inégalité avec l'inégalité de Markov

Soit $\varepsilon > 0$, la fonction $x \mapsto \exp(tx)$ est strictement croissante donc $[S_n > \varepsilon] = [\exp(tS_n) > \exp(t\varepsilon)]$ d'où

$$\begin{aligned} \mathbb{P}(S_n > \varepsilon) &\leq \mathbb{P}(\exp(tS_n) > \exp(t\varepsilon)) \\ &\leq \frac{\mathbb{E}[\exp(tS_n)]}{\exp(t\varepsilon)} \\ &\leq \exp\left(\frac{t^2}{2} \sum_{k=1}^n c_k^2 - t\varepsilon\right) \end{aligned}$$

Étape 3 : Optimisons l'inégalité

En posant $a = \sum_{k=1}^n c_k^2$, la fonction $t \mapsto \frac{a}{2}t^2 - \varepsilon t$ atteint son minimum en $\frac{-\varepsilon}{2a}$ pour $t = \frac{\varepsilon}{a} > 0$. Par croissance de l'exponentielle, on a donc

$$\mathbb{P}(S_n > \varepsilon) \leq \exp\left(\frac{\varepsilon^2}{2 \sum_{k=1}^n c_k^2}\right)$$

Conclusion

On a $[|S_n| > \varepsilon] = [S_n > \varepsilon] \cup [-S_n > \varepsilon]$, on a

$$\forall n \in \mathbb{N}, \varepsilon > 0, \mathbb{P}(|S_n| \geq \varepsilon) \leq 2 \exp\left(\frac{\varepsilon^2}{2 \sum_{k=1}^n c_k^2}\right)$$

□

Intéressons nous à trois applications.

Application ((261, 264)). Soit $(X_i)_{i \in [1, n]}$ des variables aléatoires iid de loi $X_1 \sim \mathcal{B}(p)$ avec $p \in]0, 1[$ et $\alpha \in]0, 1[$, alors un intervalle de confiance par excès de niveau $1 - \alpha$ de paramètre p est

$$I_{1-\alpha} = \left[\frac{1}{n} S_n - \sqrt{\frac{2}{n} \ln \left(\frac{2}{\alpha} \right)}, \frac{1}{n} S_n + \sqrt{\frac{2}{n} \ln \left(\frac{2}{\alpha} \right)} \right]$$

Preuve : On applique l'inégalité de Hoeffding à $(X_n - p)$ qui est borné par 1

$$\mathbb{P} \left(\left| \frac{1}{n} S_n - p \right| > \varepsilon \right) = \mathbb{P} \left(\left| \sum_{k=1}^n X_k - p \right| > n\varepsilon \right) \leq 2 \exp \left(-\frac{n^2 \varepsilon^2}{2n} \right)$$

Soit $\varepsilon' = \sqrt{\frac{2}{n} \ln \left(\frac{2}{\alpha} \right)}$ tel que $\alpha = 2 \exp(-\frac{n\varepsilon'^2}{2})$ d'où

$$\mathbb{P} \left(\left| \frac{1}{n} S_n - p \right| < \varepsilon' \right) = 1 - \mathbb{P} \left(\left| \frac{1}{n} S_n - p \right| > \varepsilon \right) \geq 1 - \alpha$$

d'où le résultat. □

□

Application ((261, 266)). Soit $I = [0, 1]^d$ muni de la mesure de Lebesgue, soit f une fonction intégrable et bornée sur I .

Soit (Y_n) une suite de variable aléatoire iid de loi uniforme sur I . On a

$$\forall \varepsilon, \mathbb{P} \left(\left| \frac{1}{n} \sum_{k=1}^n f(Y_k) - \int_I f \right| > \varepsilon \right) \leq 2 \exp \left(-\frac{n\varepsilon^2}{8\|f\|_\infty^2} \right)$$

Preuve : Posons pour $n \in \mathbb{N}$, $X_n = f(Y_n) - \int_I f$.

On a $\mathbb{E}[X_n] = 0$ d'après la formule de transfert et $|X_n| \leq 2\|f\|_\infty$ donc d'après l'inégalité de Hoeffding avec $c_n = 2\|f\|_\infty$.

Pour tout $\varepsilon > 0$,

$$\begin{aligned} \mathbb{P} \left(\left| \frac{1}{n} \sum_{k=1}^n f(Y_k) - \int_I f \right| > \varepsilon \right) &= \mathbb{P} \left(\left| \sum_{k=1}^n X_k \right| \geq n\varepsilon \right) \\ &\leq 2 \exp \left(\frac{n^2 \varepsilon^2}{2 \sum_{k=1}^n 4\|f\|_\infty^2} \right) \\ &\leq 2 \exp \left(\frac{n\varepsilon^2}{8\|f\|_\infty^2} \right) \end{aligned}$$

□

Application ((262)). Soit $\alpha > 0$, s'il existe $\beta > 0$ tel que pour tout $n \in \mathbb{N}^*$, $\sum_{k=1}^n c_k^2 \leq n^{2\alpha-\beta}$,

alors

$$\frac{S_n}{n^\alpha} \xrightarrow[n \rightarrow +\infty]{\text{p.s.}} 0$$

Preuve : Soit $\varepsilon > 0$, par inégalité de Hoeffding, on a

$$\mathbb{P}(|S_n| > n^\alpha \varepsilon) \leq 2 \exp\left(-\frac{n^{2\alpha} \varepsilon^2}{2 \sum_{k=1}^n c_k^2}\right)$$

Or comme $\sum_{k=1}^n c_k^2 \leq n^{2\alpha-\beta}$, on a

$$\mathbb{P}(|S_n| > n^\alpha \varepsilon) \leq 2 \exp(-\varepsilon n^\beta)$$

Or, comme $\sum \exp(-\varepsilon n^\beta)$ converge, la série de terme général $\mathbb{P}(|S_n| > n^\alpha \varepsilon)$ converge. Donc d'après le lemme de Borel-Cantelli, on a $\mathbb{P}(\limsup_n [|S_n| > n^\alpha \varepsilon]) = 0$.

Or, comme \mathbb{Q}^{+*} est dénombrable, on a $\mathbb{P}\left(\bigcup_{s \in \mathbb{Q}^{+*}} \limsup_n [|S_n| > n^\alpha \varepsilon]\right) = 0$.

Donc en passant au complémentaire, on a

$$\mathbb{P}\left(\bigcap_{s \in \mathbb{Q}^{+*}} \liminf_n [|S_n| > n^\alpha \varepsilon]\right) = 1$$

Donc la suite $\left(\frac{S_n}{n}\right)$ converge presque sûrement vers 0. □

Méthode de Newton pour les polynômes

Geoffrey Deperle

Leçons associées :

- 223 : Suites numériques. Convergence, valeurs d'adhérence. Exemples et applications.
- 224 : Exemples de développements asymptotiques de suites et de fonctions.
- 226 : Suites vectorielles et réelles définies par une relation $u_{n+1} = f(u_n)$. Exemples. Applications à la résolution approchée d'équations.
- 228 : Continuité, dérivabilité des fonctions réelles d'une variable réelle. Exemples et applications.
- 230 : Séries de nombres réels ou complexes. Comportement des restes ou des sommes partielles des séries numériques. Exemples.

Le but de ce développement est de montrer le théorème suivant :

Théorème. Soit $\xi_1 < \xi_2 < \dots < \xi_r$ des réels, m_i des entiers non nuls et $P = \prod_{i=1}^r (X - \xi_i)^{m_i}$.

Considérons

$$\begin{cases} x_0 > \xi_r \\ \forall n \in \mathbb{N}, x_{n+1} = x_n - \frac{P(x_n)}{P'(x_n)} \end{cases}$$

La suite (x_n) est strictement décroissante et converge vers ξ_r .

- Si $m_r = 1$ alors $\forall c > 0, |x_n - \xi_r| = o_{n \rightarrow +\infty}(c^n)$ (convergence surlinéaire)
- Si $m_r > 1$ alors $\exists c \neq 0, |x_n - \xi_r| \sim_{n \rightarrow +\infty} c \left(1 - \frac{1}{m_r}\right)^n$ (convergence linéaire)

Preuve : La fonction $\frac{P'}{P}$ est la dérivée logarithmique de P , on a donc $\frac{P'}{P} = \sum_{i=1}^r \frac{m_i}{x_n - \xi_i}$. On a donc $\forall n \in \mathbb{N}, x_{n+1} = x_n - \left(\sum_{i=1}^r \frac{m_i}{x_n - \xi_i}\right)^{-1}$ donc si $x_n > \xi_r$, alors $x_{n+1} < x_n$.

Étape 1 : Montrons la convergence de la suite (x_n)

D'après la remarque préliminaire, (x_n) est décroissante. Montrons qu'elle est minorée par ξ_r .

On a déjà $x_0 > \xi_r$.

Supposons que pour un $n \in \mathbb{N}, x_n > \xi_r$, montrons que $x_{n+1} > \xi_r$.

Soit $f : x \mapsto x - \frac{P(x)}{P'(x)}$, f se prolonge par continuité sur $[\xi_r, +\infty[$ en posant $f(\xi_r) = \xi_r$.

On a $\forall x \in]\xi_r, +\infty[, f'(x) = \frac{P(x)P''(x)}{P'(x)^2}$, D'après le théorème de Rolle (ou de Gauss-Lucas), les zéros de P' sont dans $[\xi_1, \xi_r]$, de même pour P'' donc P, P' et P'' sont strictement positives sur $]\xi_r, +\infty[$ donc

$f' > 0$ et f est croissante sur cet intervalle.

Comme $x_n > \xi_r$, on a par croissance, $\xi_r = f(\xi_r) < f(x_n) = x_{n+1}$.

Ainsi, par récurrence, on a $\forall n \in \mathbb{N}, x_n > \xi_r$.

(x_n) est décroissante, minorée par ξ_r donc converge vers un réel où $\frac{P}{P'}$ s'annule donc vers ξ_r .

Étape 2 : Déterminons la vitesse de convergence

On a $\frac{P'(x)}{P(x)} = \sum_{i=1}^r \frac{m_i}{x - \xi_i}$ donc en dérivant, on a

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

Donc

$$f'(x) = \frac{P(x)P''(x)}{P'(x)^2} = 1 - \underbrace{\left(\sum_{i=1}^r \frac{m_i}{x - \xi_i} \right)^{-2}}_{\underset{x \rightarrow \xi_r}{\sim} \frac{(x - \xi_r)^2}{m_r^2}} \underbrace{\left(\sum_{i=1}^r \frac{m_i}{(x - \xi_i)^2} \right)}_{\underset{x \rightarrow \xi_r}{\sim} \frac{m_r}{(x - \xi_r)^2}}$$

Donc $\lim_{x \rightarrow \xi_r} f'(x) = 1 - \frac{1}{m_r}$.

Deux cas de figure se présentent alors,

Supposons $m_r = 1$

On a $f'(\xi_r) = 0$, d'après l'égalité des accroissements finis,

$$\exists y_n \in]\xi_r, x_n[/ x_{n+1} - \xi_r = f(x_n) - f(\xi_r) = (x_n - \xi_r)f'(y_n)$$

Soit $c > 0$, comme $x_n \xrightarrow[n \rightarrow +\infty]{} \xi_r$, il existe $n_0 \in \mathbb{N}$ tel que $\forall n \geq n_0, |f'(y_n)| \leq c$.

Pour $n \geq n_0$, $|x_{n+1} - \xi_r| \leq c|x_n - \xi_r|$ d'où par récurrence, et donc par récurrence, pour $n \geq n_0$, $|x_n - \xi_r| \leq c^{n-n_0}|x_{n_0} - \xi_r| = O(c^n)$.

En prenant $c' < c$, on a $x_n - \xi_r = o_{n \rightarrow +\infty}(c^n)$ pour tout $c > 0$.

Supposons $m_r > 1$

On a alors $f'(\xi_r) = 1 - \frac{1}{m_r}$ et de même,

$$\exists y_n \in]\xi_r, x_n[/ x_{n+1} - \xi_r = f(x_n) - f(\xi_r) = (x_n - \xi_r)f'(y_n)$$

Donc $(\ln(x_{n+1} - \xi_r) - \ln(x_n - \xi_r))$ converge vers $\ln f'(\xi_r) \neq 0$ donc par sommation des relations de comparaison dans le cas divergent (ou théorème de Césaro), on a

$$\ln(x_n - \xi_r) \underset{n \rightarrow +\infty}{\sim} n \ln f'(\xi_r)$$

Précisons le développement asymptotique en montrant que la suite $(\ln(x_n - \xi_r) - n \ln f'(\xi_r))$ converge. Par Taylor-Lagrange, il existe $z_n \in]\xi_r, x_n[$ tel que

$$x_{n+1} - \xi_r = f'(\xi_r)(x_n - \xi_r) + \frac{f''(z_n)}{2}(x_n - \xi_r)^2$$

d'où $\varepsilon_n = \frac{x_{n+1} - \xi_r}{f'(\xi_r)(x_n - \xi_r)} - 1 = O_{n \rightarrow +\infty}(x_n - \xi_r)$.

Comme $\ln(x_n - \xi_r) \sim n \ln f'(\xi_r)$,

Il existe une suite (α_n) tel que $\alpha_n \xrightarrow{n \rightarrow +\infty} 1$ et tel que $\ln(x_n - \xi_r) = n\alpha_n \ln f'(\xi_r)$ donc

$$|x_n - \xi_r| = e^{\alpha_n} f'(\xi_r)^n$$

donc en choisissant c dans l'intervalle $]f'(\xi_r), 1[$ on a $|x_n - \xi_r| = O_{n \rightarrow +\infty}(c^n)$ d'où

$$\ln(x_{n+1} - \xi_r) - \ln(x_n - \xi_r) - \ln f'(\xi_r) = \ln(1 + \varepsilon_n) = O_{n \rightarrow +\infty}(c^n)$$

et la série $\sum c^n$ converge donc par sommation des relations de comparaison, $(\ln(x_n - \xi_r) - n \ln f'(\xi_r))$ converge vers un réel λ et

$$x_n - \xi_r \sim e^\lambda f'(\xi_r)^n$$

□

Optimisation dans un Hilbert

Geoffrey Deperle

Leçons associées :

- 213 : Espaces de Hilbert. Bases hilbertiennes. Exemples et applications.
- 219 : Extremums : existence, caractérisation, recherche. Exemples et applications.
- 229 : Fonctions monotones. Fonctions convexes. Exemples et applications.
- 253 : Utilisation de la notion de convexité.

Le but de ce développement est de montrer le théorème suivant :

Théorème. Soit H un espace Hilbert et $J : H \rightarrow \mathbb{R}$ convexe, continue et coercive (ie telle que $J(x) \xrightarrow{\|x\| \rightarrow +\infty} +\infty$). Il existe α tel que $J(\alpha) = \inf_{x \in H} J(x)$.

Preuve : L'idée de la preuve est de montrer et exploiter la compacité faible de la boule unité dans un Hilbert.

Soit (x_k) une suite de H telle que $J(x_k) \xrightarrow{k \rightarrow +\infty} \inf_{x \in H} J(x)$.

Étape 1 : Montrons que la suite (x_k) est bornée.

Par l'absurde, si (x_k) est non bornée, il existe $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ strictement croissante tel que $\|x_{\varphi(k)}\| \xrightarrow{k \rightarrow +\infty} +\infty$. Par coercivité, on a $J(x_{\varphi(k)}) \xrightarrow{k \rightarrow +\infty} +\infty$ ce qui contredit la définition de (x_k) d'où il existe $C > 0$, tel que pour tout $k \in \mathbb{N}$, $\|x_k\| \leq C$.

Étape 2 : Montrons que l'on peut extraire de (x_k) une sous-suite faiblement convergente.

La suite $(\langle x_0, x_k \rangle)_{k \in \mathbb{N}}$ est une suite réelle et bornée par inégalité de Cauchy-Schwarz, donc par théorème de Bolzano-Weierstrass, il existe $\varphi_0 : \mathbb{N} \rightarrow \mathbb{N}$ strictement croissante telle que la suite $(\langle x_0, x_{\varphi_0(k)} \rangle)$ converge.

Par récurrence, pour $i \in \mathbb{N}$, supposons avoir construit $\varphi_0, \dots, \varphi_i : \mathbb{N} \rightarrow \mathbb{N}$ strictement croissante tel que $\forall p \in \llbracket 0, i \rrbracket, (\langle x_p, x_{\varphi_0 \circ \dots \circ \varphi_p(k)} \rangle)$ converge.

La suite $(\langle x_{i+1}, x_{\varphi_0 \circ \dots \circ \varphi_p(k)} \rangle)$ est bornée d'après l'inégalité de Cauchy-Schwarz donc il existe $\varphi_{i+1} : \mathbb{N} \rightarrow \mathbb{N}$ strictement croissante telle que $(\langle x_{i+1}, x_{\varphi_0 \circ \dots \circ \varphi_{i+1}(k)} \rangle)$.

On pose $\psi : \mathbb{N} \rightarrow \mathbb{N}$
 $k \mapsto \varphi_0 \circ \dots \circ \varphi_k(k)$ (procédé d'extraction diagonale) et $y_k = x_{\psi(k)}$.

On a pour tout $p \in \mathbb{N}$, $(\langle x_p, y_k \rangle)_{k \in \mathbb{N}}$ converge.

Considérons $F = \text{Vect}(x_p, p \in \mathbb{N})$,

On a pour tout $\tilde{v} \in F$, $(\langle \tilde{v}, y_k \rangle)$ converge.

Comme H est un espace de Hilbert, par théorème du supplémentaire orthogonal on a $H = \overline{F} \oplus F^\perp$. Montrons alors que pour tout $u \in H$, $(\langle u, y_k \rangle)$ converge.

Soit $u \in H$, $\varepsilon > 0$, décomposons u comme $u = v + w$ avec $v \in \overline{F}$ et $w \in F^\perp$. Il existe $\tilde{v} \in F$ tel que $\|v - \tilde{v}\| \leq \varepsilon$.

On a pour tout $k, l \in \mathbb{N}$,

$$\begin{aligned} |\langle u, y_k - y_l \rangle| &= |\langle v, y_k - y_l \rangle| \\ &\leq |\langle v - \tilde{v}, y_k - y_l \rangle| + |\langle \tilde{v}, y_k - y_l \rangle| \\ &\leq \underbrace{\|v - \tilde{v}\|}_{\leq \varepsilon} \underbrace{\|y_k - y_l\|}_{\leq 2C} + |\langle \tilde{v}, y_k - y_l \rangle| \end{aligned}$$

De plus, $(\langle \tilde{v}, y_k \rangle)$ converge donc est de Cauchy donc il existe $N \in \mathbb{N}$ tel que $|\langle \tilde{v}, y_k - y_l \rangle| \leq \varepsilon$ pour $k, l \geq N$, d'où $k, l \geq N$, $|\langle u, y_k - y_l \rangle| \leq 2C\varepsilon + \varepsilon = (2C + 1)\varepsilon$.

La suite $(\langle u, y_k \rangle)$ est donc de Cauchy dans \mathbb{R} complet donc converge.

Étape 3 : Construisons α avec le théorème de Riesz

On pose $f : H \rightarrow \mathbb{R}$
 $u \mapsto \lim_{k \rightarrow +\infty} \langle u, y_k \rangle$, f est linéaire et continue par inégalité de Cauchy-Schwarz.

D'après le théorème de représentation de Riesz,

$$\exists \alpha \in H, \forall u \in H, f(u) = \langle u, \alpha \rangle$$

Montrons que α convient,

Soit $\beta > \inf_{x \in H} J(x)$, soit $C_\beta = \{x \in H, J(x) \leq \beta\}$.

C_β est convexe (épigraphe d'une fonction convexe), fermé (en tant qu'image réciproque d'un fermé par une fonction continue), non vide.

Soit $p : H \rightarrow H$ l'opérateur de projection sur C_β .

Comme $J(y_k) \xrightarrow{k \rightarrow +\infty} \inf_{x \in H} J(x)$, $y_k \in C_\beta$ à partir d'un certain rang. D'où :

$$\exists N \in \mathbb{N}, \forall k \geq N, \langle y_k - p(\alpha), \alpha - p(\alpha) \rangle \leq 0$$

D'où pour $k \rightarrow +\infty$, $\|\alpha - p(\alpha)\|^2 \leq 0$ d'où $\alpha = p(\alpha)$ et $\alpha \in C_\beta$.

D'où $\forall \beta > \inf_{x \in H} J(x)$, $J(\alpha) \leq \beta$ donc $J(\alpha) = \inf_{x \in H} J(x)$. □

Prolongement de la fonction Gamma et formule de Weierstrass

Geoffrey Deperle

Leçons associées :

- 236 : Illustrer par des exemples quelques méthodes de calcul d'intégrales de fonctions d'une ou plusieurs variables.
- 239 : Fonctions définies par une intégrale dépendant d'un paramètre. Exemples et applications.
- 245 : Fonctions d'une variable complexe. Exemples et applications.
- 265 : Exemples d'études et d'applications de fonctions usuelles et spéciales.

Le but de ce développement est de montrer le théorème suivant :

Théorème. *La fonction $\Gamma : z \mapsto \int_0^{+\infty} t^{z-1} e^{-t} dt$ est holomorphe sur $\Omega_0 = \{\Re > 0\}$. Elle se prolonge méromorphiquement à \mathbb{C} avec des pôles simples aux entiers $-n$, $n \in \mathbb{N}$ avec comme résidu $\frac{(-1)^n}{n!}$.*

Preuve :

Étape 1 : Montrons que Γ est holomorphe sur Ω_0 .

Soit $K \subset \Omega_0$ un compact, il existe $0 < a \leq b$ tel que $\Re(K) \subset [a, b]$. On utilise le théorème d'holomorphicité sous le signe somme :

- $\forall z \in \Omega_0, t > 0 \mapsto t^{z-1} e^{-t}$ est continue.
- $\forall t > 0, z \in \Omega_0 \mapsto t^{z-1} e^{-t}$ est holomorphe sur K

$$\text{Si } t > 0, z \in K, \text{ alors } |t^{z-1} e^{-t}| = t^{\Re(z)-1} e^{-t} \leq \underbrace{\begin{cases} t^{a-1} e^{-t} & \text{si } t \leq 1 \\ t^{b-1} e^{-t} & \text{si } t \geq 1 \end{cases}}_{:=\varphi(t)}$$

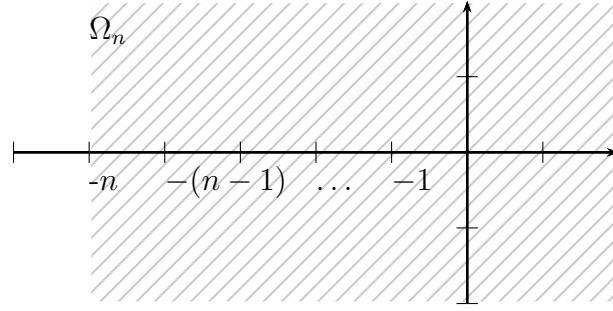
φ est intégrable sur $]0, +\infty[$ car $a > 0$ donc par théorème d'holomorphicité sous le signe somme, Γ est holomorphe sur K donc Γ est holomorphe sur Ω_0 .

Étape 2 : On prolonge Γ à $\mathbb{C} \setminus \mathbb{N}^-$

Pour $z \in \Omega_0$, on a par intégration par parties :

$$\Gamma(z+1) = \int_0^{+\infty} t^z e^{-t} dt = \left[-t^z e^{-t} \right]_0^{+\infty} + z \int_0^{+\infty} t^{z-1} e^{-t} dt = z\Gamma(z) \quad (*)$$

En notant pour $n \geq 1, \Omega_n = \{\Re > -n\} \setminus \{0, -1, \dots, -(n-1)\}$



Si $z \in \Omega_0$, par itération de (*), on a $\Gamma(z+n) = (z+n-1)\dots(z+1)\Gamma(z)$. D'où

$$\Gamma(z) = \frac{\Gamma(z+n)}{(z+n-1)\dots(z+1)z}$$

Le terme de droite définit une fonction holomorphe sur Ω_n . On définit Γ sur Ω_n par cette formule.

Si $m \geq n \geq 1$, alors les prolongements obtenues sur Ω_n coïncident par prolongement analytique (les deux valent Γ sur l'ouvert non vide Ω_0). En effectuant cela pour tout $n \geq 1$, on prolonge Γ sur tout $\mathbb{C} \setminus \mathbb{N}^-$ de façon holomorphe.

On a pour $n \geq 0$,

$$(z+n)\Gamma(z) = \frac{\Gamma(z+n+1)}{(z+n-1)\dots(z+1)} \xrightarrow{z \rightarrow -n} \frac{\Gamma(1)}{(-1)\dots(-n+1)(-n)} = \frac{(-1)^n}{n!}$$

Donc $-n$ est un pôle simple de Γ de résidu $\text{Res}_\Gamma(-n) = \frac{(-1)^n}{n!}$. □

Théorème. $\frac{1}{\Gamma}$ est une fonction entière vérifiant

$$\forall z \in \mathbb{C}, \frac{1}{\Gamma(z)} = ze^{\gamma z} \prod_{n=1}^{+\infty} \left(1 + \frac{z}{n}\right) e^{-\frac{z}{n}}$$

Preuve : Soit $x > 0$ réel, par convergence dominée,

$$\Gamma(x) = \lim_{N \rightarrow +\infty} \underbrace{\int_0^N t^{x-1} \left(1 - \frac{t}{N}\right)^N dt}_{:= I_N(x)}$$

Car on dispose de la domination $\left(1 - \frac{t}{N}\right)^N = \exp\left(N \ln\left(1 - \frac{t}{N}\right)\right) \leq \exp\left(N \frac{-t}{N}\right) = e^{-t}$.

Trouvons une autre expression de $I_N(x)$:

$$I_N(x) = \left[\frac{t^x}{x} \left(1 - \frac{t}{N}\right)^N \right]_0^N - \int_0^N \frac{t^x - N}{x} \frac{1}{N} \left(1 - \frac{t}{N}\right)^{N-1} dt = \frac{1}{x} \frac{N}{N} \int_0^N t^x \left(1 - \frac{t}{N}\right)^{N-1} dt$$

En réitérant on a

$$\begin{aligned} I_N(x) &= \frac{1}{x} \frac{N}{N} \frac{1}{x+1} \frac{N-1}{N} \int_0^N t^{x+1} \left(1 - \frac{t}{N}\right)^{N-1} dt \\ &\vdots \\ &= \frac{N(N-1)\dots(N-(N-1))}{N^N x(x+1)\dots(x+N-1)} \int_0^N t^{x+N-1} \left(1 - \frac{t}{N}\right)^0 dt \\ &= \frac{N!}{N^N x(x+1)\dots(x+N-1)} \frac{N^{x+N}}{x+N} \end{aligned}$$

$$\text{D'où } I_N(x) = \left(xN^{-x} \prod_{n=1}^N \left(1 + \frac{x}{n} \right) \right)^{-1}.$$

$$\text{D'où comme } \Gamma(x) > 0, \frac{1}{\Gamma(x)} = \lim_{N \rightarrow +\infty} \left(xN^{-x} \prod_{n=1}^N \left(1 + \frac{x}{n} \right) \right).$$

Or, $N^{-x} = \exp(-x \ln(N)) = \exp(-xH_N) \exp(x(H_N - \ln(N)))$ où H_N est la somme partielle de la série harmonique, comme $H_N - \ln(N) \xrightarrow{N \rightarrow +\infty} \gamma$, on a

$$\frac{1}{\Gamma(x)} = x e^{\gamma x} \prod_{n=1}^{+\infty} \left(1 + \frac{x}{n} \right) e^{-\frac{x}{n}}$$

Or, la fonction $z \mapsto z e^{\gamma z} \prod_{n=1}^{+\infty} \left(1 + \frac{z}{n} \right) e^{-\frac{z}{n}}$ est une fonction entière d'après le critère d'holomorphicité d'un produit de fonctions holomorphes.

En effet, pour $R > 0$ et $|z| < R$,

$$\left(1 + \frac{z}{n} \right) e^{-\frac{z}{n}} = \left(1 + \frac{z}{n} \right) \left(1 - \frac{z}{n} + O\left(\frac{1}{n^2}\right) \right) = 1 + O\left(\frac{1}{n^2}\right)$$

Comme les deux fonctions γ et $z \mapsto z e^{\gamma z} \prod_{n=1}^{+\infty} \left(1 + \frac{z}{n} \right) e^{-\frac{z}{n}}$ coïncident sur $]0, +\infty[$, elles coïncident sur \mathbb{C} . □

Remarque 5. En connaissant les zéros d'un tel produit, on obtient les zéros de $\frac{1}{\Gamma}$: ce sont les $-n$ avec $n \geq 0$, on retrouve ainsi les pôles de la fonction Γ .

Représentation des fonctions lipschitziennes

Geoffrey Deperle

Leçons associées :

- 201 : Espaces de fonctions. Exemples et applications.
- 205 : Espaces complets. Exemples et applications.
- 208 : Espaces vectoriels normés, applications linéaires continues. Exemples.
- 228 : Continuité, dérivabilité des fonctions réelles d'une variable réelle. Exemples et applications.
- 234 : Fonctions et espaces de fonctions Lebesgue-intégrables.

Le but de ce développement est de montrer le théorème suivant :

Théorème. Une application $f : \mathbb{R} \rightarrow \mathbb{R}$ est lipschitzienne si et seulement s'il existe une fonction $g \in L^\infty(\mathbb{R})$ telle que

$$\forall x, y \in \mathbb{R}, f(y) - f(x) = \int_x^y g(t) dt$$

Preuve : Le sens réciproque est immédiat, montrons le sens direct. On note $\mathcal{D}(\mathbb{R}) = \mathcal{C}_c^\infty(\mathbb{R})$ et on considère la dérivée distributionnelle T de f :

$$\begin{array}{ccc} T : \mathcal{D}(\mathbb{R}) & \rightarrow & \mathbb{R} \\ \phi & \mapsto & \langle f', \phi \rangle = - \int_{\mathbb{R}} f(x) \phi'(x) dx \end{array}$$

Étape 1 : On prolonge T sur L^1

Montrons que T est une forme linéaire continue sur $(\mathcal{D}(\mathbb{R}), \|\cdot\|_1)$, pour cela, montrons que pour $\phi \in \mathcal{D}(\mathbb{R})$,

$$\langle T, \phi \rangle = \lim_{h \rightarrow 0} \int_{\mathbb{R}} f(x) \frac{\phi(x+h) - \phi(x)}{h} dx$$

Soit $M > 0$ tel que $|x| > M \implies \phi(x) = 0$. On a :

(i) $\forall x \in \mathbb{R}, f(x) \frac{\phi(x+h) - \phi(x)}{h} \xrightarrow{h \rightarrow 0} f(x) \phi'(x)$

(ii) Par inégalité des accroissements finis,

$$\forall x \in \mathbb{R}, \forall |h| < 1, \left| f(x) \frac{\phi(x+h) - \phi(x)}{h} \right| \leq |f(x)| \|\phi'\|_\infty \mathbb{1}_{[-M-1, M+1]}(x) \in L^1(\mathbb{R})$$

D'où le résultat par théorème de convergence dominée. On a alors par linéarité et changement de variable,

$$\forall \phi \in \mathcal{D}(\mathbb{R}), \langle T, \phi \rangle = \int_{\mathbb{R}} \frac{f(x-h) - f(x)}{h} \phi(x) dx$$

Soit L une constante de Lipschitz de f , on a alors

$$\forall \phi \in \mathcal{D}(\mathbb{R}), |\langle T, \phi \rangle| \leq L \|\phi\|_1$$

Par théorème de prolongement des applications uniformément continues sur une partie dense, T admet un unique prolongement toujours noté T en une forme linéaire continue sur $(L^1(\mathbb{R}), \|\cdot\|_1)$ i.e. un élément de $L^1(\mathbb{R})'$ avec $\|T\|_1 \leq L$.

Étape 2 : On construit g grâce au théorème de Riesz

Soit $n \geq 1$, on dispose des injections suivantes :

$$L^2(-n, n) \hookrightarrow L^1(-n, n) \hookrightarrow L^1(\mathbb{R})$$

La première injection est continue par théorème de Cauchy-Schwarz et le second prolongement s'effectue en posant $\phi = 0$ sur $[-n, n]^C$. Notons $\tilde{\phi}$ un tel prolongement.

$$\begin{array}{l} \text{Posons} \\ T_n : L^2(-n, n) \rightarrow \mathbb{R} \\ \phi \mapsto \langle T, \tilde{\phi} \rangle = - \int_{\mathbb{R}} f(x) \phi'(x) dx \end{array}$$

D'après le théorème de Riesz, il existe un unique $g_n \in L^2(-n, n)$ telle que

$$\forall \phi \in L^2(-n, n), \langle T, \tilde{\phi} \rangle = \int_{\mathbb{R}} g_n(x) \phi(x)$$

Si $k \geq n$, par unicité du théorème de Riesz, on a $g_k = g_n$ presque partout sur $[-n, n]$. Posons alors $g = \liminf g_n$ mesurable, on a $\forall n \in \mathbb{N}, g_{[-n, n]} = g_n$.

Montrons que $g \in L^\infty(\mathbb{R})$,

Par l'absurde, si $A = \{x \in \mathbb{R}, |g(x)| > L\}$ n'est pas négligeable, comme $A = \bigcup_{n \in \mathbb{N}} (A \cap [-n, n])$, il

existe $N \in \mathbb{N}$ tel que $\lambda(A_N) > 0$.

En posant $u = \text{signe}(g) \in \{-1, 1\}$ afin d'avoir $|g| = ug$. Posons $\phi = u \mathbb{1}_{A_N} \in L^2(-n, n)$ et

$$\langle T, \phi \rangle = \int_{-N}^N g(x) u(x) \mathbb{1}_{A_N}(x) dx = \int_{A_N} |g(x)| dx > L \lambda(A_N) = L \|\phi\|_1$$

ce qui contredit $\|T\|_1 \leq L$. D'où $T = f' = g \in L^\infty(\mathbb{R})$.

Étape 3 : Conclusion

$$\text{Soit } G : \mathbb{R} \rightarrow \mathbb{R} \text{ qui est continue par théorème de convergence dominée.} \\ x \mapsto \int_0^x g(t) dt$$

On a d'après le théorème de Fubini, $G' = g$ au sens des distributions (*).

D'où $\langle G', \phi \rangle = \int_{\mathbb{R}} g(t) \phi(t) dt = \langle T, \phi \rangle$ donc $G' = f'$.

Donc il existe une constante $c \in \mathbb{R}$, tel que $f - G = c$ au sens des distributions (**). L'injection $L^1_{\text{loc}}(\mathbb{R})$ dans $\mathcal{D}'(\mathbb{R})$ assure que pour presque tout x , $f(x) - G(x) = c$. Comme de plus, les applications sont continues, le résultat est vraie pour tout $x \in \mathbb{R}$, d'où

$$f(y) - f(x) = G(y) - G(x) = \int_x^y g(t) dt$$

□

Annexe

Lemme 12 (*). Soit $G : \mathbb{R} \rightarrow \mathbb{R}$
 $x \mapsto \int_0^x g(t) dt$, on a $G' = g$ au sens des distributions .

Preuve : Pour $\phi \in \mathcal{D}(\mathbb{R})$,

$$\langle G', \phi \rangle = - \int_{\mathbb{R}} G(x) \phi'(x) dx = \int_{-\infty}^0 \int_x^0 \phi'(x) g(t) dt dx - \int_0^{+\infty} \int_0^x \phi'(x) g(t) dt dx$$

Soit M tel que $\phi(x) = 0$ si $|x| > M$.

Pour presque tout (t, x) on a $|g(t)\phi'(x)| \mathbf{1}_{x \leq t \leq 0} \leq \|g\|_{\infty} \|\phi'\|_{\infty} \mathbf{1}_{-M \leq x \leq t \leq 0} \in L^1(\mathbb{R}^- \times \mathbb{R}^-)$. Donc par théorème de Fubini-Lebesgue

$$\begin{aligned} \langle G', \phi \rangle &= \int_{-\infty}^0 \int_{-\infty}^t g(t) \phi'(x) dx dt - \int_0^{+\infty} \int_t^{+\infty} g(t) \phi'(x) dx dt \\ &= \int_{\mathbb{R}} g(t) \phi(t) dt \end{aligned}$$

□

Lemme 13 ()**. Soit T une distribution telle que $T' = 0$, alors T est constant.

Preuve : Les éléments de $\mathcal{D}(\mathbb{R})$ d'intégrale nulle sont exactement les dérivées des fonctions tests :

En effet, si ψ est la dérivée d'une fonction test ϕ alors $\int \psi = 0$ car $\text{Supp}(\phi)$ borné.

Réciproquement, soit ψ d'intégrale nulle, alors $\varphi(x) = \int_{-\infty}^x \psi(t) dt$, φ est de classe C^∞ (car $\text{Supp}(\psi)$ est bornée car $\int_{-\infty}^{+\infty} \psi(x) dx$) et convient.

Notons E l'ensemble des éléments de $\mathcal{D}(\mathbb{R})$ d'intégrale nulle,

Soit $\theta \in \mathcal{D}(\mathbb{R})$ telle que $\int_{\mathbb{R}} \theta = 1$.

Pour $\varphi \in \mathcal{D}(\mathbb{R})$, on écrit

$$\varphi = \psi + \left(\int_{\mathbb{R}} \phi(x) dx \right) \theta \quad \text{avec } \psi \in E$$

$$\langle T, \varphi \rangle = \langle T, \psi \rangle + \left(\int_{\mathbb{R}} \varphi \right) \langle T, \theta \rangle = -\langle T', \int \psi \rangle + \left(\int_{\mathbb{R}} \varphi \right) \langle T, \theta \rangle$$

Donc en posant $C = \langle T, \theta \rangle$, on a

$$\langle T, \varphi \rangle = C \int_{\mathbb{R}} \varphi(x) dx = \langle C, \varphi \rangle$$

Donc $T = C$ au sens des distributions.

□

Résolution de $-u'' + u = f$ sur le cercle

Geoffrey Deperle

Leçons associées :

- 201 : Espaces de fonctions. Exemples et applications.
- 220 : Équations différentielles ordinaires. Exemples de résolution et d'études de solutions en dimension 1 et 2.
- 221 : Équations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications.
- 246 : Séries de Fourier. Exemples et applications.

Le but de ce développement est de montrer le théorème suivant :

Théorème. Notons $H^1(T)$ l'ensemble des fonctions de $L^2((0, 2\pi))$ 2π -périodique de dérivée appartenant à $L^2((0, 2\pi))$. Soit $f \in H^1(T)$, une fonction $u \in H^1(T)$ est solution faible de

$$\begin{cases} -u'' + u = f & (*) \\ u(0) = u(2\pi) \end{cases}$$

(c'est-à-dire une fonction $u \in H^1(T)$ vérifie $\forall \phi \in H^1(T)$, $\int_0^{2\pi} u' \phi' + u \phi = \int_0^{2\pi} f \phi$) si et seulement si u est de la forme $u = e \star f$ avec $\forall x \in [0, 2\pi]$, $e(x) = \frac{1}{2}e^{-|x|} + \frac{1}{e^{2\pi} - 1} \text{ch}(x)$

Preuve :

Étape 1 : Montrons que $u \in H^1(T)$ est solution faible de (*) si et seulement si $u = K \star f$ où K est une fonction à déterminer.

Analyse :

Soit u une solution faible de (*), On a

$$\forall \phi \in H^1(T), \int_0^{2\pi} u' \phi' + u \phi = \int_0^{2\pi} f \phi \text{ d'où } \int_0^{2\pi} u' \overline{\phi'} + u \overline{\phi} = \int_0^{2\pi} f \overline{\phi}$$

Comme les fonctions considérées sont dans $L^2((0, 2\pi))$ d'après la formule de Parseval on a :

$$\sum_{n \in \mathbb{Z}} \underbrace{c_n(u')}_{=inc_n(u)} \overline{\underbrace{c_n(\phi')}_{=inc_n(\phi)}} + c_n(u) \overline{c_n(\phi)} = \sum_{n \in \mathbb{Z}} c_n(f) \overline{c_n(\phi)}$$

car $\forall n \in \mathbb{Z}, c_n(u') = inc_n(u)$.

D'où $\sum_{n \in \mathbb{Z}} \left[(1+n^2)c_n(u) - c_n(f) \right] \overline{c_n(\phi)} = 0$.

Comme l'égalité est vraie pour tout $\phi \in H^1(T)$, avec $\phi_n : x \mapsto e^{inx}$, on a $\forall n \in \mathbb{Z}, c_n(u) = \frac{c_n(f)}{1+n^2}$

d'où u est déterminée par $u = \sum_{n \in \mathbb{Z}} \frac{c_n(f)}{1+n^2} e_n$ (limite L^2 de la suite des sommes partielles).

Synthèse :

La fonction $u : x \mapsto \sum_{n \in \mathbb{Z}} \frac{c_n(f)}{1+n^2} e^{inx}$ est bien définie car $\frac{|c_n(f)|}{1+n^2} \leq \frac{\|f\|_2}{1+n^2}$ et $f \in L^2((0, 2\pi))$ d'où $\sum_{n \in \mathbb{Z}} \frac{|c_n(f)|}{1+n^2} < +\infty$ donc u est bien définie et est continue (comme limite uniforme d'une suite de fonctions continues).

De plus,

$$\sum_{n \in \mathbb{Z}} \frac{|inc_n(f)|}{1+n^2} \leq \underbrace{\left(\sum_{n \in \mathbb{Z}} \left(\frac{n}{1+n^2} \right)^2 \right)^{\frac{1}{2}}}_{:=C} \left(\sum_{n \in \mathbb{Z}} c_n(f)^2 \right)^{\frac{1}{2}} \leq C \|f\|_2$$

donc u est de classe C^1 et $u \in H^1(T)$.

Ainsi, u est solution de (*) si et seulement si u est de la forme $u = K \star f$ avec $K : x \mapsto \frac{1}{2\pi} \sum_{n \in \mathbb{Z}} \frac{e^{inx}}{1+n^2}$.

Étape 2 : Cherchons une expression explicite de K en résolvant l'équation au sens des distributions

Chercher les solutions faibles d'une équation différentielles revient à chercher les solutions au sens des distributions. Cherchons alors à résoudre l'équation $-T'' + T = T_f$ au sens des distributions. Soit e une solution élémentaire, c'est-à-dire une solution au sens des distributions de l'équation $-T'' + T = \delta_0$.

Sur \mathbb{R}^{+*} et sur \mathbb{R}^{-*} , on a $-e'' + e = 0$ donc

$$\exists \alpha, \beta, \lambda, \mu \in \mathbb{R}, \forall x \in \mathbb{R}, e(x) = \begin{cases} \alpha e^x + \beta e^{-x} & \text{si } x \in \mathbb{R}^{+*} \\ \lambda e^x + \mu e^{-x} & \text{si } x \in \mathbb{R}^{-*} \end{cases}$$

Or, d'après la formule des sauts, on a

$$\begin{aligned} e'' &= \{e''\} + (e(0^+) - e(0^-))\delta'_0 + (e'(0^+) - e'(0^-))\delta_0 \\ &= -e + (\alpha + \beta - \lambda - \mu)\delta'_0 + (\alpha - \beta - \lambda + \mu)\delta_0 \end{aligned}$$

d'où on doit avoir

$$\begin{cases} \alpha + \beta - \lambda - \mu = 0 \\ \alpha - \beta + \lambda + \mu = 1 \end{cases} \iff \begin{cases} \alpha - \lambda = -\frac{1}{2} \\ \beta - \mu = \frac{1}{2} \end{cases} \iff \begin{cases} \lambda = \alpha + \frac{1}{2} \\ \beta = \mu + \frac{1}{2} \end{cases}$$

donc $e(x) = \begin{cases} \alpha e^x + \mu e^{-x} + \frac{1}{2} e^{-x} & \text{si } x \in \mathbb{R}^+ \\ \alpha e^x + \mu e^{-x} + \frac{1}{2} e^x & \text{si } x \in \mathbb{R}^- \end{cases}$ d'où $e(x) = \frac{1}{2} e^{-|x|} + \alpha e^x + \mu e^{-x}$.

Par changement de variable, on peut ré-écrire $e(x)$ sous la forme $e(x) = \frac{1}{2} e^{-|x|} + a \cosh(x) + b \sinh(x)$.

Ainsi e est une fonction continue (et non plus seulement une distribution).

Comme e est une solution élémentaire, on a $\forall f \in \mathcal{C}^0((0, 2\pi))$, $e \star f$ est solution de $-T'' + T = T_f$ au sens des distributions donc est solution faible de l'équation $-u'' + u = f$.

Étape 3 : Conclusion

Montrons que $e \star f \in H^1(T)$,

— $e \star f$ est 2π -périodique car f l'est.

— $\|e \star f\|_2 \leq \|e\|_1 \|f\|_2 < +\infty$ car $e \in \mathcal{C}^0((0, 2\pi))$.

— $\|(e \star f)'\|_2 = \|e \star f'\|_2 \leq \|e\|_1 \|f'\|_2 < +\infty$ car $f \in H^1(T)$.

donc $e \star f \in H^1(T)$, d'après ce qui précède, $c_n(e \star f) = c_n(K \star f)$ et par injectivité des coefficients de Fourier, on a $e \star f = K \star f$.

Comme l'égalité est vrai pour tout $f \in H^1(T)$, on a $e = K$ (il suffit de tester l'égalité sur des fonctions tests)

Ainsi, pour tout $x \in \mathbb{R}$, $e(x) = \frac{1}{2}e^{-|x|} + a \cosh(x) = K(x)$ donc e est une fonction paire (car K l'est), donc $b = 0$ d'où $e(x)$ est de la forme $\frac{1}{2}e^{-|x|} + a \cosh(x)$.

De plus, comme $e(0) = e(2\pi)$, on a $\frac{1}{2} + a = \frac{1}{2}e^{-2\pi} + a \cosh(2\pi)$ d'où $a = \frac{\frac{1}{2}e^{-2\pi} - \frac{1}{2}}{\cosh(2\pi) - 1} = \frac{1}{e^{2\pi} - 1}$. \square

Théorème de Hadamard-Lévy (cas C^2)

Geoffrey Deperle

Leçons associées :

- 204 : Connexité. Exemples et applications.
- 214 : Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications en analyse et en géométrie.
- 215 : Applications différentiables définies sur un ouvert de \mathbb{R}^n . Exemples et applications.
- 220 : Équations différentielles ordinaires. Exemples de résolution et d'études de solutions en dimension 1 et 2.

Le but de ce développement est de montrer le théorème suivant :

Théorème. *Soit $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$ une application C^2 . Les assertions suivantes sont équivalentes :*

1. *f est un C^1 -difféomorphisme de \mathbb{R}^n sur \mathbb{R}^n*
2. *f est propre et $df(x)$ est inversible pour tout $x \in \mathbb{R}^n$.*

Preuve : Si f est un C^1 -difféomorphisme de \mathbb{R}^n sur \mathbb{R}^n alors f est propre car f^{-1} est continue (donc pour tout compact K , $f^{-1}(K)$ est compact) et $f^{-1} \circ f = \text{id}$ d'où

$$\forall x \in \mathbb{R}^n \quad df^{-1}(f(x)) \circ df(x) = \text{id}$$

donc $df(x)$ est inversible.

Passons au sens réciproque, supposons f est propre et $df(x)$ inversible pour tout $x \in \mathbb{R}^n$. Montrons que f est bijective. Quitte à considérer $x \mapsto f(x) - a$ pour $a \in \mathbb{R}^n$ il suffit de montrer que l'ensemble $S := f^{-1}(\{0\})$ est de cardinal 1.

Étape 1 : Cherchons un flot sur lequel f décroît vers 0

Soit

$$\begin{aligned} F &: \mathbb{R}^n \rightarrow \mathbb{R}^n \\ x &\mapsto -df(x)^{-1} \cdot f(x) \end{aligned}$$

F est de classe C^1 car $f \in C^2(\mathbb{R}^n, \mathbb{R}^n)$.

Le problème de Cauchy $\begin{cases} y' = F(y) \\ y(0) = x \in \mathbb{R}^n \end{cases}$ admet donc une unique solution maximale noté $\varphi^t(x)$ sur un intervalle de la forme $]T_-, T_+[$ contenant 0 d'après le théorème de Cauchy-Lipschitz,

Posons

$$\begin{aligned} g &: [0, T_+[\rightarrow \mathbb{R}^n \\ t &\mapsto f \circ \varphi^t(x) \end{aligned}$$

g est de classe C^1 et

$$\begin{aligned}\forall t \in [0, T_+[, g'(t) &= df(\varphi^t(x)) \cdot \partial_t \varphi^t(x) \\ &= df(\varphi^t(x)) \cdot [(-df(\varphi^t(x)))^{-1} \cdot f(\varphi^t(x))] \\ &= -g(t)\end{aligned}$$

d'où comme $g(0) = f(x)$, on a

$$\forall t \in [0, T_+[, f(\varphi^t(x)) = e^{-t} f(x)$$

Donc $\varphi^t(x) \in f^{-1}(\overline{B}(0, \|f(x)\|))$ compact car f est une application propre.

D'après le lemme de sortie de tout compact, φ est une solution globale donc $T_+ = +\infty$.

Remarque 6. On observe que S est l'ensemble des points d'équilibre du système différentiel autonome. Montrons dans les étapes 2 et 3 que les points d'équilibres sont asymptotiquement stables.

Étape 2 : Montrons que pour tout $x \in \mathbb{R}^n$, il existe $y \in S$ et \mathcal{U}_y un voisinage de y dans \mathbb{R}^n et $t_0 \in \mathbb{R}$ tel que $\varphi^{t_0}(x) \in \mathcal{U}_y$

La suite $(\varphi^k(x))_{k \in \mathbb{N}}$ est à valeurs dans le compact $f^{-1}(\overline{B}(0, \|f(x)\|))$ donc admet une valeur d'adhérence : il existe une sous-suite (n_k) et $y \in \mathbb{R}^n$ tels que $\varphi^{n_k}(x) \xrightarrow[k \rightarrow +\infty]{} y$ avec

$$f(y) = \lim_{k \rightarrow +\infty} f(\varphi^{n_k}(x)) = \lim_{k \rightarrow +\infty} e^{-n_k} f(x) = 0$$

donc $y \in S$.

Remarque 7. On a $\#S \geq 1$ et f est surjective.

Soit \mathcal{U}_y un voisinage de y dans \mathbb{R}^n et $B_y = B(0, \delta_y)$ tel que f soit un C^1 -difféomorphisme de \mathcal{U}_y sur B_y . D'après ce qui précède, il existe $t_0 > 0$ tel que $\varphi^{t_0}(x) \in \mathcal{U}_y$.

Étape 3 : Montrons qu'alors $\forall t \geq t_0, \varphi^t(x) \in \mathcal{U}_y$

On a

$$\underbrace{\{t \in [t_0, +\infty[, \varphi^t(x) \in \mathcal{U}_y\}}_{\substack{= \varphi^{t_0}(x)^{-1}(\mathcal{U}_y) \cap [t_0, +\infty[\\ \text{ouvert de } [t_0, +\infty[}} = \underbrace{\{t \in [t_0, +\infty[, \varphi^t(x) = f|_{\mathcal{U}_y}^{-1}(e^{-t} f(x))\}}_{\text{fermé de } [t_0, +\infty[}$$

En effet,

(\supset) par définition.

(\subset) $f(\varphi^{t_0}(x)) = e^{-t_0} f(x) \in B_y$ et la norme décroît lorsque t croît et en appliquant $f|_{\mathcal{U}_y}^{-1}$ et on obtient l'inclusion.

Par connexité, on a donc $\{t \in [t_0, +\infty[, \varphi^t(x) \in \mathcal{U}_y\} = [t_0, +\infty[$ donc pour tout $t \geq t_0, \varphi^t(x) \in \mathcal{U}_y$ et $\varphi^t(x) = f|_{\mathcal{U}_y}^{-1}(\underbrace{e^{-t} f(x)}_{\xrightarrow[t \rightarrow +\infty]{} 0})$ donc $\varphi^t(x) \xrightarrow[t \rightarrow +\infty]{} y$.

Étape 4 : On conclut par un argument de connexité

Soit $W_y = \{x \in \mathbb{R}^n, \varphi^t(x) \xrightarrow[t \rightarrow +\infty]{} y\}$.

On a d'après précédemment, $\mathbb{R}^n = \bigcup_{y \in f^{-1}(\{0\})} W_y$.

Or, $W_y = \bigcup_{t \in \mathbb{R}} (\varphi^t)^{-1}(\mathcal{U}_y)$,

En effet,

(\subset) Si $x \in W_y$, $\varphi^t(x) \xrightarrow[t \rightarrow +\infty]{} y$ donc $\exists t \in \mathbb{R}$, $\varphi^t(x) \in \mathcal{U}_y$, $x \in (\varphi^t)^{-1}(\mathcal{U}_y)$.

(\supset) S'il existe $t_0 \in \mathbb{R}$ tel que $\varphi^{t_0}(x) \in \mathcal{U}_y$, on a d'après ce qui précède $\varphi^t(x) \xrightarrow[t \rightarrow +\infty]{} 0$. D'où W_y est ouvert en tant qu'union quelconque d'ouverts (par continuité de $x \mapsto \varphi^t(x)$) comme les W_y sont disjoints, par connexité de \mathbb{R}^n , on a $\#S = 1$ donc f est bijective. \square

Théorème de Korovkin et applications

Geoffrey Deperle

Leçons associées :

- 206 : Exemples d'utilisation de la notion de dimension finie en analyse.
- 209 : Approximation d'une fonction par des fonctions régulières. Exemples et applications.
- 241 : Suites et séries de fonctions. Exemples et contre-exemples.

Définition 1. Soit $E = \mathcal{C}([0, 1], \mathbb{R})$, on dit qu'un opérateur $u \in \mathcal{L}(E)$ est positif si pour tout $f \in E$, $f \geq 0 \implies u(f) \geq 0$

Le but de ce développement est de montrer le théorème suivant :

Théorème. En notant pour $k \in \mathbb{N}$, e_k l'application : $e_k : x \mapsto x^k$. Pour toute suite d'opérateurs $(u_n)_{n \in \mathbb{N}} \in \mathcal{L}(E)^{\mathbb{N}}$ positifs tel que la suite $(u_n(e_k))_{n \in \mathbb{N}}$ converge uniformément vers e_k sur $[0, 1]$ pour $k \in \{0, 1, 2\}$ alors pour toute fonction $f \in E$, la suite $(u_n(f))_{n \in \mathbb{N}}$ converge uniformément vers f .

Preuve : Commençons par une remarque préliminaire sur les opérateurs positifs, Soit u un opérateur positif et $f, g \in E$ et tel que $f \leq g$ alors $g - f \geq 0$ donc $u(g - f) \geq 0$ par positivité de u et donc $u(g) \geq u(f)$ par linéarité de u .

Ainsi, comme pour tout $f \in E$, on a $-|f| \leq f \leq |f|$, on a $|u(f)| \leq u(|f|)$.

Passons maintenant à un lemme,

Lemme 14. Soit $f \in E$, pour tout $\varepsilon > 0$, il existe une constante $c > 0$ tel que pour tout $x, y \in [0, 1]$,

$$|f(x) - f(y)| \leq \varepsilon + c(y - x)^2$$

Preuve du lemme : Comme f est continue sur le compact $[0, 1]$, f est uniformément continue d'après le théorème de Heine.

Il existe $\eta > 0$ tel que

$$\forall x, y \in [0, 1], |x - y| \leq \eta \implies |f(x) - f(y)| \leq \varepsilon$$

Ainsi, pour $x, y \in [0, 1]$, si $|x - y| \leq \eta$, tout c positif convient.

Si $|x - y| \geq \eta$, alors $\frac{(x-y)^2}{\eta^2} \geq 1$ et

$$|f(x) - f(y)| \leq 2\|f\|_{\infty} \leq \frac{2\|f\|_{\infty}}{\eta^2}(y - x)^2$$

donc $\forall x, y \in [0, 1], |f(x) - f(y)| \leq \varepsilon + \frac{2\|f\|_\infty}{\eta^2}(y - x)^2$ □

Soit $\varepsilon > 0$, et $n \in \mathbb{N}$

Étape 1 : Étudions la quantité $|u_n(f)(x) - f(x)|$ à $x \in \mathbb{R}$ fixé

Soit $x \in \mathbb{R}$,

$$\begin{aligned} |u_n(f)(x) - f(x)| &= |u_n(f)(x) - f(x)u_n(e_0)(x) + f(x)u_n(e_0)(x) - f(x)| \\ &\leq |u_n(f)(x) - f(x)u_n(e_0)(x)| + |f(x)||u_n(e_0) - 1| \end{aligned}$$

Par hypothèse, il existe $n_0, n_1, n_2 \in \mathbb{N}$ tel que pour tout $i \in \{1, 2, 3\}, n \geq n_i$ $u_n(e_i) - e_i$ est bornée et $\|u_n(e_i) - e_i\|_\infty \leq \varepsilon$. D'où

$$|u_n(f)(x) - f(x)| \leq |u_n(f)(x) - f(x)u_n(e_0)(x)| + \|f\|_\infty \|u_n(e_0) - e_0\|_\infty$$

Il suffit donc de majorer le premier terme du membre de droite.

Étape 2 : Étudions la quantité $|u_n(f)(x) - f(x)u_n(e_0)(x)|$ à $x \in \mathbb{R}$ fixé

D'après le lemme, on a en fixant $x \in [0, 1]$, pour tout $y \in [0, 1]$

$$|f(y) - f(x)| \leq \varepsilon + c(y^2 - 2xy + x^2)$$

d'où l'inégalité fonctionnelle :

$$|f - f(x)e_0| \leq \varepsilon e_0 + c(e_2 - 2xe_1 + x^2e_0)$$

En appliquant u_n , on a pour tout $y \in [0, 1]$:

$$|u_n(f) - f(x)u_n(e_0)| \leq \varepsilon u_n(e_0) + c(u_n(e_2) - 2xu_n(e_1) + x^2u_n(e_0))$$

En évaluant cette égalité en $x \in \mathbb{R}$, on obtient l'inégalité

$$|u_n(f)(x) - f(x)u_n(e_0)(x)| \leq \varepsilon u_n(e_0)(x) + c(u_n(e_2)(x) - 2xu_n(e_1)(x) + x^2u_n(e_0)(x))$$

Or, comme $u_n(e_k) \xrightarrow[n \rightarrow +\infty]{\text{CVU}} e_k$ pour $k \in \{0, 1, 2\}$ et que les fonctions e_1, e_2 sont bornés. Donc la fonction $(u_n(e_2) - 2e_1u_n(e_1) + e_2u_n(e_0))$ converge uniformément vers $e_2 - 2e_1e_1 + e_2 = 0$.
Donc il existe $N \in \mathbb{N}$ tel que pour tout $n \geq N$, $|u_n(f)(x) - f(x)u_n(e_0)(x)| \leq 2\varepsilon$.

Étape 3 : Conclusion

On a donc $u_n(f) - f$ est borné à partir d'un certain rang, et $\|u_n(f) - f\|_\infty \leq (2 + \|f\|_\infty)\varepsilon$. Donc $(u_n(f))$ converge uniformément vers f . □

Application. Soit (B_n) la suite d'opérateurs définies par :

$$\forall f \in E, x \in [0, 1], B_n(f)(x) = \sum_{k=0}^n \binom{n}{k} f\left(\frac{k}{n}\right) x^k (1-x)^{n-k}$$

alors pour toute fonction $f \in E$, $(B_n(f))$ converge uniformément vers f .

Preuve : (B_n) est une suite d'opérateurs positifs avec

$$B_n(e_0)(x) = \sum_{k=0}^n \binom{n}{k} x^k (1-x)^{n-k} = 1 = e_0(x)$$

Afin de calculer $B_n(e_1)$ et $B_n(e_2)$ (qui peut s'avérer calculatoire), remarquons que

$$\forall k, n \in \mathbb{N}, B_n(e_k)(x) = \mathbb{E} \left[\left(\frac{X_n}{n} \right)^k \right] \text{ où } X_n \simeq \mathcal{B}(n, x)$$

D'où

$$B_n(e_1)(x) = \mathbb{E} \left[\frac{X_n}{n} \right] = \frac{nx}{n} = e_1(x)$$

et

$$\begin{aligned} B_n(e_2)(x) &= \mathbb{E} \left[\frac{X_n^2}{n^2} \right] = \frac{1}{n^2} \left(\text{Var}(X_n) + \mathbb{E}[X_n]^2 \right) \\ &= \frac{1}{n^2} \left(nx(1-x) + (nx)^2 \right) \end{aligned}$$

D'où $(B_n(e_2))$ converge uniformément vers e_2 .

D'après le théorème de Korovkin, pour toute fonction $f \in E$, $(B_n(f))$ converge uniformément vers f . □

Théorème de Riesz-Fréchet-Kolmogorov

Geoffrey Deperle

Leçons associées :

- 201 : Espaces de fonctions. Exemples et applications.
- 203 : Utilisation de la notion de compacité.
- 209 : Approximation d'une fonction par des fonctions régulières. Exemples et applications.
- 234 : Fonctions et espaces de fonctions Lebesgue-intégrables

Posons pour $h \in \mathbb{R}^N, x \in \mathbb{R}^N, \tau_h f(x) = f(x - h)$.

Le but de ce développement est de montrer le théorème suivant :

Théorème. Soit Ω un ouvert de \mathbb{R}^N , une partie bornée de A de $L^p(\Omega, \mathbb{K}), 1 \leq p < +\infty$ vérifiant :

1. $\forall \varepsilon > 0, \exists \delta > 0 / \forall f \in A, \forall \|h\| \geq \delta, \|\tau_h \tilde{f} - \tilde{f}\|_p \leq \varepsilon$
2. Pour tout $\varepsilon > 0$, il existe $B \subset \Omega$ un borélien borné tel que

$$\forall f \in A, \left(\int_{\Omega \setminus B} |f(x)|^p dx \right)^{\frac{1}{p}} \leq \varepsilon$$

avec $\tilde{f} : \mathbb{R}^N \rightarrow \mathbb{K}$ le prolongement par 0 de $f : \Omega \rightarrow \mathbb{K}$ en dehors de Ω , alors A est une partie relativement compacte de $L^p(\Omega, \mathbb{K})$.

Preuve : Soit $K = \overline{B}$, K une partie compacte de \mathbb{R}^N , nous allons régulariser par convolution puis appliquer le théorème d'Ascoli.

Soit $\varepsilon > 0, \delta = \delta(\varepsilon)$ tel 1).

Soit (ρ_n) une approximation de l'unité de \mathbb{R}^N . Posons $\tilde{f}_n = \tilde{f} \star \rho_n$.

Étape 1 : Montrons que $\forall f \in A, n > \frac{1}{\delta}, \|\tilde{f}_n - \tilde{f}\|_p \leq \varepsilon$

Soit $x \in \Omega, n \in \mathbb{N}^*$,

$$\begin{aligned} |\tilde{f}_n(x) - \tilde{f}(x)| &\leq \int_{\mathbb{R}^N} |\tilde{f}(x-y) - \tilde{f}(x)| \rho_n(y) dy \\ &= \int_{\mathbb{R}^N} |\tilde{f}(x-y) - \tilde{f}(x)| \rho_n(y)^{\frac{1}{p}} \rho_n(y)^{1-\frac{1}{p}} dy \end{aligned}$$

Comme $\rho_n \in \mathcal{C}_c^\infty(\mathbb{R}^N)$ et $\tilde{f} \in L^p(\mathbb{R}^N)$, $|\tilde{f}(x - \cdot) - \tilde{f}(x)|\rho_n^{\frac{1}{p}} \in L^p(\mathbb{R}^N)$ et $\rho_n \in L^q(\mathbb{R}^N)$. D'après l'inégalité de Hölder :

$$|\tilde{f}_n(x) - \tilde{f}(x)| \leq \left(\int_{\mathbb{R}^N} |\tilde{f}(x - y) - \tilde{f}(x)|^p \rho_n(y) dy \right)^{\frac{1}{p}} \left(\int_{\mathbb{R}^N} \rho_n(y)^{q(1-\frac{1}{p})} dy \right)^{\frac{1}{q}}$$

avec $q = \frac{p}{p-1}$ le conjugué de p donc $q(1 - \frac{1}{p}) = 1$ et (ρ_n) est une identité approchée.

$$|\tilde{f}_n(x) - \tilde{f}(x)|^p \leq \left(\int_{\mathbb{R}^N} |\tilde{f}(x - y) - \tilde{f}(x)|^p \rho_n(y) dy \right)$$

En intégrant sur Ω , par théorème de Fubini

$$\begin{aligned} \int_{\Omega} |\tilde{f}_n(x) - \tilde{f}(x)|^p dx &\leq \int_{\Omega} \int_{B(0, \frac{1}{n})} |\tilde{f}(x - y) - \tilde{f}(x)|^p \rho_n(y) dy dx \\ &= \int_{B(0, \frac{1}{n})} \rho_n(y) \int_{\Omega} |\tilde{f}_n(x) - \tilde{f}(x)|^p dx dy \\ &= \int_{B(0, \frac{1}{n})} \rho_n(y) \|\tau_y \tilde{f} - \tilde{f}\|_p^p dy \end{aligned}$$

Donc pour $n > \frac{1}{\delta}$, on a $\|\tilde{f}_n - \tilde{f}\|_p < \varepsilon$ pour tout $f \in A$ par hypothèse.

Étape 2 : Montrons que $C_n := \{\tilde{f}_n|_K, f \in A\}$ vérifie les hypothèses du théorème d'Ascoli

On a $C_n \subset \mathcal{C}(K, \mathbb{K})$ et $\forall x \in K, |\tilde{f}_n(x)| \leq \|f\|_p \|\rho_n\|_q$ donc C_n est une partie bornée de $\mathcal{C}(K, \mathbb{K})$. De plus, pour $x, y \in K$,

$$\begin{aligned} |\tilde{f}_n(x) - \tilde{f}_n(y)| &\leq \left(\int_{\mathbb{R}^N} |\tilde{f}(x - z) - \tilde{f}(y - z)|^p dy \right)^{\frac{1}{p}} \|\rho_n\|_q \\ &\leq \|\rho_n\|_q \|\tau_{x-y} \tilde{f} - \tilde{f}\|_p \end{aligned}$$

Donc pour $\|x - y\| \leq \delta$, on a $|\tilde{f}_n(x) - \tilde{f}_n(y)| \leq \varepsilon \|\rho_n\|_q$ donc C_n est une partie équicontinue. D'après le théorème d'Ascoli, C_n est précompact donc il existe un ensemble fini I et une famille de fonctions $(f_i)_{i \in I}$ de A telle que

$$\forall f \in A, \exists i \in I, \sup_{x \in K} |\tilde{f}_n(x) - \tilde{f}_{i,n}(x)| \leq \varepsilon \mu(K)^{-\frac{1}{p}}$$

Étape 3 : On se ramène à $L^p(\Omega, \mathbb{K})$

Pour $f \in A, n > \frac{1}{\delta}$

$$\begin{aligned} \|f - f_i\|_p &\leq \left(\int_{\Omega} |f(x) - f_i(x)|^p dx \right)^{\frac{1}{p}} \\ &\leq \underbrace{\left(\int_{\Omega \setminus K} |f(x)|^p dx \right)^{\frac{1}{p}}}_{\leq \varepsilon} + \underbrace{\left(\int_{\Omega \setminus K} |f_i(x)|^p dx \right)^{\frac{1}{p}}}_{\leq \varepsilon} + \left(\int_{\Omega \cap K} |f(x) - f_i(x)|^p dx \right)^{\frac{1}{p}} \end{aligned}$$

Or, $|f - f_i| \mathbf{1}_{\Omega \cap K} \leq (|f - \tilde{f}| + |\tilde{f} - \tilde{f}_n| + |\tilde{f}_n - \tilde{f}_{i,n}|) \mathbf{1}_{\Omega \cap K}$. D'où

$$\left(\int_{\Omega \cap K} |f(x) - f_i(x)|^p dx \right)^{\frac{1}{p}} \leq \|\tilde{f} - \tilde{f}_n\|_p + \|\tilde{f}_n - \tilde{f}_{i,n}\|_p + \left(\int_{\Omega \cap K} |\tilde{f}_n(x) - \tilde{f}_{i,n}(x)|^p dx \right)^{\frac{1}{p}}$$

et

$$\left(\int_{\Omega \cap K} |\tilde{f}_n(x) - \tilde{f}_{i,n}(x)|^p dx \right)^{\frac{1}{p}} \leq \left(\int_{\Omega \cap K} (\varepsilon \mu(K)^{-\frac{1}{p}})^p dx \right)^{\frac{1}{p}} \leq \varepsilon$$

d'où $\|f - f_i\|_p \leq 5\varepsilon$ donc les $B(f_i, 5\varepsilon)$ recouvrent A donc A est précompact. Comme L^p est complet, A est relativement compact. \square

Théorème de Stampacchia

Geoffrey Deperle

Leçons associées :

- 205 : Espaces complets
- 208 : Espaces vectoriels normés, applications linéaires continues. Exemples.
- 213 : Espaces de Hilbert. Bases hilbertiennes. Exemples et applications.
- 219 : Extremums : existence, caractérisation, recherche. Exemples et applications.
- 253 : Utilisation de la notion de convexité en analyse.

Le but de ce développement est de montrer le théorème suivant :

Théorème. Soit H un espace de Hilbert et $a(\cdot, \cdot)$ une forme bilinéaire continue et coercive sur H i.e. vérifiant les conditions :

$$(i) \exists c > 0 / \forall u, v \in H, |a(u, v)| \leq c \|u\| \|v\|$$

$$(ii) \exists \alpha > 0 / \forall v \in H, a(v, v) \geq \alpha \|v\|^2$$

Soit K un convexe fermé non vide, étant donné $\varphi \in H'$, il existe $u \in K$ tel que

$$\forall v \in K, a(u, v - u) \geq \varphi(v - u) \quad (*)$$

Si de plus a est symétrique, alors u est caractérisé par

$$\begin{cases} u \in K \\ \frac{1}{2} a(u, u) - \varphi(u) = \min_{v \in K} \left\{ \frac{1}{2} a(v, v) - \varphi(v) \right\} \end{cases}$$

Preuve :

Étape 1 : Reformulons le problème (*) en terme de problème de point fixe.

D'après le théorème de représentation de Riesz,

$$\exists ! f \in H / \forall v \in H, \varphi(v) = \langle f, v \rangle$$

De plus, pour tout $u \in H$ fixé, $v \mapsto a(u, v)$ est linéaire continue donc il existe un unique $Au \in H$ tel que $a(u, v) = \langle Au, v \rangle$.

A est alors un opérateur linéaire de H dans H par unicité avec $\forall u \in H, \begin{cases} \|Au\| & \leq c \|u\| \\ \langle Au, u \rangle & \geq \alpha \|u\|^2 \end{cases}$.

Le problème (*) consiste alors à trouver $u \in K$ tel que

$$\begin{aligned} \forall v \in K, \langle Au, v - u \rangle &\geq \langle f, v - u \rangle \\ \iff \forall v \in K, \forall \rho > 0, \langle \rho f - \rho Au + u - u, v - u \rangle &\leq 0 \\ \iff u = P_K(\rho f - \rho Au + u) \end{aligned}$$

Étape 2 : Trouvons ρ tel que
$$\begin{array}{ccc} S : K & \rightarrow & K \\ v & \mapsto & P_K(\rho f - \rho Av + v) \end{array}$$
 soit une contraction afin d'utiliser un théorème de point fixe.

Comme P_K est 1-lipschitzienne,

$$\forall v_1, v_2 \in K, \|S(v_1) - S(v_2)\| \leq \|(v_1 - v_2) - \rho(Av_1 - Av_2)\|$$

D'où

$$\begin{aligned} \|S(v_1) - S(v_2)\|^2 &\leq \|v_1 - v_2\|^2 - 2\rho \langle v_1 - v_2, Av_1 - Av_2 \rangle + \rho^2 \|Av_1 - Av_2\|^2 \\ &\leq (1 - 2\rho\alpha + \rho^2 c^2) \|v_1 - v_2\|^2 \end{aligned}$$

Comme $1 - 2\rho\alpha + \rho^2 c^2 \underset{\rho \rightarrow 0}{\sim} 1 - 2\rho\alpha < 1$, il existe $\rho > 0$ tel que $1 - 2\rho\alpha + \rho^2 c^2 < 1$.

On a alors

$$\|S(v_1) - S(v_2)\| \leq k \|v_1 - v_2\|$$

Par théorème de point fixe de Picard, S admet un point fixe.

Supposons de plus que $a(\cdot, \cdot)$ est symétrique

Si de plus $a(\cdot, \cdot)$ est symétrique, $(u, v) \mapsto a(u, v)$ définit un nouveau produit scalaire sur H de norme $u \mapsto a(u, u)^{\frac{1}{2}}$ équivalente à $\|\cdot\|$. H est donc un espace de Hilbert pour ce produit scalaire. Par théorème de Riesz, il existe $g \in H$ tel que pour tout $v \in H$, $\varphi(v) = a(g, v)$.

Ainsi,

$$\begin{aligned} (*) \iff \forall v \in K, a(g - u, v - u) &\leq 0 \\ \iff u = \widetilde{P}_K g \end{aligned}$$

où \widetilde{P}_K désigne la projection de g au sens du produit scalaire défini par a .

Il faut donc trouver $u \in K$ réalisant $\min_{v \in K} a(g - v, g - v)^{\frac{1}{2}}$.

Ceci revient à minimiser sur K la quantité $a(g - v, g - v)$ donc à minimiser $a(v, v) - 2a(g, v)$ donc minimiser $\frac{1}{2}a(v, v) - \varphi(v)$. □

Annexe

Application (Résolution du problème de Dirichlet non homogène en dimension 1). Soit $I =]0, 1[$, $f \in L^2(I)$ et $\alpha, \beta \in \mathbb{R}$, il existe $u \in H^2(I)$ unique vérifiant :

$$\begin{cases} -u'' + u = f & \text{sur } I \\ \tilde{u}(0) = \alpha, \tilde{u}(1) = \beta \end{cases}$$

avec \tilde{u} le représentant continue de u .

De plus, u s'obtient par

$$u = \min_{\substack{v \in H^1 \\ v(0)=\alpha, v(1)=\beta}} \left\{ \frac{1}{2} \int_I (v'^2 + v^2) - \int_I f v \right\}$$

Preuve : Soit K la partie de $H^1(I)$ définie par

$$K = \{v \in H^1(I), v(0) = \alpha, v(1) = \beta\}$$

K est un convexe fermé de $H^1(I)$ Si u est une solution classique, alors

$$\forall v \in K, \int_I u'(v-u)' + \int_I u(v-u) = \int_I f(v-u) \geq \int_I f(v-u)$$

Donc par théorème de Stampacchia, il existe un unique $u \in K$ solution du problème de Dirichlet. Ce u s'obtient par

$$u = \min_{\substack{v \in H^1 \\ v(0)=\alpha, v(1)=\beta}} \left\{ \frac{1}{2} \int_I (v'^2 + v^2) - \int_I f v \right\}$$

□

Théorème du point fixe de Brouwer

Geoffrey Deperle

Leçons associées :

- 203 : Utilisation de la notion de compacité.
- 204 : Connexité. Exemples et applications.
- 206 : Exemples d'utilisation de la notion de dimension finie en analyse.
- 214 : Théorème d'inverse locale, théorèmes des fonctions implicites. Exemples et applications en analyse et géométrie.
- 215 : Applications différentiables définies sur un ouvert de \mathbb{R}^n . Exemples et applications.

Le but de ce développement est de montrer le théorème suivant :

Théorème. *Toute application de classe C^1 de la boule unité fermée de \mathbb{R}^d dans elle-même admet un point fixe.*

Preuve : Supposons par l'absurde qu'il existe $f : B \rightarrow B$ de classe C^1 sans point fixe.

Étape 1 : Montrons qu'il existe $\varphi : B \rightarrow S = \partial B$ de classe C^1 telle que $\varphi|_S = \text{id}|_S$

Pour $x \in B$, notons $\varphi(x)$ le point d'intersection de la demi-droite $[f(x), x)$ et S , $\varphi(x)$ est de la forme $\varphi(x) = f(x) + \lambda(x)(x - f(x))$ avec $\lambda(x) \geq 0$ et vérifie

$$\begin{aligned} \|f(x) + \lambda(x)(x - f(x))\|^2 &= 1 \\ \iff \|x - f(x)\|^2 \lambda(x)^2 + 2\lambda(x)\langle f(x), x - f(x) \rangle + (\|f(x)\|^2 - 1) &= 0 \end{aligned}$$

Posons $\Delta(x) = \langle f(x), x - f(x) \rangle^2 + \underbrace{\|x - f(x)\|^2(1 - \|f(x)\|^2)}_{>0} > 0$.

D'où $\lambda(x) = -\frac{\langle f(x), x - f(x) \rangle + \sqrt{\Delta(x)}}{\|x - f(x)\|^2}$ donc λ est de classe C^1 et φ est de classe C^1 et par construction on a $\varphi|_S = \text{id}|_S$

Étape 2 : Construisons une fonction volume

$$\text{Posons } F : B \times [0, 1] \rightarrow B \\ (x, t) \mapsto (1 - t)x + t\varphi(x) .$$

On a en particulier $F(\cdot, 0) = \text{id}_B$ et $F(\cdot, 1) = \varphi$ et pour $x \in S, t \in [0, 1]$, on a $F(x, t) = x$.

Pour $t \in [0, 1]$, posons $V(t) = \int_{\mathring{B}} \det \partial_1 F(x, t) dx$ qui est polynomiale avec $F(x, 1) = \varphi(x)$ qui n'est pas différentielle inversible en tout point de \mathring{B} .

En effet, comme $\|\varphi(x)\|^2 = 1$, en différentiant on a $\forall h \in \mathbb{R}^d, x \in \mathring{B}, \langle \varphi(x), d\varphi(x) \cdot h \rangle = 0$ d'où $\text{Im}(d\varphi(x)) \subset \{\varphi(x)\}^\perp$. Or, comme $\varphi(x) \neq 0$, on a $d\varphi(x)$ non inversible (de rang $< d$). D'où $V(1) = 0$.

Étape 3 : Montrons que pour t assez petit $x \mapsto \det \partial_1 F(x, t)$ est strictement positive et injective.

Par l'absurde, si pour tout $n \in \mathbb{N}^*$, il existe $t_n \in]0, \frac{1}{n}]$ et $x_n \in B$ telle que $\det \partial_1 F(x_n, t_n) \leq 0$. Par propriété de Bolzano-Weierstrass, il existe $x \in B$ et une sous-suite $(x_{\phi(n)})$ telle que $x_{\phi(n)} \xrightarrow[n \rightarrow +\infty]{} x$. Par continuité de $\partial_1 F$ et de \det , en passant à la limite, on a $\det \partial_1 F(x, 0) \leq 0$. Absurde car $F(\cdot, 0) = \text{id}$.

Donc il existe $N \in \mathbb{N}$ tel que pour tout $t < \frac{1}{N}$ et $x \in B$ on a $\det \partial_1 F(x, t) > 0$.

Ainsi, par théorème d'inversion locale, on a $F(\overset{\circ}{B}, t)$ est un ouvert de \mathbb{R}^d .

Montrons que $F(\cdot, t)$ est injective pour t assez petit, Soit $t < \frac{1}{N}$ et $x, y \in B$, si $F(x, t) = F(y, t)$ alors par inégalité des accroissements finis,

$$\begin{aligned} (1-t)\|x-y\| &= t\|\varphi(x) - \varphi(y)\| \\ &\leq tM\|x-y\| \end{aligned}$$

avec $M = \sup_{z \in B} \|\text{d}\varphi(z)\|$.

Donc $\|x-y\| \leq \frac{Mt}{1-t}\|x-y\|$ il existe donc $\alpha < \frac{1}{N}$ tel que pour tout $t \leq \alpha$, on ait $\frac{Mt}{1-t} < 1$ donc pour $t < \alpha$, $F(\cdot, t)$ est injective.

Étape 4 : Conclusion

Pour $t < \alpha$, comme pour $x \in S$, $F(x, t) = x$ donc $F(\overset{\circ}{B}, t) \cup S = F(B, t)$ qui est compact donc fermé, d'où en passant au complémentaire $F(\overset{\circ}{B}, t) = F(B, t) \cap \overset{\circ}{B}$ fermé dans $\overset{\circ}{B}$.

Or, par théorème d'inversion locale, $F(\overset{\circ}{B}, t)$ est ouvert donc par connexité, $F(\overset{\circ}{B}, t) = \overset{\circ}{B}$.

Ainsi pour $t < \alpha$,

$$\begin{aligned} V(t) &= \int_{\overset{\circ}{B}} \det \partial_1 F(x, t) \, dx = \int_{\overset{\circ}{B}} |\det \partial_1 F(x, t)| \, dx \\ &= \int_{\overset{\circ}{B}} d\lambda_d \\ &= \lambda(\overset{\circ}{B}) \end{aligned}$$

donc cette fonction polynomiale est constante sur un intervalle non vide donc constante, donc elle est constante égale à cette valeur sur $[0, 1]$. Or, comme $V(1) = 0 \neq \lambda(\overset{\circ}{B})$.

Absurde, f admet un point fixe. □

Annexe

Théorème. Toute application continue de la boule unité fermée de \mathbb{R}^d dans elle-même admet un point fixe.

Preuve : Comme B est compacte, soit $\varepsilon > 0$ tel que pour tout $x \in B$, $\|f(x) - x\| > \varepsilon$. Par théorème de Stone-Weierstrass, il existe $P : \mathbb{R}^d \rightarrow \mathbb{R}^d$ de coordonnées polynomiales telle que $\|f - P\|_\infty < \frac{\varepsilon}{2}$.

Pour tout $x \in B$, on a $\|P(x)\| \leq \|P(x) - f(x)\| + \|f(x)\| < \frac{\varepsilon}{2} + 1$.

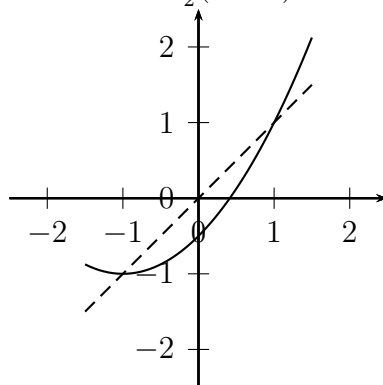
D'où $\frac{1}{1+\frac{\varepsilon}{2}}P$ est polynomiale, C^1 et vérifie $Q(B) \subset B$.

Pour tout $x \in B$, $\|Q(x) - f(x)\| \leq \|Q(x) - P(x)\| + \|P(x) - f(x)\| \leq \left(1 - \frac{1}{1+\frac{\varepsilon}{2}}\right) \|P(x)\| + \frac{\varepsilon}{2}$.

D'où $\|Q(x) - x\| \geq \|f(x) - x\| - \|Q(x) - f(x)\| > 0$ donc Q n'admet pas de point fixe. \square

Contre-exemples :

- Si la boule est ouverte : $f :]-1, 1[\rightarrow]-1, 1[$
 $x \mapsto \frac{1}{2}(x+1)^2 - 1$ n'admet pas de point fixe.



- Si la dimension est infinie, pour $H = l^2(\mathbb{Z})$, (e_n) sa base hilbertienne usuelle, en considérant l'application $T : H \rightarrow H$
 $(x_n) \mapsto (1 - \|x\|)e_0 + U(x)$ avec U l'opérateur de Shift : $U : (x_n) \mapsto (x_{n+1})$.

On a $\forall x \in B_H(0, 1)$, $\|T(x)\| \leq |1 - \|x\|| + \|x\| = 1$ mais T n'admet pas de point fixe, en effet,

$$\text{pour } x \in B_H(0, 1), T(x) = x \iff \begin{cases} x_0 = 1 - \|x\| + x_{-1} \\ x_n = x_{n-1} \quad \text{si } n \neq 0 \end{cases}$$

$$\text{D'où } \begin{cases} x_n = x_0 & \text{si } n \geq 0 \\ x_n = x_{-1} & \text{sinon} \end{cases}$$

Or, $x \in H$, $x_0 = x_{-1} = 0$ donc $x = 0$ ce qui est impossible car $x_0 = 1 - \|x\| + x_{-1}$.

Théorème de Levy et TCL

Geoffrey Deperle

Leçons associées :

- 250 : Transformation de Fourier. Applications.
- 262 : Convergences d'une suite de variables aléatoires. Théorèmes limite. Exemples et applications.

Le but de ce développement est de montrer le théorème suivant :

Définition 2. On dit qu'une suite de variables aléatoires réelles (X_n) converge en loi vers X si pour tout $f \in \mathcal{C}_b(\mathbb{R})$, on a

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

Lemme 15. Soit (X_n) une suite de variables aléatoires réelles et X une variable aléatoire réelle.

$$X_n \xrightarrow[n \rightarrow +\infty]{\mathcal{L}} X \iff \forall f \in \mathcal{C}_0(\mathbb{R}), \mathbb{E}[f(X_n)] \xrightarrow{n \rightarrow +\infty} \mathbb{E}[f(X)]$$

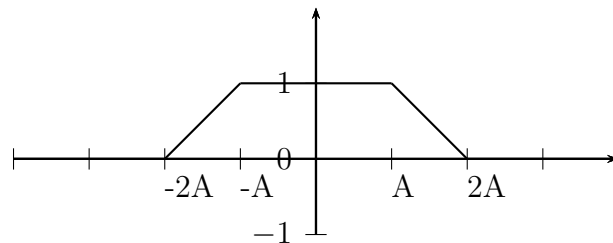
avec $\mathcal{C}_0 = \{f \in \mathcal{C}(\mathbb{R}), f(x) \xrightarrow{x \rightarrow \pm\infty} 0\}$

Preuve :

(\implies) Comme $\mathcal{C}_0(\mathbb{R}) \subset \mathcal{C}_b(\mathbb{R})$.

(\impliedby) Soit $\varepsilon > 0$ et $A > 0$ tel que $\mathbb{P}_X(\{x; |x| > A\}) \leq \varepsilon$.

Posons φ :



de sorte que $\int_{\mathbb{R}} (1 - \varphi) d\mathbb{P}_X \leq \mathbb{P}_X(\{x; |x| > A\}) \leq \varepsilon$.

Soit $f \in \mathcal{C}_b^0(\mathbb{R})$,

$$\int_{\mathbb{R}} f d\mathbb{P}_{X_n} - \int_{\mathbb{R}} f d\mathbb{P}_X = \underbrace{\int_{\mathbb{R}} f(1 - \varphi) d\mathbb{P}_X}_{\leq \|f\|_{\infty} \int_{\mathbb{R}} (1 - \varphi) d\mathbb{P}_X} + \underbrace{\left[\int_{\mathbb{R}} f \varphi d\mathbb{P}_{X_n} - \int_{\mathbb{R}} f \varphi d\mathbb{P}_X \right]}_{\xrightarrow{n \rightarrow +\infty} 0}$$

Or,

$$\begin{aligned} \limsup_{n \rightarrow +\infty} \int_{\mathbb{R}} f(1 - \varphi) d\mathbb{P}_{X_n} &\leq \|f\|_{\infty} \left(1 - \int \varphi d\mathbb{P}_X\right) \quad \text{car } \varphi \in \mathcal{C}_b^0(\mathbb{R}) \\ &\leq \varepsilon \|f\|_{\infty} \end{aligned}$$

D'où $\limsup_{n \rightarrow +\infty} \left| \int_{\mathbb{R}} f d\mathbb{P}_{X_n} - \int_{\mathbb{R}} f d\mathbb{P}_X \right| \leq 2\varepsilon \|f\|_{\infty}$.

D'où $|\mathbb{E}[f(X_n) - f(X)]| \xrightarrow{n \rightarrow +\infty} 0$. □

Théorème. Soit X et (X_n) des variables aléatoires réelles, on a équivalence entre

- (i) (X_n) converge en loi vers X
- (ii) La suite (φ_{X_n}) des fonctions caractéristiques des X_n converge simplement vers φ_X .

Preuve : (i) \implies (ii) Vrai car $x \mapsto e^{ixt}$ est borné pour tout $t \in \mathbb{R}$.

(ii) \implies (i)

Soit $f \in \mathcal{C}_0(\mathbb{R})$ $\varepsilon > 0$, il existe $g \in \mathcal{C}_c^{\infty}(\mathbb{R})$, $\|f - g\|_{\infty} \leq \varepsilon$.

Or, $\mathcal{C}_c^{\infty}(\mathbb{R}) \subset S(\mathbb{R})$ donc il existe $\varphi \in L^1(\mathbb{R})$ tel que $g = \widehat{\varphi}$.

$$|\mathbb{E}[f(X_n) - f(X)]| \leq \underbrace{|\mathbb{E}[(f - g)(X_n)]|}_{\leq \|f - g\|_{\infty} \leq \varepsilon} + \underbrace{|\mathbb{E}[(f - g)(X)]|}_{\leq \|f - g\|_{\infty} \leq \varepsilon} + |\mathbb{E}[g(X_n) - g(X)]|$$

Or,

$$\begin{aligned} \mathbb{E}[g(X_n)] &= \mathbb{E} \left[\int_{\mathbb{R}} e^{itX_n} \varphi(t) dt \right] = \int_{\mathbb{R}} \varphi(t) \mathbb{E}[e^{itX_n}] dt \quad \text{par théorème de Fubini} \\ &\xrightarrow{n \rightarrow +\infty} \int_{\mathbb{R}} \varphi(t) \mathbb{E}[e^{itX}] dt \quad \text{par théorème de convergence dominé} \\ &= \mathbb{E} \left[\int_{\mathbb{R}} \varphi(t) e^{itX} dt \right] \\ &= \mathbb{E}[g(X)] \end{aligned}$$

D'où $\limsup_{n \rightarrow +\infty} |\mathbb{E}[f(X_n)] - \mathbb{E}[f(X)]| \leq 2\varepsilon$. □

Lemme 16. Soit (z_n) une suite de nombres complexes convergeant vers $z \in \mathbb{C}$, on a

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

Preuve : On note Log la détermination principale du logarithme complexe.

Comme $\frac{z_n}{n} \xrightarrow{n \rightarrow +\infty} 0$, il existe $N \in \mathbb{N}$ tel que pour tout $n \geq N$, $\frac{z_n}{n} \in D(0, 1)$ donc

$$\left(1 + \frac{z_n}{n}\right)^n = \exp \left(n \text{Log} \left(1 + \frac{z_n}{n}\right) \right) = \exp \left(n \left(\frac{z_n}{n} + o\left(\frac{z_n}{n}\right) \right) \right) = \exp(z_n + o(z_n))$$

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

Théorème. Soit (X_n) une suite de variable aléatoire réelle indépendante et identiquement distribuées admettant un moment d'ordre 2. En notant $\mu = \mathbb{E}[X_1]$ et $\sigma^2 = \text{Var}(X_1)$, on pose

$$S_n = \sum_{k=1}^n X_k, \text{ on a}$$

$$\frac{S_n - n\mu}{\sigma\sqrt{n}} \xrightarrow[n \rightarrow +\infty]{\mathcal{L}} \mathcal{N}(0, 1)$$

Preuve : Sans perte de généralité, supposons $\sigma = 1$ et $\mu = 0$. On doit montrer que $\varphi_{\frac{S_n}{\sqrt{n}}}(t)$ converge vers $e^{-\frac{t^2}{2}}$ pour tout $t \in \mathbb{R}$.

Posons $\varphi = \varphi_{X_1}$, φ est de classe C^2 car $X_1 \in \mathbb{L}^2(\Omega)$ avec de plus

$$\begin{cases} \varphi'(0) &= i\mathbb{E}[X_1] = 0 \\ \varphi''(0) &= \mathbb{E}[-X_1^2] = -1 \end{cases}$$

D'où

$$\begin{aligned} \varphi_{\frac{S_n}{\sqrt{n}}}(t) &= \mathbb{E} \left[\prod_{k=1}^n e^{it\frac{X_k}{\sqrt{n}}} \right] = \prod_{k=1}^n \mathbb{E} \left[e^{it\frac{X_1}{\sqrt{n}}} \right] \quad \text{par indépendance des } X_k \\ &= \left(\mathbb{E} \left[e^{it\frac{X_1}{\sqrt{n}}} \right] \right)^n \\ &= \varphi \left(\frac{t}{\sqrt{n}} \right)^n \\ &= \left(1 - \frac{t^2}{2n} + o\left(\frac{1}{n}\right) \right)^n \end{aligned}$$

et on conclut avec le lemme. □