Développements pour l'Agrégation externe de Mathématiques

Florian Bertuol

23 novembre 2018

Résumé

Ce document contient l'ensemble des développements que j'ai choisi de préparer pour l'oral de l'Agrégation externe de Mathématiques 2016, ainsi que l'ensemble des leçons au programme cette année-là classées par numéro, chacune d'entre elle étant accompagnée de mon choix de couplage.

Table des matières

1 Développements d'Algèbre **13**

1.1 Topologie des orbites de l'action de Steinitz 13
1.2 Théorème de Burnside 17
1.3 Automorphismes de $\mathfrak{S}_n$ 21
1.4 Un anneau principal et non-euclidien 24
1.5 Théorème des deux carrés 28
1.6 Points extrémaux de la boule unité de $\mathcal{L}(E)$ 31
1.7 Théorème de Wedderburn 34
1.8 Théorème de l'élément primitif 36
1.9 Le cube et les représentations de $\mathfrak{S}_4$ 39
1.10 Ellipsoïde de John-Loewner 42
1.11 Partitions d'un entier en parts fixées 46
1.12 Dénombrement des polynômes irréductibles sur $\mathbb{F}_q$ 49
1.13 Décomposition de Dunford 53
1.14 Réduction des endomorphismes normaux 56
1.15 Générateurs de $\mathrm{GL}_n(K)$ et de $\mathrm{SL}_n(K)$ 59
1.16 Théorème de Kronecker 62
1.17 Loi de réciprocité quadratique 65
1.18 Groupes des K-automorphismes de $K(X)$ 68
1.19 L'hexagone et les représentations de D_6 71

2 Développements d'Analyse **75**

2.1 Lemme de Morse 75
2.2 Marche aléatoire sur $\mathbb{Z}$ 79
2.3 Théorème de Cartan-von Neumann 82
2.4 Théorème de Liapounov 86
2.5 Théorème de Cauchy-Lipschitz global 89
2.6 Méthode du gradient à pas optimal 92
2.7 Méthode de Newton 95
2.8 Une fonction continue, nulle part dérivable 99
2.9 Développement asymptotique de la série harmonique 101

2.10 Densité des polynômes orthogonaux . . . 104
2.11 Théorème d'approximation de Weierstrass . . . 108
2.12 Théorème central limite . . . 110
2.13 Théorème de projection dans un espace de Hilbert . . . 113
2.14 Prolongement méromorphe de la fonction Γ . . . 116
2.15 Théorèmes d'Abel angulaire et Taubérien faible . . . 120
2.16 Théorème de Riesz-Fischer . . . 123
2.17 Théorème des extrema liés . . . 127
2.18 Inégalité de Hoeffding . . . 130
2.19 Théorème de Sarkovski . . . 133
2.20 Équation de la chaleur . . . 136
2.21 Formule sommatoire de Poisson . . . 139
2.22 Formule d'inversion de Fourier dans $\mathcal{S}$ . . . 142

3 Leçons d'Algèbre **145**
3.1 101 : Groupe opérant sur un ensemble. Exemples et applications. 145
3.2 102 : Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications. . . . 145
3.3 103 : Exemples de sous-groupes distingués et de groupes quotients. Applications. . . . 145
3.4 104 : Groupes finis. Exemples et applications. . . . 146
3.5 105 : Groupe des permutations d'un ensemble fini. Applications. 146
3.6 106 : Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $\mathrm{GL}(E)$. Applications. . . . 146
3.7 107 : Représentations et caractères d'un groupe fini sur un $\mathbb{C}$-espace vectoriel. . . . 146
3.8 108 : Exemples de parties génératrices d'un groupe. Applications. 146
3.9 . . . 147
3.10 110 : Caractère d'un groupe abélien fini et transformée de FOURIER discrète. Applications. . . . 147
3.11 120 : Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications. . . . 147
3.12 121 : Nombres premiers. Applications. . . . 147
3.13 122 : Anneaux principaux. Exemples et applications. . . . 147
3.14 123 : Corps finis. Applications. . . . 147
3.15 124 : Anneau des séries formelles. Applications. . . . 148
3.16 125 : Extensions de corps. Exemples et applications. . . . 148
3.17 126 : Exemples d'équations diophantiennes. . . . 148
3.18 127 : Droite projective et birapport. . . . 148
3.19 140 : Corps des fractions rationnelles à une indéterminée sur un corps commutatif. Applications. . . . 148

3.20 141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications. 148
3.21 149
3.22 143 : Résultant. Applications. 149
3.23 144 : Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications. 149
3.24 150 : Exemples d'actions de groupes sur les espaces de matrices. 149
3.25 151 : Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications. 149
3.26 152 : Déterminant. Exemples et applications. 150
3.27 153 : Polynômes d'endomorphisme en dimension finie. Applications à la réduction d'un endomorphisme en dimension finie. . . 150
3.28 154 : Sous-espaces stables par un endomorphisme ou une famille d'endomorphismes d'un espace vectoriel en dimension finie. Applications. 150
3.29 155 : Endomorphismes diagonalisables en dimension finie. 150
3.30 151
3.31 157 : Endomorphismes trigonalisables. Endomorphismes nilpotents. 151
3.32 158 : Matrices symétriques réelles, matrices hermitiennes. 151
3.33 159 : Formes linéaires et dualité en dimension finie. Exemples et applications. 151
3.34 160 : Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie). 151
3.35 161 : Isométries d'un espace affine euclidien de dimension finie. Applications en dimensions 2 et 3. 152
3.36 162 : Systèmes d'équations linéaires, opérations élémentaires, aspects algorithmiques et conséquences théoriques. 152
3.37 170 : Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications. 152
3.38 171 : Formes quadratiques réelles. Exemples et applications. . . . 152
3.39 180 : Coniques. Applications. 152
3.40 153
3.41 182 : Applications des nombres complexes à la géométrie. Homographies. 153
3.42 183 : Utilisation des groupes en géométrie. 153
3.43 190 : Méthodes combinatoires, problèmes de dénombrements. . . 153

4 Leçons d'Analyse **155**
4.1 201 : Espaces de fonctions : exemples et applications. 155
4.2 202 : Exemples de parties denses et applications. 155

4.3 203 : Utilisation de la notion de compacité. 155
4.4 204 : Connexité. Exemples et applications. 155
4.5 205 : Espaces complets. Exemples et applications. 156
4.6 206 : Théorèmes de point fixe. Exemples et applications. 156
4.7 207 : Prolongement de fonctions. Exemples et applications. 156
4.8 208 : Espaces vectoriels normés, applications linéaires continues. Exemples. 156
4.9 209 : Approximation d'une fonction par des polynômes et des polynômes trigonométriques. Exemples et applications. 156
4.10 157
4.11 214 : Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications. 157
4.12 215 : Applications différentiables définies sur un ouvert de $\mathbb{R}^n$. Exemples et applications. 157
4.13 217 : Sous variétés de $\mathbb{R}^n$. Exemples. 157
4.14 218 : Applications des formules de TAYLOR. 157
4.15 219 : Extremums : existence, caractérisation, recherche. Exemples et applications. 157
4.16 220 : Équations différentielles $X' = f(t, X)$. Exemples d'étude des solutions en dimension 1 et 2. 158
4.17 221 : Équations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications. 158
4.18 222 : Exemples d'équations aux dérivées partielles linéaires. . . . 158
4.19 223 : Suites numériques. Convergence, valeurs d'adhérence. Exemples et applications. 158
4.20 224 : Exemples de développements asymptotiques de suites et de fonctions. 158
4.21 159
4.22 228 : Continuité et dérivabilité des fonctions réelles d'une variable réelle. Exemples et contre-exemples. 159
4.23 229 : Fonctions monotones. Fonctions convexes. Exemples et applications. 159
4.24 230 : Séries de nombres réels ou complexes. Comportement des restes ou des sommes partielles des séries numériques. Exemples. 159
4.25 232 : Méthodes d'approximation des solutions d'une équation $F(X) = 0$. Exemples. 159
4.26 233 : Analyse numérique matricielle : résolution approchée de systèmes linéaires, recherche de vecteurs propres, exemples. . . . 160
4.27 234 : Espaces $L^p, 1 \leq p \leq +\infty$. 160
4.28 235 : Problèmes d'interversion de limites et d'intégrales. 160

4.29 236 : Illustrer par des exemples quelques méthodes de calcul d'intégrales de fonctions d'une ou plusieurs variables réelles. 160
4.30 161
4.31 240 : Produit de convolution, transformation de FOURIER. Applications. 161
4.32 241 : Suites et séries de fonctions. Exemples et contre-exemples. . 161
4.33 243 : Convergence des séries entières, propriétés de la somme. Exemples et applications. 161
4.34 244 : Fonctions développables en série entière, fonctions analytiques. Exemples. 161
4.35 245 : Fonctions holomorphes sur un ouvert de $\mathbb{C}$. Exemples et applications. 162
4.36 246 : Séries de FOURIER. Exemples et applications. 162
4.37 247 : Exemples de problèmes d'interversion de limites. 162
4.38 249 : Suites de variables de BERNOULLI indépendantes. 162
4.39 253 : Utilisation de la notion de convexité en analyse. 162
4.40 163
4.41 260 : Espérance, variance et moments d'une variable aléatoire. . . 163
4.42 261 : Fonction caractéristique et transformée de LAPLACE d'une variable aléatoire. Exemples et applications. 163
4.43 262 : Modes de convergence d'une suite de variables aléatoires. Exemples et applications. 163
4.44 263 : Variables aléatoires à densité. Exemples et applications. . . 163
4.45 264 : Variables aléatoires discrètes. Exemples et applications. . . . 164

Bibliographie

[Ave91] André AVEZ : *Calcul différentiel*. Masson, deuxième édition, 1991.

[BL07] Philippe BARBE et Michel LEDOUX : *Probabilités*. EDP sciences, 2007.

[BMP05] Vincent BECK, Jérôme MALICK et Gabriel PEYRÉ : *Objectif Agrégation*. H et K, 2005.

[Bre05] Haïm BREZIS : *Analyse fonctionnelle*. Dunod, 2005.

[CG13] Philippe CALDERO et Jérôme GERMONI : *Histoires hédonistes de groupes et de géométries, tome premier*. Calvage et Mounet, 2013.

[CG14] Philippe CALDERO et Jérôme GERMONI : *Histoires hédonistes de groupes et de géométries, tome second*. Calvage et Mounet, 2014.

[Cia82] Philippe CIARLET : *Introduction à l'analyse numérique matricielle et à l'optimisation*. Masson, 1982.

[FG97] Serge FRANCINOU et Hervé GIANELLA : *Exercices de mathématiques pour l'agrégation*. Masson, 1997.

[FGN09] Serge FRANCINOU, Hervé GIANELLA et Serge NICOLAS : *Oraux X-ENS algèbre*, volume 2. Cassini, deuxième édition, 2009.

[FGN10] Serge FRANCINOU, Hervé GIANELLA et Serge NICOLAS : *Oraux X-ENS algèbre*, volume 3. Cassini, deuxième édition, 2010.

[FGN14a] Serge FRANCINOU, Hervé GIANELLA et Serge NICOLAS : *Oraux X-ENS algèbre*, volume 1. Cassini, troisième édition, 2014.

[FGN14b] Serge FRANCINOU, Hervé GIANELLA et Serge NICOLAS : *Oraux X-ENS analyse*, volume 2. Cassini, deuxième édition, 2014.

[FGN14c] Serge FRANCINOU, Hervé GIANELLA et Serge NICOLAS : *Oraux X-ENS analyse*, volume 1. Cassini, deuxième édition, 2014.

[GK11] Olivier GARET et Aline KURTZMANN : *De l'intégration aux probabilités*. Ellipses, 2011.

[Gou08] Xavier GOURDON : *Analyse*. Ellipses, deuxième édition, 2008.

[Gou09] Xavier GOURDON : *Algèbre*. Ellipses, deuxième édition, 2009.

[GT98] Stéphane GONNORD et Nicolas TOSEL : *Calcul différentiel*. Ellipses, 1998.

[Mad97] Karine MADÈRE : *Développements d'Analyse*. Ellipses, 1997.

[Mar07] Jean-Pierre MARCO : *Mathématiques L2*. Pearson Education, 2007.

[Ort04] Pascal ORTIZ : *Exercices d'algèbre*. Ellipses, 2004.

[Per96] Daniel PERRIN : *Cours d'algèbre*. Ellipses, 1996.

[Pey04] Gabriel PEYRÉ : *L'algèbre discrète de la transformée de Fourier*. Ellipses, 2004.

[QZ13] Hervé QUEFFÉLEC et Claude ZUILY : *Analyse pour l'agrégation*. Dunod, quatrième édition, 2013.

[Rou09] François ROUVIÈRE : *Petit guide de calcul différentiel*. Cassini, troisième édition, 2009.

[Szp09] Aviva SZPIRGLAS : *Mathématiques L3 : Algèbre*. Pearson Education, 2009.

Chapitre 1

Développements d'Algèbre

1.1 Topologie des orbites de l'action de Steinitz

1.1.1 Développement

Proposition 1. *Soit* $\mathbb{K} = \mathbb{R}$ *ou* $\mathbb{C}$*, et soient* m *et* n *deux entiers. On note* $\mathcal{G} := \mathrm{GL}_m(\mathbb{K}) \times \mathrm{GL}_n(\mathbb{K})$*.*

L'application α *définie par*

$$\alpha : \begin{array}{ccc} \mathcal{G} \times \mathscr{M}_{m,n}(\mathbb{K}) & \longrightarrow & \mathscr{M}_{m,n}(\mathbb{K}) \\ ((P,Q),A) & \longmapsto & (P,Q)\cdot A = PAQ^{-1} \end{array}$$

est une action de groupe à gauche, appelée action de Steinitz.

Démonstration. Vérifions que les deux conditions pour que α définisse une action soient bien remplies. Soit $A \in \mathscr{M}_{m,n}(\mathbb{K})$ et soit $G = (P,Q) \in \mathcal{G}$ et $G' = (P',Q') \in \mathcal{G}$. On a que :

1. $(\mathrm{I}_m, \mathrm{I}_n)\cdot A = \mathrm{I}_m A \mathrm{I}_n^{-1} = \mathrm{I}_m A \mathrm{I}_n A = A$.
2. $G\cdot(G'\cdot A) = G\cdot(P'AQ'^{-1}) = PP'AQ'^{-1}Q^{-1} = (PP')A(QQ')^{-1} = (GG')\cdot A$.

Par conséquent α définit bien une action à gauche. □

Lemme 1. *Soit* $A \in \mathscr{M}_{m,n}(\mathbb{K})$*. L'orbite* $\mathcal{G}\cdot A$ *de* A *est l'ensemble des matrices de même rang que* A [1]*.*

1. Voir la partie *Questions classiques* pour les détails.

Démonstration.

$$\begin{aligned}\mathcal{G}\cdot A &= \{B \in \mathscr{M}_{m,n}(\mathbb{K}) \ ; \ \exists (P,Q) \in \mathcal{G} \text{ tq } B = PAQ^{-1}\}\\ &= \{B \in \mathscr{M}_{m,n}(\mathbb{K}) \ ; \ B \text{ est équivalente à } A\}\\ &= \{B \in \mathscr{M}_{m,n}(\mathbb{K}) \ ; \ \operatorname{rg} B = \operatorname{rg} A\}.\end{aligned}$$

□

Sachant que, pour $A \in \mathscr{M}_{m,n}(\mathbb{K})$, $\operatorname{rg} A \leq \min(m,n)$, on partitionne ainsi $\mathscr{M}_{m,n}(\mathbb{K})$ comme

$$\mathscr{M}_{m,n}(\mathbb{K}) = \biguplus_{0\leq k\leq \min(m,n)} \mathscr{O}_k.$$

On notera en particulier que

$$\mathrm{I}_{m,n,r} := \begin{pmatrix} \mathrm{I}_r & 0_{r,n-r} \\ 0_{m-r,r} & 0_{m-r,n-r}\end{pmatrix}$$

est un élément de $\mathscr{O}_r$ pour $r \leq \min(m,n)$.

Le résultat qui nous intéresse est le théorème principal suivant :

Théorème 1. *Soit m et n deux entiers et soit $r \leq \min(m,n)$. Alors*

$$\overline{\mathscr{O}_r} = \biguplus_{0\leq k\leq r} \mathscr{O}_k.$$

Avant de commencer la preuve, on rappelle la définition d'un mineur, ainsi que le théorème d'algèbre linéaire qui justifie l'introduction de cet objet :

Définition 1. Soit $A = (a_{ij})_{\substack{1\leq i\leq m\\ 1\leq j\leq n}} \in \mathscr{M}_{m,n}$. Si $I \subset \{1,...,m\}$, $J \subset \{1,...,n\}$ et $|I| = |J| = r$, le mineur d'indice (I,J) et d'ordre r est l'application

$$\Delta_{I,J} : \begin{array}{ccc} \mathscr{M}_{m,n}(\mathbb{K}) & \longrightarrow & \mathbb{K} \\ (a_{ij})_{\substack{1\leq i\leq m\\ 1\leq j\leq n}} & \longmapsto & \det(a_{ij})_{\substack{i\in I\\ j\in J}} \end{array}.$$

Théorème 2. *Soit $A \in \mathscr{M}_{m,n}(\mathbb{K})$. Alors*

$$\operatorname{rg} A = \max\{r \in \mathbb{N} \ ; \ \exists I \text{ tq } \exists J \text{ tq } |I| = |J| = r \text{ et } \Delta_{I,J} \neq 0\}.$$

Commençons maintenant la preuve du théorème principal, par double inclusion.

Démonstration. La première étape consiste à montrer que $\biguplus_{0\leq k\leq r}\mathscr{O}_k$ est un fermé de $\mathscr{M}_{m,n}(\mathbb{K})$, ce qui donne la première inclusion. On a d'après le théorème précédent que le rang d'une matrice A est au plus r si et seulement si tous ses mineurs d'ordres supérieurs ou égaux à $r+1$ sont nuls. Si l'on note $\widehat{\mathscr{O}_r} := \biguplus_{0\leq k\leq r}\mathscr{O}_k$, on a donc l'égalité

$$\widehat{\mathscr{O}_r} = \cap_{|I|=|J|\geq r+1}\Delta_{I,J}^{-1}(\{0\}).$$

Les fonctions $\Delta_{I,J}$ étant continues, la partie $\widehat{\mathscr{O}_r}$ est fermée en tant qu'intersection de fermés. On a alors $\overline{\mathscr{O}_r}\subset\overline{\widehat{\mathscr{O}_r}} = \widehat{\mathscr{O}_r}$.

Soit à présent $A\in\mathscr{M}_{m,n}(\mathbb{K})$ une matrice de rang $k\leq r$. On a l'existence de $(P,Q)\in\mathcal{G}$ telles que $A = P\mathrm{I}_{m,n,k}Q^{-1}$. On définit alors la suite de matrices par blocs suivante : pour un entier $l\in\mathbb{N}^*$, on pose

$$A_l := P\begin{pmatrix}\mathrm{I}_k & 0 & 0\\ 0 & \frac{1}{l}\mathrm{I}_{r-k} & 0\\ 0 & 0 & 0\end{pmatrix}Q^{-1}.$$

Pour tout entier $l\in\mathbb{N}^*$ on a que $\operatorname{rg}A_l = r$, et on vérifie que $A_n \underset{l\to+\infty}{\longrightarrow} A$. Par conséquent $A\in\overline{\mathscr{O}_r}$, et comme A était choisie quelconque dans $\widehat{\mathscr{O}_r}$, on a $\widehat{\mathscr{O}_r}\subset\overline{\mathscr{O}_r}$. □

Corollaire 1. *1. L'unique orbite fermée est l'orbite de la matrice nulle, dite "minimale" : $\mathscr{O}_0 = \{0\}$.*

2. L'unique orbite ouverte est l'orbite dite "maximale" : $\mathscr{O}_{\min(m,n)}$. En particulier, si $m=n$, alors le groupe des matrices inversibles est ouvert dans $\mathscr{M}_{m,n}(\mathbb{K})$.

Démonstration. 1. D'après le théorème précédent, $\overline{\mathscr{O}_0} = \biguplus_{0\leq k\leq 0}\mathscr{O}_k = \mathscr{O}_0$.

2. Supposons pour commencer que $k<\min(m,n)$ et montrons que $\mathscr{O}_k$ n'est pas ouverte, en montrant que $\mathrm{I}_{m,n,k}\notin\mathring{\mathscr{O}}_k$. On travaillera avec la norme $|||A||| = \max\limits_{\substack{1\leq i\leq m\\ 1\leq j\leq n}}|a_{ij}|$. Soit $\varepsilon>0$ quelconque. En posant

$$B_\varepsilon = \begin{pmatrix}\mathrm{I}_k & 0\\ 0 & \frac{\varepsilon}{2}\mathrm{I}_{m-k,n-k,m-k}\end{pmatrix},$$

on a que $|||B_\varepsilon - \mathrm{I}_{m,n,k}||| = \frac{\varepsilon}{2}$ d'où $B_\varepsilon\in B(\mathrm{I}_{m,n,k},\varepsilon)$, mais $B_\varepsilon\notin\mathscr{O}_k$ car $\operatorname{rg}B_\varepsilon = min(m,n)$.

Supposons maintenant que $k = \min(m,n)$ et montrons que $\mathscr{O}_k$ est ouverte. On remarque déjà que, pour $I = J = \{1,...,k\}$, on a $\Delta_{I,J}(\mathrm{I}_{m,n,k}) = 1 \neq 0$. Par continuité de $\Delta_{I,J}$, il existe donc un voisinage U de $\mathrm{I}_{m,n,k}$ tel que $\Delta_{I,J}$ ne s'annule pas sur U. Les matrices appartenant à U étant au moins de rang k et au plus de rang k, on a $U \subset \mathscr{O}_k$. Pour $A \in \mathscr{O}_k$, on remarque qu'il existe $(P,Q) \in G$ telles que $A = P\mathrm{I}_{m,n,k}Q^{-1}$. L'application

$$\phi_{P,Q} : \begin{array}{ccc} \mathscr{O}_k & \longrightarrow & \mathscr{O}_k \\ M & \longmapsto & PMQ^{-1} \end{array}$$

étant clairement un homéomorphisme, il vient que $\phi_{P,Q}(U)$ est un voisinage de A dans $\mathscr{O}_k$.

□

Application 1. $\mathrm{GL}_n(\mathbb{K})$ est dense dans $\mathscr{M}_n(\mathbb{K})$.

Démonstration. $\overline{\mathrm{GL}_n(\mathbb{K})} = \overline{\mathscr{O}_n} = \biguplus_{0\leq k\leq n} \mathscr{O}_k = \mathscr{M}_{m,n}(\mathbb{K})$. □

1.1.2 Références

[CG13], pp. 9-11.

1.1.3 Questions classiques

1. *Montrer que deux matrices sont équivalentes si et seulement si elles ont le même rang* : L'implication est immédiate car multiplier par une matrice inversible à gauche et à droite ne change pas le rang d'une matrice. La réciproque se prouve en montrant que toute matrice A de rang r est équivalente à $\mathrm{I}_{m,n,k}$. On procède en appliquant le théorème du rang à A ($\dim\ker A = m - r$), puis en prenant une base $(e_{m-r+1},...,e_m)$ du noyau de A, en la complétant en une base par des vecteurs $(e_1,...,e_r)$. La base à l'arrivée qui donne la forme matricielle attendue est alors $(Ae_1,...,Ae_r)$ (libre car A est injective sur l'espace engendré par les $(e_1,...,e_r)$) complétée en une base quelconque.
2. *Montrer que les mineurs sont des applications continues* : Le mineur est la composée du déterminant avec une restriction de l'identité, et ces deux dernières fonctions étant continues car polynomiales on obtient notre résultat.

1.1.4 Remarques

— Ernst Steinitz : mathématicien allemand, 1871-1928

1.2 Théorème de Burnside

1.2.1 Développement

Définition 2. Un groupe G est dit d'indice fini s'il existe un entier n tel que, pour tout élément g de G, on a $g^n = e$.

Théorème 3 (Théorème de Burnside)**.** *Soit G un sous-groupe de $\mathrm{GL}_n(\mathbb{C})$.*
G est fini si et seulement si G est d'indice fini.

La démonstration se fait en quatre étapes : trois lemmes et le théorème qui nous intéresse.

Commençons par démontrer le lemme suivant :

Lemme 2. *Soit $A \in \mathscr{M}_n(\mathbb{C})$ telle que pour tout $k \in \mathbb{N}^*$ on a $\mathrm{Tr}(A^k) = 0$. Alors A est nilpotente.*

Démonstration. Supposons par l'absurde que A ne soit pas nilpotente. Cela revient à dire que le polynôme caractéristique de A (scindé car nous sommes sur $\mathbb{C}$) admet des racines non-nulles. Notons $\lambda_1, ..., \lambda_r$ ces racines et $n_1, ..., n_r$ leur multiplicité. On sait qu'alors A est semblable à une matrice triangulaire où sur la diagonale apparait n_i fois λ_i. Pour $k \in \mathbb{N}^*$, en élevant cette matrice à la puissance k-ième, on a que

$$\mathrm{Tr}(A^k) = n_1\lambda_1^k + ... + n_r\lambda_r^k = 0.$$

En mettant ce résultat sous forme matricielle pour k variant de 1 à r, on a l'égalité

$$\begin{pmatrix} \lambda_1 & \lambda_2 & \dots & \lambda_r \\ \lambda_1^2 & \lambda_2^2 & \dots & \lambda_r^2 \\ \vdots & \vdots & & \vdots \\ \lambda_1^r & \lambda_2^r & \dots & \lambda_r^r \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_r \end{pmatrix} = 0.$$

Cette matrice est inversible car son déterminant vaut

$$\lambda_1 \dots \lambda_r \prod_{1 \le i < j \le r} (\lambda_j - \lambda_i) \neq 0$$

par la formule de Vandermonde. Par conséquent $n_1 = ... = n_r = 0$, ce qui est contradictoire. □

Il s'agit à présent de prouver que :

Lemme 3. *Soit G un sous-groupe de $\mathrm{GL}_n(\mathbb{C})$, $(M_i)_{1\leq i\leq m} \in G^m$ une base de $\mathrm{vect}(G)$ et $f : G \to \mathbb{C}^m$ l'application qui à $A \in G$ associe $(\mathrm{Tr}(AM_i))_{1\leq i\leq m}$. On a l'implication*

$$f(A) = f(B) \Longrightarrow AB^{-1} - \mathrm{I}_n \text{ est nilpotente.}$$

Démonstration. Soient A et B deux matrices de G. Supposons que $f(A) = f(B)$. Par linéarité de la trace, on a que $\mathrm{Tr}(AM) = \mathrm{Tr}(BM)$ pour toute matrice $M \in \mathrm{vect}(G)$, en particulier cette égalité reste valable pour $M \in G$. Posons $D = AB^{-1}$. Cette matrice est dans G, donc pour tout $k \in \mathbb{N}^*$, on a que

$$\mathrm{Tr}(D^k) = \mathrm{Tr}(AB^{-1}D^{k-1}) = \mathrm{Tr}(BB^{-1}D^{k-1}) = \mathrm{Tr}(D^{k-1}).$$

Une récurrence immédiate donne que, pour tout $k \in \mathbb{N}$, $\mathrm{Tr}(D^k) = \mathrm{Tr}(\mathrm{I}_n) = n$. Ainsi, pour tout $k \in \mathbb{N}^*$,

$$\mathrm{Tr}(D - \mathrm{I}_n)^k = \mathrm{Tr}\Big(\sum_{j=0}^{k} \binom{k}{j} (-1)^j D^{k-j}\Big) = n \sum_{j=0}^{k} \binom{k}{j} (-1)^j = n(1-1)^k = 0.$$

On conclut grâce au lemme précédent. □

Le dernier lemme est :

Lemme 4. *Avec les notations du lemme précédent, on suppose de plus que toutes les matrices de G sont diagonalisables. Alors f est injective.*

Démonstration. Supposons que $f(A) = f(B)$. Le lemme précédent assure que $AB^{-1} - \mathrm{I}_n$ est nilpotente. Or, comme AB^{-1} est dans G, elle est diagonalisable. Mais alors $AB^{-1} - \mathrm{I}_n$ est encore diagonalisable, et la seule matrice diagonalisable et nilpotente étant la matrice nulle, il vient que $AB^{-1} = \mathrm{I}_n$ et par conséquent $A = B$. □

On démontre enfin notre théorème.

Démonstration. Soit G un sous-groupe de $\mathrm{GL}_n(\mathbb{C})$.

- ($\Rightarrow$) Supposons que G est fini d'ordre N. Alors le théorème de Lagrange assure que tout élément A de G vérifie que $A^N = \mathrm{I}_n$, et ainsi G est d'indice fini.
- ($\Leftarrow$) Supposons que G soit d'indice fini N. Toute matrice A de G est annulée par le polynôme $X^N - 1 = \prod_{1\leq k\leq N}(X - e^{\frac{2i\pi k}{N}})$ qui est scindé à racines simples, et est donc diagonalisable. On applique le lemme précédent qui nous donne l'injectivité de $f : G \to \mathbb{C}^m$. On remarque que $f(G) \subset T^m$,

où T est l'ensemble des traces des éléments de G. Or les éléments de T sont des sommes de n termes choisi dans les racines N-ièmes de l'unité, on en dénombre donc au plus N^n. Par injectivité de f, on a finalement que $|G| \leq (N^n)^m$.

□

1.2.2 Références

[FGN09], pp. 111, 185-186.

1.2.3 Questions classiques

1. *Calculer le déterminant d'une matrice de Vandermonde* : Soit

$$V(\lambda_1, \lambda_2, ..., \lambda_n) = \begin{pmatrix} 1 & \lambda_1 & \lambda_1^2 & \dots & \lambda_1^{n-1} \\ 1 & \lambda_2 & \lambda_2^2 & \dots & \lambda_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \lambda_n & \lambda_n^2 & \dots & \lambda_n^{n-1} \end{pmatrix}$$

une matrice de Vandermonde. On a tout d'abord en remplaçant chaque colonne C_k par $C_k - \lambda_1 C_{k-1}$ (avec k allant de n à 2) que

$$\det(V(\lambda_1, \lambda_2, ..., \lambda_n)) = \begin{vmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & \lambda_2 - \lambda_1 & \lambda_2^2 - \lambda_1\lambda_2 & \dots & \lambda_2^{n-1} - \lambda_1\lambda_2^{n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \lambda_n - \lambda_1 & \lambda_n^2 - \lambda_1\lambda_n & \dots & \lambda_n^{n-1} - \lambda_1\lambda_n^{n-2} \end{vmatrix}.$$

En développant par rapport à la première ligne, puis en mettant en facteur $(\lambda_k - \lambda_1)$ sur chaque ligne, on obtient que

$$\begin{aligned} \det(V(\lambda_1, \lambda_2, ..., \lambda_n)) &= \begin{vmatrix} \lambda_2 - \lambda_1 & \lambda_2^2 - \lambda_1\lambda_2 & \dots & \lambda_2^{n-1} - \lambda_1\lambda_2^{n-2} \\ \vdots & \vdots & & \vdots \\ \lambda_n - \lambda_1 & \lambda_n^2 - \lambda_1\lambda_n & \dots & \lambda_n^{n-1} - \lambda_1\lambda_n^{n-2} \end{vmatrix} \\ &= \prod_{2 \leq k \leq n} (\lambda_k - \lambda_1) \times \begin{vmatrix} 1 & \lambda_2 & \dots & \lambda_2^{n-2} \\ \vdots & \vdots & & \vdots \\ 1 & \lambda_n & \dots & \lambda_n^{n-2} \end{vmatrix} \\ &= \prod_{2 \leq k \leq n} (\lambda_k - \lambda_1) \times \det(V(\lambda_2, ..., \lambda_n)). \end{aligned}$$

Il suffit de voir que $\det(V(\lambda_n)) = 1$ pour obtenir par récurrence la formule

$$\det(V(\lambda_1, ..., \lambda_n)) = \prod_{1 \leq i < j \leq n} (\lambda_j - \lambda_i).$$

1.2.4 Remarques

— William Burnside : mathématicien anglais, 1852-1927

— Alexandre-Théophile Vandermonde : mathématicien français, 1735-1796

1.3 Automorphismes de $\mathfrak{S}_n$

1.3.1 Développement

Théorème 4. *Soit $n \in \mathbb{N}^*$, $n \neq 6$. Alors les automorphismes de $\mathfrak{S}_n$ sont les automorphismes intérieurs, i.e. de la forme $s \mapsto \sigma \circ s \circ \sigma^{-1}$, où $\sigma \in \mathfrak{S}_n$.*

Le résultat est trivial pour $n = 1, 2$, on ne s'intéresse vraiment qu'au cas $n \geq 3$. On va avoir besoin de deux lemmes pour démontrer ce résultat, que nous donnons ci-après[2] :

Lemme 5. *Les transpositions $(1\,2), (1\,3), \ldots, (1\,n)$ engendrent $\mathfrak{S}_n$.*

Lemme 6. *Soit $\sigma \in \mathfrak{S}_n$ et $(a_1 \ \ldots \ a_k)$ un $k-$cycle. Alors*

$$\sigma(a_1 \ \ldots \ a_k)\sigma^{-1} = \big(\sigma(a_1)\,\sigma(a_2) \ \ldots \ \sigma(a_k)\big).$$

On remarque que le lemme précédent donne en particulier que, pour $s \in \mathfrak{S}_n$ et $s_1, s_2 \ldots, s_k$ les cycles disjoints de sa décomposition $s = s_1 s_2 \ldots s_k$, on obtient que $\sigma s \sigma^{-1} = (\sigma s_1 \sigma^{-1})(\sigma s_2 \sigma^{-1}) \ldots (\sigma s_k \sigma^{-1})$, et donc la décomposition de $\sigma s \sigma^{-1}$ en produit de cycles à supports disjoints.

Commence alors la preuve du théorème :

Démonstration. Commençons par montrer qu'un automorphisme φ transforme toute transposition en une transposition, en remarquant que si τ est une transposition alors $\varphi(\tau)$ est d'ordre 2 mais n'a *a priori* aucune raison d'être une transposition (considérer par exemple $(1\,2)(3\,4)$ dans $\mathfrak{S}_4$). On note T_k l'ensemble des permutations de $\mathfrak{S}_n$ qui sont produits de k transpositions à support disjoints, avec $2k \leq n$, seules cibles pour $\varphi(\tau)$ (l'ordre d'une permutation étant le ppcm des longueurs de ses supports dans son écriture en cycles à supports disjoints). On remarque que T_1 est l'ensemble des transpositions et que $\varphi(T_1)$ est l'un des T_k : en effet le lemme assure que les T_k sont des classes de conjugaison, et la relation $\varphi(\sigma\tau\sigma^{-1}) = \varphi(\sigma)\varphi(\tau)\varphi(\sigma)^{-1}$ assure que φ envoie une classe de conjugaison sur une classe de conjugaison (car la classe de conjugaison de σ est envoyé dans la classe de conjugaison de $\varphi(\sigma)$, et $s\varphi(\sigma)s^{-1}$ est atteint par $\varphi^{-1}(s)\sigma\varphi^{-1}(s)^{-1}$, qui est bien dans la classe de conjugaison de σ). On a alors

$$|T_1| = \binom{n}{2} = \frac{n(n-1)}{2}$$

2. On donne les démonstrations dans la partie *Questions classiques* mais on ne les fait pas à l'oral pour gagner du temps.

et

$$|T_k| = \frac{\binom{n}{2}\binom{n-2}{2}\dots\binom{n-2k+2}{2}}{k!} = \frac{n(n-1)\dots(n-2k+1)}{2^k k!},$$

dénombrements que l'on obtient en choisissant les supports des transpositions sans tenir compte de leur ordre. Montrons que nécessairement $k = 1$: comme on a égalité entre ces cardinaux, il vient

$$2^{k-1}k! = (n-2)\dots(n-2k+1).$$

Pour $k = 2$ on aurait ainsi

$$4 = (n-2)(n-3)$$

qui n'admet pas de solutions entières, et pour $k \geq 3$ il vient

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

qui implique forcément $n-2 = n-k+1$, sans quoi le terme à droite contiendrait un facteur impair. Alors $k = 3$ et

$$4 = (n-2)\binom{n-3}{3} \iff 24 = (n-2)(n-3)(n-4)(n-5)$$

qui implique que $n = 6$. Ce cas-là étant exclu on a forcément $\varphi(T_1) = T_1$.

Reste à voir qu'il existe $\alpha \in \mathfrak{S}_n$ tel que pour toute transposition $\tau = (1\,a_i)$ on ait $\varphi(\tau) = \alpha\tau\alpha^{-1}$, le premier lemme nous donnant alors la conclusion. On remarque que comme $(1\,2)$ et $(1\,3)$ ne commutent pas lorsque $i \neq j$, il en est de même de $\varphi(1\,2)$ et $\varphi(1\,3)$: leurs supports ne sont donc pas disjoints, et possèdent donc un élément commun a_1. On écrit $\varphi(1\,2) = (a_1\,a_2)$ et $\varphi(1\,3) = (a_1\,a_3)$, avec $a_2 \neq a_3$ par injectivité de φ. Montrons par récurrence sur $i \in \{2,\dots,n\}$ que $\varphi(1\,i)$ s'écrit $(a_1\,a_i)$ avec $a_i \neq a_k$ lorsque $k < i$. On vient de voir que c'était vrai pour $i = 2, 3$. Supposons maintenant $i \geq 4$. On a que $\varphi(1\,i)$ rencontre le support de $\varphi(1\,a_k)$ pour $2 \leq k \leq i-1$ par hypothèse de récurrence. Si a_1 n'était pas dans le support de $\varphi(1\,a_i)$, ceci implique que $i = 4$ (sinon le support de $\varphi(1\,i)$ contiendrait a_2, a_3 et a_4, ce qui est impossible). On a a lors nécessairement

$$\varphi(1\,4) = (a_2\,a_3) = (a_1\,a_3)(a_2\,a_1)(a_1\,a_3) = \varphi\big((1\,3)(1\,2)(1\,3)\big) = \varphi(2\,3)$$

et donc $(1\,4) = (2\,3)$ d'où la contradiction. On écrit alors $\varphi(1\,i) = (a_1\,a_i)$ avec a_i distinct des a_k par injectivité de φ. En considérant finalement la permutation $\alpha \in \mathfrak{S}_n$ définie par $\alpha(i) = a_i$, on a $\varphi(1\,i) = (a_1\,a_i) = \alpha(1\,i)\alpha^{-1}$ d'où le théorème. □

1.3.2 Références

[FGN14a], pp. 74-77.

1.3.3 Questions classiques

1. *Donnez la démonstration des deux lemmes* :

   Preuve du premier :

   Démonstration. On procède par récurrence sur n. Pour $n = 2$, il est évident que $(1\,2)$ engendre $\mathfrak{S}_2$. Pour $n \geq 2$ et $\sigma \in \mathfrak{S}_{n+1}$, on a deux alternatives :
   (a) soit $\sigma(n+1) = n+1$ auquel cas $\sigma|_{\{1,\dots,n\}} \in \mathfrak{S}_n$ et on conclut par hypothèse de récurrence,
   (b) soit $\sigma(n+1) = j$ avec $j \in \{1,\dots,n\}$ et alors on conclut en posant $\sigma' = (1\,n+1)(1\,j)\sigma$ et en remarquant que $\sigma'(n+1) = n+1$.

   □

   Preuve du second :

   Démonstration. Si $x \notin \{\sigma(a_1),\dots,\sigma(a_k)\}$ on a que $\sigma^{-1}(x) \notin \{a_1,\dots,a_k\}$ et donc
   $$\sigma(a_1 \dots a_k)\sigma^{-1}(x) = \sigma\sigma^{-1}(x) = x.$$
   Si $x = \sigma(a_i)$, alors
   $$\sigma(a_1 \dots a_k)\sigma^{-1}(x) = \sigma(a_{i+1})$$
   où l'on a pris les indices modulo k. □

2. *Évoquez ce qu'il se passe-t-il lorsque $n = 6$* : On constate que les automorphismes ne sont plus exclusivement intérieurs. En effet, on peut vérifier qu'on compte 1440 automorphismes pour seulement 720 automorphismes intérieurs.

1.3.4 Remarques

— Le développement peut paraître long, mais il est ici relativement détaillé et il n'y a pas tant de choses à écrire au tableau.

1.4 Un anneau principal et non-euclidien

1.4.1 Développement

Le résultat consiste à exhiber le contre-exemple suivant :

Théorème 5. *L'anneau* $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ *est principal et non-euclidien.*

Commençons par montrer qu'il n'est pas euclidien. On a la proposition suivante :

Proposition 2. *Soit* A *un anneau euclidien, de stathme* v*. Il existe* $x \in A \setminus A^\times$ *tel que la restriction à* $A^\times \cup \{0\}$ *de la projection canonique de* $\pi : A \to A/(x)$ *soit surjective.*

Démonstration. Si A est un corps, 0 convient. Sinon, on a que $\{v(x)\ ;\ x \in A \setminus (A^\times \cup \{0\})\}$ est une partie non-vide de $\mathbb{N}$, on choisit alors un $x \in A$ tel que $v(x)$ minimise cet ensemble. Pour $a \in A$ on a l'écriture $a = xq + r$ avec $r = 0$ ou $v(r) < v(x)$. Mais, si r est différent de 0, il vient que r est inversible sans quoi on aurait $v(r) \geq v(x)$. Dans tous les cas on a que a est bien égal modulo x à 0 ou à un élément de $A^\times$. □

On remarque dès à présent que, l'image d'un inversible par la projection canonique étant un inversible, on a que $A/(x)$ est un corps. On donne un exemple pour se familiariser avec la proposition : dans $\mathbb{Z}$, on a $\mathbb{Z}^\times \cup \{0\} = \{-1, 0, 1\}$ et on peut prendre $x = 2$ ou $x = 3$.

Corollaire 2. *L'anneau* $A := \mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ *n'est pas euclidien.*

Démonstration. On a que $\alpha := \frac{1+i\sqrt{19}}{2}$ vérifie l'équation

$$\alpha^2 - \alpha + 5 = 0$$

via le fait que $\alpha + \overline{\alpha} = 1$ et $\alpha\overline{\alpha} = 5$[3]. La proposition précédente nous invite à calculer les inversibles de $A = \{a + b\alpha\ ;\ a, b \in \mathbb{Z}\}$, ce que l'on va faire à l'aide de l'application $N(z) = z\overline{z} = a^2 + ab + 5b^2$ qui vérifie $N(z) \in \mathbb{N}, N(zz') = N(z)N(z')$ et $N(z) > 0$ pour $z > 0$. En effet, comme on doit avoir $N(zz^{-1}) = N(z)N(z^{-1}) = 1$ dans $\mathbb{N}$, le seul choix possible reste $N(z) = a^2 + ab + 5b^2 = 1$. Or, les inégalités

$$b^2 + a^2 + ab \geq b^2 + a^2 - |ab| \geq (|b| - |a|)^2 \geq 0$$

3. I.e. via la relation entre coefficients et racines.

impliquent que l'on doit avoir $1 = a^2 + ab + 5b^2 \geq 4b^2$, ce qui donne $b = 0$ et $a = \pm 1$. Réciproquement, ces valeurs conviennent et finalement $A^\times = \{-1, 1\}$ [4]. Si l'anneau était euclidien, on aurait par la proposition un $x \in A$ tel que $A/(x)$ soit un corps à 2 ou 3 éléments, et un morphisme surjectif $\varphi : A \to \mathbb{F}_p$ avec $p = 2$ ou 3 (par unicité des corps finis). La restriction de φ à $\mathbb{Z}$ est la projection canonique de $\mathbb{Z}$ sur $\mathbb{F}_2$ ou $\mathbb{F}_3$: elle est en effet entièrement caractérisée par le fait que

$$\varphi(n) = \varphi(n \cdot 1) = n \cdot \varphi(1) = n \cdot \overline{1} = \overline{n}.$$

Appliqué à notre équation, on aurait alors en notant $\beta := \varphi(\alpha)$ que $\beta^2 - \beta + 5 = 0$ dans $\mathbb{F}_2$ ou $\mathbb{F}_3$. Or on vérifie rapidement que cette équation n'a pas de solution, ce qui constitue une contradiction. □

Montrons maintenant que notre anneau est principal. On va utiliser la proposition suivante :

Proposition 3 (pseudo division euclidienne)**.** *Soient $a, b \in A^*$. Alors il existe $q, r \in A$ tels que :*

1. *$r = 0$ ou $N(r) < N(b)$,*
2. *$a = bq + r$ ou $2a = bq + r$.*

Démonstration. Soit $x = \frac{a}{b} = \frac{a\overline{b}}{b\overline{b}} \in \mathbb{C}$, que l'on peut alors écrire $x = u + v\alpha$, avec $u, v \in \mathbb{Q}$. On note $n = \lfloor v \rfloor$ la partie entière de v : on a donc $v \in [n, n+1[$.

1. Supposons que $v \notin]n + \frac{1}{3}, n + \frac{2}{3}[$, et soient alors s et t les entiers les plus proches de u et v respectivement. On a $|s - u| \leq \frac{1}{2}$ et $|t - v| \leq \frac{1}{3}$. On pose alors $q = s + t\alpha \in A$ et on vérifie que :

$$N(x - q) = (s-u)^2 + (s-u)(t-v) + 5(t-v)^2 \leq \frac{1}{4} + \frac{1}{6} + \frac{5}{9} = \frac{35}{36} < 1.$$

   Si on pose $r = a - bq = b(x - q)$, on a bien $N(r) < N(q)$ et le résultat voulu.

2. Supposons que $v \in]n + \frac{1}{3}, n + \frac{2}{3}[$. On considère $2x = 2u + 2v\alpha$, et on a $2v \in]2n + \frac{2}{3}, 2n + 1 + \frac{1}{3}[$. Si $m = \lfloor 2v \rfloor$, on a $2v \notin]m + \frac{1}{3}, m + \frac{2}{3}[$ [5] et on est ramenés au cas précédent et on a $2a = bq + r$, avec $N(r) < N(b)$, ce qui prouve la proposition.

□

Corollaire 3. *L'anneau A est principal.*

4. On pourra admettre cette partie facile dans le but de gagner du temps.
5. Faire un dessin !

Démonstration. 1. Montrons que (2) est maximal dans A : on remarque que $A \simeq \mathbb{Z}[T]/(T^2 - T + 5)$ (comme on le voit par division euclidienne et à l'aide du premier théorème d'isomorphisme), et le second théorème d'isomorphisme donne alors

$$A/(2) \simeq \mathbb{Z}[T]/(2, T^2 - T + 5) \simeq (\mathbb{Z}/2\mathbb{Z})[T]/(T^2 + T + 1),$$

où l'on a utilisé le fait que si $P = p \in A$, alors on a $A[X]/(p) \simeq A/(p)[X]$. Or $T^2 + T + 1$ est irréductible sur $\mathbb{F}_2$, ce qui équivaut dans l'anneau principal (car euclidien) $(\mathbb{Z}/2\mathbb{Z})[X]$ au fait que l'idéal $(T^2 + T + 1)$ soit maximal : finalement, (2) est maximal dans A.

2. Soit $I \neq \{0\}$ un idéal de A et soit $a \in I, a \neq 0$, tel que $N(a)$ soit minimal. Si $I = (a)$, on a terminé, sinon soit $x \in I \setminus (a)$. On effectue la pseudo division euclidienne de x par a :
   (a) Si $x = aq + r$ avec $N(r) < N(a)$ ou $r = 0$, comme $r = x - aq \in I$, on a $r = 0$, donc $x \in (a)$ est c'est une contradiction.
   (b) On a donc $2x = aq + r$ avec $N(r) < N(a)$ ou $r = 0$, et pour la même raison que précédemment, $r = 0$ et $2x = aq$.

   Comme (2) est maximal, donc premier, on doit avoir $a \in (2)$ ou $q \in (2)$. Si $q \in (2)$, alors $q = 2q'$ et $x \in (a)$, contradiction. Donc $q \notin (2)$ et $a \in (2)$, $a = 2a'$ d'où $x = a'q \in (a')$. Il suffit pour conclure de montrer que a' est dans I, car cela contredira la minimalité de $N(a)$ (puisque $a = 2a'$). Comme (2) est maximal et ne contient pas q, $(2, q)$ est égal à A tout entier. On a une relation de Bézout : $\lambda 2 + \mu q = 1$, avec $\lambda, \mu \in A$. On en déduit $a' = \lambda 2a' + \mu q a' = \lambda a + \mu x \in I$ et on a fini.

□

1.4.2 Références

[Per96], pp. 53-55.

1.4.3 Questions classiques

1.

1.4.4 Remarques

— On pourra sauter la construction de la pseudo division euclidienne, à condition de bien mentionner que c'est ici que l'on comprend le choix bizarre de α.

— Ce développement joker est particulièrement long, il faut extrêmement bien le préparer et maîtriser tous les résultats invoqués !

1.5 Théorème des deux carrés

1.5.1 Développement

On cherche à expliciter l'ensemble $\Sigma = \{n \in \mathbb{N} \ ; \ n = a^2 + b^2, a, b \in \mathbb{N}\}$. Le résultat est le suivant :

Théorème 6 (Théorème des deux carrés)**.** *Soit $p \in \mathbb{N}$ un nombre premier impair On a l'équivalence suivante :*

$$p \in \Sigma \iff p \equiv 1 \mod 4.$$

L'idée est de remarquer que $n = a^2 + b^2$ s'écrit $n = (a + ib)(a - ib)$, relation qui a lieu dans l'anneau $\mathbb{Z}[i] = \{a + ib \ ; \ a, b \in \mathbb{Z}\}$ des entiers de Gauss. Commençons par dégager quelques propriétés de cet anneau : il est intègre en tant que sous-anneau de $\mathbb{C}$, muni d'un automorphisme donné par la restriction de la conjugaison complexe $\sigma(z) = \bar{z} = a - ib$, et possède une "norme" N définie par $N(z) = z\bar{z} = a^2 + b^2 \in \mathbb{N}$. On a de plus $N(zz') = N(z)N(z')$. Listons à présent des résultats qui vont nous permettre de démontrer le théorème :

Proposition 4. *On a que $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.*

Démonstration. Si $z \in \mathbb{Z}[i]^\times$, alors il existe $z' \in \mathbb{Z}[i]$ tel que $zz' = 1$, et donc $N(z)N(z') = 1$. On a forcément $N(z) = a^2 + b^2 = 1$, et finalement $z \in \{\pm 1, \pm i\}$. L'inclusion réciproque est immédiate. □

Proposition 5. *L'ensemble Σ est stable par multiplication.*

Démonstration. On traduit la propriété $n \in \Sigma$ en termes d'entiers de Gauss :

$$n \in \Sigma \iff \exists z \in \mathbb{Z}[i] \text{ tq } N(z) = n.$$

Ainsi, si $n, n' \in \Sigma$, on a $n = N(z)$ et $n' = N(z')$ et alors $nn' = N(zz') \in \Sigma$ (c'est en fait l'identité de Lagrange : $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$). □

On ramène ainsi essentiellement l'étude de Σ à la détermination des nombres premiers p qui sont dans Σ. Pour cela, on détaille la structure arithmétique de $\mathbb{Z}[i]$:

Proposition 6. *L'anneau $\mathbb{Z}[i]$ est euclidien pour le stathme N, donc principal.*

Démonstration. Soit $z \in \mathbb{Z}[i]$ et $t \in \mathbb{Z}[i]^*$. On a que $\frac{z}{t} = x + iy$, avec $x, y \in \mathbb{R}$. On choisit $a, b \in \mathbb{N}$ tels que $|x - a| \leq \frac{1}{2}$ et $|y - b| \leq \frac{1}{2}$. On a alors en posant $q = a + ib$ que

$$\left|\frac{z}{t} - q\right| \leq \frac{\sqrt{2}}{2} < 1.$$

On pose alors $r = z - qt \in \mathbb{Z}[i]$ (car $z, q, t \in \mathbb{Z}[i]$), qui vérifie $r = t(\frac{z}{t} - q)$ et ainsi $|r| = |t|\,|\frac{z}{t} - q| < |t|$. En élevant au carré, on a finalement écrit $z = tq + r$ avec $N(r) < N(t)$. □

Il reste un dernier lemme avant de commencer la preuve du théorème :

Lemme 7. *On a l'équivalence (pour p premier) :*

$$p \in \Sigma \iff p \text{ n'est pas irréductible dans } \mathbb{Z}[i].$$

Démonstration. $\implies$ Si $p = a^2 + b^2$, alors on écrit $p = (a + ib)(a - ib)$ et comme $a, b \neq 0$ on a que ni $(a + ib)$ ni $(a - ib)$ n'est inversible et donc z n'est pas irréductible.

$\impliedby$ On écrit $p = zz'$ avec $z, z' \notin \{\pm 1, \pm i\}$ et alors $N(p) = N(z)N(z') = p^2$. Comme p est premier et que $N(z), N(z') \neq 1$, on a forcément $N(z) = p$ et ainsi $p \in \Sigma$.

□

Démontrons maintenant le théorème :

Démonstration. On voit facilement que la condition $p \equiv 1 \mod 4$ est nécessaire, car on a que $a^2 \equiv 0, 1 \mod 4$ d'où $p = a^2 + b^2 \equiv 0, 1, 2 \mod 4$ et comme p est premier impair on ne peut avoir $p \equiv 0, 2 \mod 4$. De manière plus générale, on peut raisonner par équivalences [6] et voir que comme $\mathbb{Z}[i]$ est factoriel, p n'est pas irréductible dans $\mathbb{Z}[i]$ si et seulement si p n'est pas premier dans $\mathbb{Z}[i]$, i.e. si et seulement si $\mathbb{Z}[i]/(p)$ n'est pas intègre. De plus, comme on a l'isomorphisme $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2 + 1)$, on a que

$$\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[X]/(X^2 + 1, p) \simeq \big(\mathbb{Z}[X]/(p)\big)/(X^2 + 1) \simeq \mathbb{Z}/p\mathbb{Z}[X]/(X^2 + 1)$$

via les théorèmes d'isomorphismes. On a donc que p n'est pas irréductible dans $\mathbb{Z}[i]$ si et seulement si $X^2 + 1$ n'est pas irréductible dans $\mathbb{Z}/p\mathbb{Z}$, ce qui équivaut encore à dire que $X^2 + 1$ admet une racine dans $\mathbb{Z}/p\mathbb{Z}$, i.e. -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$. Reste à prouver que ceci arrive si et seulement si $p \equiv 1 \mod 4$:

Lemme 8. *Si $q = p^n$ avec $p > 2$, alors $x \in \mathbb{F}_q^{*2} \iff x^{\frac{q-1}{2}} = 1$ et $-1 \in \mathbb{F}_q^{*2} \iff q \equiv 1 \mod 4$.*

Démonstration du lemme. On pose $X = \{x \in \mathbb{F}_q \ ; \ x^{\frac{q-1}{2}} = 1\}$. On a $|X| \leq \frac{q-1}{2}$ (un polynôme de degré $\frac{q-1}{2}$ a au plus $\frac{q-1}{2}$ racines). D'autre part, si $x \in \mathbb{F}_q^{*2}$, on

6. Merci David.

a $x = y^2$ donc $x^{\frac{q-1}{2}} = y^{q-1} = 1$ par le théorème de Lagrange, et donc $\mathbb{F}_q^{*2} \subset X$. Par cardinalité[7], on obtient $X = \mathbb{F}_q^{*2}$. De ce résultat découle

$$-1 \in \mathbb{F}_q^{2*} \iff (-1)^{\frac{q-1}{2}} = 1 \iff \frac{q-1}{2} \text{ est pair } \iff q \equiv 1 \mod 4.$$

□

On a ce que l'on avait anoncé. □

1.5.2 Références

[Per96], pp. 56-58, p. 75.

1.5.3 Questions classiques

1. *Comment vous occupez-vous du cas n quelconque* : On décompose n en produit de facteurs premiers : $n = \prod_{p \in \mathcal{P}} p^{\nu_p(n)}$ où $\mathcal{P} = \{\text{nombres premiers}\}$. Le résultat est alors :

$$n \in \Sigma \iff \forall p \in \mathcal{P} \text{ tq } p \equiv 3 \mod 4, \nu_p(n) \text{ est pair.}$$

L'implication $\Leftarrow$ est claire, en remarquant qu'un carré est toujours dans $\sum$. Pour $\Rightarrow$, on procède de la manière suivante : si $\nu_p(n) = 0$, c'est clair. Sinon, on remarque que $p \in \sum$ est irréductible dans $\mathbb{Z}[i]$ par un lemme précédemment établi, et divise $n = a^2 + b^2 = (a+ib)(a-ib)$, donc $(a+ib)$ (par exemple). Comme p est entier, il divise a et b donc p^2 divise n, et $\nu_{(\frac{n}{p^2})} = \nu_p(n) - 2$. On réitère le même argument un nombre fini de fois, ce qui nous permet de conclure.

1.5.4 Remarques

— Pour le fait que $\mathbb{Z}[i]$ est euclidien, on peut enjoliver et faire le dessin pris dans le L3 Pearson.

7. On a $|\mathbb{F}_q^{2*}| = \frac{q-1}{2}$ via le morphisme de groupes surjectif $\mathbb{F}_q^* \to \mathbb{F}_q^{2*}$, de noyau $\{-1, +1\}$ qui est de cardinal 2 car $p \neq 2$.

1.6 Points extrémaux de la boule unité de $\mathcal{L}(E)$

1.6.1 Développement

Théorème 7. *Soit E un espace euclidien et $B = \{u \in \mathcal{L}(E); |||u||| \leq 1\}$. Alors*

$$\mathrm{Extr}(B) = O(E).$$

On aura besoin d'un lemme, version plus faible de la décomposition polaire :

Lemme 9. *Soit $A \in \mathscr{M}_n(\mathbb{R})$. Il existe un couple $(O, S) \in O_n(\mathbb{R}) \times S_n^+(\mathbb{R})$ tel que $A = OS$.*

Démonstration du lemme. On suppose que A est inversible. Alors ${}^tAA$ est symétrique définie positive (car A inversible), donc elle admet une racine carrée $S \in S_n^{++}(\mathbb{R})$. On pose $O = AS^{-1}$ et comme ${}^tOO = {}^tS^{-1}{}^tAAS^{-1} = \mathrm{I}_n$, un tel couple (O, S) convient.
Si A est non-inversible on utilise la densité de $\mathrm{GL}_n(\mathbb{R})$ dans $\mathscr{M}_n(\mathbb{R})$: on choisit une suite de matrices inversibles $A_p \in \mathrm{GL}_n(\mathbb{R})$ qui converge vers A. Pour tout $p \in \mathbb{N}$, on écrit $A_p = O_pS_p$ avec $(O_p, S_p) \in O_n(\mathbb{R}) \times S_n^{++}(\mathbb{R})$. Par compacité de $O_n(\mathbb{R})$ (fermé borné de $\mathscr{M}_n(\mathbb{R})$), on peut extraire une sous-suite $(O_{\varphi(p)})$ - toujours notée (O_p) - qui converge vers $O \in O_n(\mathbb{R})$. Donc $S_p = O_p^{-1}A_p \underset{p\to+\infty}{\longrightarrow} O^{-1}A =: S$, où S symétrique (l'ensemble des matrices symétriques est un fermé de $\mathscr{M}_n(\mathbb{R})$). S est de plus positive car $0 \leq {}^tXS_pX \underset{p\to+\infty}{\longrightarrow} {}^tXSX$ par continuité de la multiplication. □

On peut à présent prouver le théorème :

Démonstration du théorème. On montre que si $u \in O(E)$ alors u est extrémal : comme $|||u||| = 1$ (car $\sup_{||x||=1} ||u(x)|| = \sup_{||x||=1} ||x|| = 1$), on a déjà que $u \in B$.
On suppose par l'absurde que u est le milieu d'un segment, en l'écrivant $u = \frac{1}{2}(v + w)$, $v, w \in B$. Soit $x \in E$ tel que $||x|| = 1$. On a alors :

$$1 = ||x|| = ||u(x)|| = \frac{1}{2}||v(x) + w(x)|| \leq \frac{1}{2}(||v(x)|| + ||w(x)||) \leq \frac{1}{2}(|||v||| + |||w|||) \leq 1,$$

et donc toutes les inégalités sont des égalités. En particulier $|||v||| = |||w||| = 1, ||v(x)|| = ||w(x)|| = 1$ et on a de plus que $v(x) = \lambda w(x)$ avec $\lambda > 0$ (cas d'égalité dans l'inégalité triangulaire pour une norme euclidienne), et l'égalité des normes donne finalement $u(x) = v(x)$. Ceci étant vrai pour tout x unitaire, c'est encore valable par linéarité sur E tout entier et finalement $v = w$. Finalement u est bien un point extrémal de $\mathcal{L}(E)$.

Réciproquement, considérons $u \in B \setminus O(E)$ et montrons que u n'est pas extrémal. On travaille matriciellement en considérant la matrice A de u dans une base orthonormée de E, et en considérant sa décomposition polaire donnée par le lemme $A = OS$. On a que $S = {}^tPDP$ avec $P \in O_n(\mathbb{R})$ et $D = \mathrm{diag}(d_1, \dots, d_n)$ où l'on suppose $d_1 \leq \cdots \leq d_n$ et $\dim E = n$. On sait que $|||S||| = |||A|||$ par le fait que $||AX|| = ||OSX|| = ||SX||$, et ainsi $|||S||| = |||A||| \leq 1$. Ceci implique que pour tout $k \in \{1, \dots, n\}$, on a $0 \leq d_k \leq 1$[8]. Par hypothèse, A n'est pas orthogonale et l'on peut supposer $d_1 < 1$ (sinon on aurait $S = {}^tP\mathrm{I}_nP = \mathrm{I}_n$ et $A = O$). On écrit alors $d_1 = \frac{\alpha+\beta}{2}$ avec $-1 \leq \alpha < \beta \leq 1$ (comme d_1 n'est pas un point extrémal du segment $[-1, 1]$). On pose $D' = \mathrm{diag}(\alpha, d_2, \dots, d_n)$ et $D'' = \mathrm{diag}(\beta, d_2, \dots, d_n)$. On a $\frac{1}{2}(D' + D'') = D$ avec $D' \neq D''$, et donc

$$A = \frac{1}{2}(O^tPD'P + O^tPD''P).$$

Vérifions que les deux points ainsi obtenus sont bien dans B : on a

$$|||O^tPD'P||| \leq \underbrace{|||O|||}_{=1}\underbrace{|||{}^tP|||}_{=1}\underbrace{|||D'|||}_{\leq 1}\underbrace{|||P|||}_{=1} \leq 1.$$

On fait exactement la même chose pour D'', et on a notre résultat.

□

1.6.2 Références

[FGN10], pp. 128-131.

1.6.3 Questions classiques

1. *Rappelez la définition de point extrémal* : Un point u d'un convexe C de E est dit extrémal si toute égalité $u = (1-t)v + tw$ avec $v, w \in C$ entraîne que $v = u$ ou $w = u$.
2. *Montrez que ${}^tAA$ est symétrique définie positive* : On a ${}^t({}^tAA) = {}^tA{}^{tt}A = {}^tAA$. De plus, pour $X \in \mathbb{R}^n$ quelconque on a ${}^tX{}^tAAX = ||AX||^2 \geq 0$. Comme A est inversible, on a que $||AX||^2 = 0$ si et seulement si $X = 0$.

8. En remarquant que $|||S||| = |||D|||$ par le fait que

$$|||S||| = \sup_{||X||=1} \frac{||SX||}{||X||} = \sup_{||X||=1} \frac{||{}^tPDPX||}{||X||} = \sup_{||X||=1} \frac{||DPX||}{||X||} = \sup_{||X||=1} \frac{||DPX||}{||PX||} = |||D|||$$

car P est inversible, puis en remarquant que $d_i = \frac{||DE_i||}{||E_i||}$.

3. *Montrez que $O_n(\mathbb{R})$ est compact* : On montre que c'est un fermé borné de $\mathscr{M}_n(\mathbb{R}) \simeq \mathbb{R}^{n^2}$. Il est fermé car il s'écrit $f^{-1}(\{\mathrm{I}_n\})$ où $f(M) = {}^tMM$. Il est borné car on a $||M||_\infty \leq n^2$, chaque terme de la matrice étant de module plus petit que 1.

1.6.4 Remarques

— La norme d'un endomorphisme est égale à celle de sa matrice en base orthonormée, pour la norme subordonnée usuelle sur $\mathbb{R}^n$.

— En dimension 1, on identifie E et $\mathcal{L}(E)$ à $\mathbb{R}$ et B s'identifie au segment $[-1, 1]$. Ses point extrémaux sont $\{\pm 1\}$, ce qui correspond bien à $O(E) = \{\pm \mathrm{id}_E\}$.

1.7 Théorème de Wedderburn

1.7.1 Développement

Théorème 8. *Toute algèbre à division finie est un corps.*

Démonstration. Soit k une algèbre à division finie. On note Z son centre :

$$Z = \{a \in k \ ; \ \forall x \in k, ax = xa\},$$

Z est un corps inclus dans k de cardinal $q \geq 2$. Comme k est un $Z-$espace vectoriel de dimension nécessairement finie, on a $|k| = q^n$ pour un certain entier n. Supposons par l'absurde que k soit non-commutatif, donc que $n > 1$. Faisons agir le groupe multiplicatif k^* sur lui-même par automorphismes intérieurs. Pour $x \in k^*$, on note $\omega(x)$ l'orbite de x. On pose par ailleurs : $k_x = \{y \in k \ ; \ yx = xy\}$, k_x est une sous-algèbre à division de k et on a que $\text{Stab}(x) = k_x^*$. On a que $|k_x| = q^d$ pour la même raison que précédemment. De plus, cet entier d (qui, remarquons-le dès à présent, dépend de x) est un diviseur de n : on a en effet que $k_x^* < k^*$, et par conséquent le théorème de Lagrange implique que $q^d - 1 | q^n - 1$. En écrivant alors par division euclidienne que $n = ad + b$ avec $b < d$, puis que

$$1 \equiv q^n \equiv (q^d)^a q^b \equiv q^b \mod q^d - 1,$$

on remarque que l'on doit avoir $q^d - 1 | q^b - 1$ avec $b < d$ et $q \geq 2$, ce qui nous donne bien $b = 0$ puis le résultat. Le cardinal de l'orbite de x est alors, par la formule des classes :

$$|\omega(x)| = \frac{|k^*|}{|k_x^*|} = \frac{q^n - 1}{q^d - 1}.$$

En utilisant le fait que les polynômes cyclotomiques sont à coefficients entiers, on a dans $\mathbb{Z}$ la relation $q^n - 1 = \prod_{m|n} \Phi_m(q)$, et de même $q^d - 1 = \prod_{m|d} \Phi_m(q)$, donc

$$\frac{q^n - 1}{q^d - 1} = \prod_{\substack{m|n \\ m \nmid d}} \Phi_m(q).$$

Pour $d \neq n$, on voit en particulier que $\Phi_n(q)$ divise $\frac{q^n-1}{q^d-1}$. On écrit ensuite l'équation aux classes :

$$|k^*| = |Z^*| + \sum_{x \notin Z} |\omega(x)|,$$

où la somme porte sur un représentant x de chaque orbite non-réduite à un seul élément, ce qui signifie que dans ces cas-là on a $d \neq n$, de sorte qu'on a

$$q^n - 1 = q - 1 + \sum \frac{q^n - 1}{q^d - 1},$$

la somme portant sur certains diviseurs stricts de n. Il en résulte que $\Phi_n(q)$ divise $q-1$, en particulier on a que $|\Phi_n(q)| \leq q-1$. Comme enfin $\Phi_n(q) = (q-\zeta_1)\dots(q-\zeta_l)$, où $\zeta_1, \dots, \zeta_l \in \mathbb{C}$ sont les racines $n-$ièmes primitives de l'unité qui sont toutes différentes de 1 (car $n \neq 1$), on vérifie que $|q-\zeta_i| > q-1$ pour tout $i \in \{1, \dots, l\}$ et donc $|\Phi_n(q)| > (q-1)^l \geq q-1$, et c'est une contradiction. □

1.7.2 Références

[Per96], p. 82.

1.7.3 Questions classiques

1. *Montrez que les polynômes cyclotomiques sont unitaires à coefficients entiers* : On procède par récurrence. On a

$$\Phi_1(X) = X - 1 \in \mathbb{Z}[X],$$

ce qui constitue l'initialisation. Puis on écrit

$$X^n - 1 = \prod_{\substack{d|n \\ d \neq n}} \Phi_d(X) \times \Phi_n(X),$$

où le terme de gauche dans le membre de droite de l'égalité est unitaire à coefficients entiers par hypothèse de récurrence : la division euclidienne dans $\mathbb{Z}[X]$ assure alors que $\Phi_n(X) \in \mathbb{Z}[X]$, et ceci constitue notre hérédité.

1.7.4 Remarques

— On se convainc plus facilement de la contradiction finale à l'aide d'un dessin, que l'on trouve dans le L3 Pearson par exemple.

1.8 Théorème de l'élément primitif

1.8.1 Développement

Théorème 9 (Théorème de l'élément primitif)**.** *Soit K un corps de caractéristique nulle. Toute extension finie (i.e. de degré fini) de K est monogène.*

Démonstration. Soit K un corps de caractéristique nulle et soit L une extension finie de K. On va montrer que, pour deux éléments $x, y \in L$ quelconques, le corps $K(x,y) \subset L$ s'écrit $K(x,y) = K(z)$ pour un certain $z \in L$. En prenant ensuite une base $a_1, \ldots, a_n$ de L sur K, on aura notre résultat par récurrence. Soit alors $x, y \in L$ quelconque : toute extension finie étant algébrique, on peut considérer leurs polynômes minimaux $P_x, P_y \in K[X]$. On choisit ensuite comme extension de corps $\mathrm{Dec}_K(P_xP_y)$, de sorte à ce qu'on ait l'écriture

$$P_x = \prod_{i=1}^{p}(X - x_i) \qquad \text{et} \qquad P_y = \prod_{i=1}^{q}(X - y_i),$$

où $x_1 = x$ et $y_1 = y$.

Lemme 10. *On a que* $\mathrm{pgcd}_K(P_x, P_x') = 1$.

Démonstration. En effet, on a que P_x est irréductible sur K et que P_x' est non-nul (car de K est de caractéristique nulle) avec $\deg P'x < \deg P_x$: un diviseur commun étant alors de degré strictement inférieur à $\deg P_x$, seul 1 convient. □

Comme le pgcd est invariant par extension de corps (on peut l'obtenir par divisions euclidiennes successives et on a unicité du quotient et du reste dans $K[X]$ muni du stathme deg), on a que P_x est scindé à racines simples sur $\mathrm{Dec}_K(P_xP_y)$. Un raisonnement analogue sur P_y montre que l'ensemble

$$\left\{\frac{x_i - x_{i'}}{y_j - y_{j'}} \ ; \ 1 \leq i, i' \leq p \text{ et } 1 \leq j \neq j' \leq q\right\}$$

est bien défini. Comme c'est un sous-ensemble fini, il existe un $t \in K^*$ (infini) tel que

$$\forall 1 \leq i, i' \leq p, \forall 1 \leq j \neq j' \leq q, x_i + ty_j \neq x_{i'} + ty_{j'}.$$

On note alors $z = x + ty$.

Lemme 11. *On a que* $\mathrm{pgcd}_{K(z)}(P_y, P_x(z - tX)) = X - y$.

Démonstration. On a que y est racine commune à chacun des deux polynômes. De plus, si a est racine commune aux deux polynômes, on a $a = y_j$ et $z - ta = x_i$, i.e. $z = x_i + ty_j$ pour certains i et j. Ceci implique que $j = 1$, et alors $a = y$. Les polynômes considérés étant scindés à racines simples, on a déterminé le pgcd recherché. □

Ainsi on a d'une part $K(z) \subset K(x,y)$ vu la relation $z = x + ty$, puis $K(x,y) \subset K(z)$ vu que $X - y \in K(z)[X]$ et donc $y \in K(z)$, et enfin $x = z - ty \in K(z)$. On a bien montré que $K(x,y) = K(z)$.

□

On détaille un contre-exemple lorsque le corps considéré est de caractéristique $p > 0$:

Proposition 7.

$[\mathbb{F}_p(X,Y) : \mathbb{F}_p(X^p, Y^p)] = p^2$ et $\forall x \in \mathbb{F}_p(X,Y), [\mathbb{F}_p(X^p, Y^p)(x) : \mathbb{F}(X^p, Y^p)] \leq p$.

On utilisera le :

Lemme 12. *Soit k un corps et soit $n \in \mathbb{N}^*$. On a : $[k(X) : k(X^n)] = n$.*

Démonstration. On a que $k[X^n] \simeq k[Y]$ via le morphisme fixant k et envoyant X^n sur Y. Par conséquent, $k[X^n]$ est factoriel. Comme X^n est irréductible dans $k[X^n]$ (pour des raisons de degré), on a d'après le critère d'Eisenstein que le polynôme $Y^n - X^n$ est irréductible sur $k[X^n]$, et donc comme il est primitif sur $k(X^n)$. C'est donc le polynôme minimal de X sur $k(X^n)$, et l'extension est donc de degré n. □

Finalement, on a $[\mathbb{F}_p(X,Y) : \mathbb{F}_p(X^p, Y^p)] = [\mathbb{F}_p(X,Y) : \mathbb{F}_p(X^p, Y)] \cdot [\mathbb{F}_p(X^p, Y) : \mathbb{F}_p(X^p, Y^p)] = p^2$, et comme pour un élément $x = \frac{P(X,Y)}{Q(X,Y)}$ dans $\mathbb{F}_p(X,Y)$ on a $x^p = \frac{P(X^p,Y^p)}{Q(X^p,Y^p)} \in \mathbb{F}_p(X^p, Y^p)$ par le morphisme de Frobenius (automorphisme sur $\mathbb{F}_p$, puis morphisme sur $\mathbb{F}_p(X)$), le degré du polynôme minimal de x (et donc de l'extension monogène engendrée par x) est majoré par p, et ainsi cette extension ne saurait être monogène.

1.8.2 Références

[Gou09], pp. 89-90, [Ort04], pp. 124-125.

1.8.3 Questions classiques

1. *Que peut-on dire lorsque K est fini* : Une extension L de degré fini est finie, et on sait alors que L^* est un groupe multiplicatif cyclique : pour un générateur x, il est clair que $L = K(x)$.
2. *Pourquoi P_x et P_y restent-ils scindés sur* $\mathrm{Dec}_K(P_xP_y)$: On sait que l'on eut écrire $P_xP_y = \prod_{i=1}^{r}(X - z_i)$, et comme $\mathrm{Dec}_K(P_xP_y)[X]$ est factoriel (car euclidien, puis principal), l'unicité de la décomposition en facteurs irréductibles assure que chacun de ces deux polynômes soient scindés à racines simples.

1.8.4 Remarques

— Il faut aller vite sur ce développement, et être prêt à seulement détailler le contre-exemple final.

1.9 Le cube et les représentations de $\mathfrak{S}_4$

1.9.1 Développement

L'objectif de ce développement est de dresser la table des caractères de $\mathfrak{S}_4$. Pour cela on utilisera une construction particulière de représentations irréductibles, la représentation par permutation associée. Si l'on dispose de $G \curvearrowright X$ où G est fini et X est fini de cardinal n, alors en notant $\mathbb{C}X = \mathbb{C}e_{x_1} \oplus \cdots \oplus \mathbb{C}e_{x_n}$, où les e_{x_i} sont les vecteurs de la base canonique de $\mathbb{C}^n$ indexés par les éléments de X, on définit une représentation $\rho : G \to \mathrm{GL}(\mathbb{C}X)$ en posant $\rho(g)(e_x) = e_{g\cdot x}$, où $\cdot$ désigne l'action initiale $G \curvearrowright X$. On remarque que, en posant $s = \sum_{x\in X} e_x$, le sous-espace vectoriel $\mathbb{C}s$ est invariant par G. Le théorème de Maschke nous autorise à considérer un sous-espace supplémentaire $\mathbb{C}X = \mathbb{C}s \oplus V_X$.

Proposition 8. [9] *On note χ le caractère de la sous-représentation $\rho|_{V_X}$. Alors :*

1. $\forall g \in G, \chi(g) = |\mathrm{Fix}(g)| - 1$,
2. *Si G agit 2 fois transitivement sur X, alors χ est irréductible.*

Démonstration.

1. Un 1 sur la diagonale de $\rho(g)$ dans la base $(e_{x_1}, \dots e_{x_n})$ correspond à un point fixe de l'action $G \curvearrowright X$. Comme $\rho|_{\mathbb{C}s}$ est la représentation triviale qui est de caractère identiquement 1, on conclut par additivité du caractère.
2. On a que

$$\langle \chi, \chi \rangle = \frac{1}{|G|} \sum_{g\in G} (|\mathrm{Fix}(g)| - 1)^2 = \frac{1}{|G|} \sum_{g\in G} |\mathrm{Fix}(g)|^2 - 2 \cdot \frac{1}{|G|} \sum_{g\in G} |\mathrm{Fix}(g)| + 1.$$

La formule de Burnside nous donne que

$$1 = |\{\text{orbites de } G \curvearrowright X\}| = \frac{1}{|G|} \sum_{g\in G} |\mathrm{Fix}(g)|,$$

par transitivité de $G \curvearrowright X$. De plus, l'hypothèse que G agit deux fois transitivement sur X se traduit par le fait que l'action $G \curvearrowright X \times X$ possède deux orbites : la diagonale et son complémentaire. Par conséquent, la formule de Burnside se reformule en

$$2 = |\{\text{orbites de } G \curvearrowright X \times X\}| = \frac{1}{|G|} \sum_{g\in G} |(X \times X)^g| = \frac{1}{|G|} \sum_{g\in G} |\mathrm{Fix}(g)|^2.$$

Finalement, $\langle \chi, \chi \rangle = 2 - 2 + 1 = 1$ et la représentation est bien irréductible.

□

9. On admettra cette proposition dans les leçons qui se concentrent sur la géométrie.

On complète alors au fur et à mesure :

$\mathfrak{S}_4$	(1) id	(6) $(**)$	(8) $(***)$	(6) $(****)$	(3) $(**)(**)$
1	$\boxed{1}$	$\boxed{1}$	$\boxed{1}$	$\boxed{1}$	$\boxed{1}$
ε	$\boxed{1}$	-1	$\boxed{1}$	-1	$\boxed{1}$
perm	$\boxed{3}$	1	0	-1	-1
faces	$\boxed{2}$	0	-1	0	$\boxed{2}$
manquante	$\boxed{3}$	-1	0	1	-1

On a 5 classes de conjugaison en vertu de la formule de conjugaison des cycles. Comme une représentation de degré 1 est la donnée d'un morphisme de $\mathfrak{S}_4$ dans $\mathrm{GL}_1(\mathbb{C}) \simeq \mathbb{C}^*$ et que les seuls morphismes de ce type existants sont id et ε (comme on peut le remarquer en observant sur quoi doivent être envoyées les transpositions, qui engendrent $\mathfrak{S}_4$), on a nos deux premières lignes. Pour obtenir perm et faces, on réalise $\mathfrak{S}_4$ comme le groupe $\mathrm{Isom}^+(\text{cube})$ de la manière suivante :

— l'identité reste l'identité,

— une transposition correspond à une rotation d'angle $\pm\pi$ et d'axe la médiatrice commune à deux arêtes symétriques par rapport au centre du cube,

— un 3-cycle correspond à une rotation d'angle $\pm\frac{2\pi}{3}$ d'axe une grande diagonale,

— un 4-cycle correspond à une rotation d'angle $\pm\frac{\pi}{2}$ d'axe une droite passant par le milieu de deux faces opposées du cube,

— une double transposition correspond à un rotation d'angle $\pm\pi$ d'axe une droite passant par le milieu de deux faces opposées du cube.

En faisant agir $\mathfrak{S}_4$ sur les grandes diagonales du carré puis sur ses paires de faces opposées, on obtient deux représentations irréductibles. La manquante est obtenue à l'aide de la relation $\sum_{i=1}^{5}(\dim V_i)^2 = |G|$ (qui découle de l'étude de la représentation régulière) et des relations d'orthogonalité entre les colonnes.

1.9.2 Références

[CG14], pp. 458-459, 493, [Pey04], pp. 228-230.

1.9.3 Questions classiques

1. *Pourquoi a-t-on bien l'isomorphisme que vous annoncez* : Le groupe des isométries (quelconques) I du cube agit sur les grandes diagonales D (dis-

tance maximale entre deux points du cube). Par suite, on a un morphisme $\rho : I \mapsto \mathfrak{S}(D) \simeq \mathfrak{S}_4$. Il est surjectif par le fait que l'on atteint les transpositions, qui engendrent $\mathfrak{S}_4$, et son noyau est $\{\mathrm{id}, s_O\}$ comme on voit qu'un élément non-trivial du noyau doit permuter les sommets de chaque grande diagonale (il en permute une et par isométrie il les permute toutes), et coïncide avec s_O car les deux applications sont égales sur un repère affine. En passant au quotient, comme chaque classe d'équivalence doit contenir un déplacement et un antidéplacement, on a $I/\{\mathrm{id}, s_O\} \simeq I^+$ et l'isomorphisme demandé.

2. *Comment retrouvez-vous les sous-groupes distingués de $\mathfrak{S}_4$ grâce à la table de ses caractères* [10] : On remarque d'abord que si ρ est une représentation de degré d, son noyau est $\ker\rho = \{g \in G \,;\, \chi(g) = d\}$. En effet, $\rho(g)$ est diagonalisable car d'ordre fini, et ses valeurs propres sont des racines de l'unité. La condition $\chi(g) = d$ est équivalente à dire que toutes ses valeurs propres sont égales à 1 (cas d'égalité dans l'inégalité triangulaire), i.e. que $\rho(g)$ est l'identité. Ensuite, on remarque que si $H \lhd \mathfrak{S}_4$, alors H est l'intersection de noyaux de représentations irréductibles de $\mathfrak{S}_4$. En effet, en notant $\pi : \mathfrak{S}_4 \to \mathfrak{S}_4/H$ la surjection canonique et ρ_H la représentation régulière associée à $\mathfrak{S}_4/H$, on a que ρ_H est fidèle et qu'ainsi H est le noyau de la représentation $\rho_H \circ \pi$. En écrivant $\rho_H \circ \pi$ comme une somme directe de représentations irréductibles, on a notre résultat. On a fait apparaître ces points dans le tableau à l'aide d'encadrements.

1.9.4 Remarques

— Un dessin pour l'identification $\mathfrak{S}_4 \simeq \mathrm{Isom}^+(\text{cube})$ reste le meilleur moyen de visualiser cet isomorphisme.

10. Cette question est à développer dans la leçon portant sur les sous-groupes distingués.

1.10 Ellipsoïde de John-Loewner

1.10.1 Développement

Notations préliminaires : Q est l'ensemble des formes quadratiques de $\mathbb{R}^n$, Q^+ celles qui sont positives, Q^{++} celles qui sont définies positives et $D(q)$ est le déterminant d'une matrice représentant la forme quadratique q dans une base orthonormée (pour le produit scalaire euclidien usuel) quelconque (il est bien défini : on le montre dans le lemme 1).

Théorème 10. *Soit K un compact d'intérieur non-vide de $\mathbb{R}^n$. Il existe un unique ellipsoïde centré en O de volume minimal contenant K.*

On munit $\mathbb{R}^n$ de sa structure euclidienne usuelle. Un ellispoïde plein centré en O a une équation du type $q(x) \leq 1$ où $q \in Q^{++}$. On note $\mathcal{E}_q := \{x \in \mathbb{R}^n \ ; \ q(x) \leq 1\}$ l'ellipsoïde associé à q.

Lemme 13. [11] *Le volume de $\mathcal{E}_q$ est $V_q = \frac{V_0}{\sqrt{D(q)}}$, où l'on a noté V_0 le volume de la boule unité pour la norme euclidienne canonique.*

Preuve du lemme. Le théorème spectral nous autorise à considérer une base orthonormée $\mathcal{B}$ (pour le produit scalaire euclidien usuel) dans laquelle q s'écrit $q(x) = \sum_{i=1}^n a_i x_i^2$, avec les $a_i > 0$ comme q est définie positive. On a donc $V_q = \int_{\sum_{i=1}^n a_i x_i^2 \leq 1} dx_1 \dots dx_n$. Le changement de variable $\varphi(x) = (\frac{x_1}{\sqrt{a_1}}, \dots, \frac{x_n}{\sqrt{a_n}})$, qui est un C^1-difféomorphisme de jacobien $\frac{1}{\sqrt{a_1 \dots a_n}}$, donne alors $V_q = \int_{\sum_{i=1}^n t_i^2 \leq 1} \frac{dt_1 \dots dt_n}{\sqrt{a_1 \dots a_n}}$. Si l'on note S la matrice représentative de q dans une base orthonormée $\mathcal{B}'$ quelconque, on a en notant $P = \text{Pass}(\mathcal{B}, \mathcal{B}')$ que $S = {}^tP[q]_{\mathcal{B}}P = {}^tP\text{diag}(a_1, \dots, a_n)P$ où P est orthogonale en tant que matrice de passage entre bases orthonormées, d'où $\det(S) = a_1 \dots a_n$. On a finalement prouvé le lemme. □

On s'est donc ramenés à montrer l'existence d'une unique forme quadratique $q \in Q^{++}$ telle que $D(q)$ soit maximal et que $\forall x \in K, q(x) \leq 1$. Prouvons le théorème :

Démonstration. Munissons l'espace vectoriel Q de la norme $N : q \mapsto \sup_{||x|| \leq 1} |q(x)|$. On cherche à maximiser D sur l'ensemble $A := \{q \in Q^+ \ ; \ \forall x \in K, q(x) \leq 1\}$, avec l'espoir que le max soit atteint par une forme quadratique définie positive : pour cela, montrons que A est un convexe, compact (i.e. fermé borné comme Q est de dimension finie $\frac{n(n+1)}{2}$, c'est pour cette raison - et pour un futur passage

11. Par manque de temps, on choisira de ne présenter qu'un des deux lemmes en fonction de la leçon concernée.

à la limite - que l'on prend A comme un sous-ensemble de Q^+ et non de Q^{++}) de Q et qu'il est non-vide.

— A **est convexe :** Soit $q, q' \in A$, et soit $\lambda \in [0,1]$. On a que :
  — $\forall x \in \mathbb{R}^n, (\lambda q + (1-\lambda)q')(x) = \lambda q(x) + (1-\lambda)q'(x) \geq 0$ (en tant que somme de termes positifs),
  — $\forall x \in K, (\lambda q + (1-\lambda)q')(x) \leq \lambda + 1 - \lambda \leq 1$.

  Donc $\lambda q + (1-\lambda)q' \in A$.

— A **est fermé :** Soit (q_n) une suite convergente (au sens de N) d'éléments de A. On note $q \in Q$ sa limite. On a [12] que

$$\forall x \in \mathbb{R}^n, |q_n(x) - q(x)| \leq N(q_n - q)||x||^2 \underset{n\to+\infty}{\longrightarrow} 0\,.$$

  On en déduit par passage à la limite les inégalités $\forall x \in \mathbb{R}^n, 0 \leq q(x)$ et $\forall x \in K, q(x) \leq 1$, d'où $q \in A$.

— A **est borné :** Par hypothèse, il existe $a \in K$ et $r > 0$ tq $B(a,r) \subset K$. Soit $q \in A$ quelconque. Si $||x|| \leq r$ alors $a + x \in K$ et donc $q(a+x) \leq 1$. D'autre part, $q(-a) = q(a) \leq 1$. On a donc :

$$\sqrt{q(x)} = \sqrt{q(x+a-a)} \leq \sqrt{q(x+a)} + \sqrt{q(-a)} \leq 1 + 1 = 2,$$

  où la première inégalité est celle de Minkowski (que l'on peut employer car q est supposée positive). Donc $q(x) \leq 4$. Si $||x|| \leq 1$, on a que $||rx|| \leq r$. Donc on a $|q(x)| = q(x) = \frac{1}{r^2}q(rx) \leq \frac{4}{r^2}$. Donc en prenant le sup à gauche, $N(q) \leq \frac{4}{r^2}$ et A est borné.

— A **est non-vide :** K est compact, donc borné : on choisit $M > 0$ tq $\forall x \in K, ||x|| \leq M$. En posant $q_1(x) = \frac{\langle x,x\rangle}{M^2}$, on a $q_1 \in Q^{++}$ et $\forall x \in K, q_1(x) \leq 1$. Donc $q_1 \in A$.

□

Achevons la preuve : on a que comme det est continue, l'application $q \mapsto D(q)$ l'est aussi [13]. Elle atteint son maximum sur le compact A, en une certaine forme quadratique q_0. Comme pour $x \in \mathbb{R}^n$ non-nul on a $D(q_0) \geq D(q_1) = \frac{1}{M^{2n}} > 0$, on a bien $q_0 \in Q^{++}$. On a montré l'existence d'un ellipsoïde de volume minimal contenant K : montrons pour conclure l'unicité. Supposons qu'il existe $q \in A$ tel que $D(q) = D(q_0)$ et $q \neq q_0$. En notant S et S_0 leurs matrices

12. En normalisant les vecteurs.
13. Voir la première remarque

dans la base canonique de $\mathbb{R}^n$, il vient en utilisant la convexité de A et la stricte concavité logarithmique de det sur $S_n^{++}(\mathbb{R})$ que

$$D(\frac{1}{2}(q+q_0)) = \det \frac{1}{2}(S+S_0) > (\det S)^{\frac{1}{2}}(\det S_0)^{\frac{1}{2}} = D(q_0),$$

ce qui est contradictoire.

Lemme 14 (Stricte concavité logarithmique de det sur $S_n^{++}(\mathbb{R})$)**.** *Soient $A, B \in S_n^{++}(\mathbb{R})$ et soient $\alpha, \beta \in \mathbb{R}^{+*}$ tels que $\alpha + \beta = 1$. Alors*

$$\det(\alpha A + \beta B) \geq \det(A)^{\alpha} \det(B)^{\beta}.$$

De plus, si $A \neq B$, l'inégalité est stricte.

Démonstration. On peut écrire par le théorème de pseudo-réduction simultanée que $A = {}^tPP$ et $B = {}^tPDP$, avec $P \in \mathrm{GL}_n(\mathbb{R})$ et $D = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$, où on a pour tout $i \in \{1, \ldots, n\}$ que $\lambda_i > 0$. Donc

$$(\det A)^{\alpha}(\det B)^{\beta} = (\det P)^2(\det D)^{\beta}$$

et

$$\det(\alpha A + \beta B) = (\det P)^2 \det(\alpha \mathrm{I}_n + \beta D).$$

On veut montrer que $\det(\alpha \mathrm{I}_n + \beta D) \geq (\det D)^{\beta}$, i.e. $\prod_{i=1}^n (\alpha + \beta\lambda_i) \geq (\prod_{i=1}^n \lambda_i)^{\beta}$, i.e. $\sum_{i=1}^n \ln(\alpha + \beta\lambda_i) \geq \beta \sum_{i=1}^n \ln(\lambda_i)$: or, par concavité de ln, on a que

$$\ln(\alpha + \beta\lambda_i) \geq \alpha \ln(1) + \beta \ln(\lambda_i) = \beta\lambda_i \qquad \text{pour tout } i \in \{1, \ldots, n\}.$$

Finalement, on a notre résultat en sommant sur i. Si $A \neq B$, l'un des λ_i est différent de 1 le fait que la concavité de ln soit stricte permet de conclure. □

1.10.2 Références

[FGN10], pp. 219-220, 222, 229-231.

1.10.3 Questions classiques

1. *Comment démontrez-vous le théorème de pseudo-réduction simultanée* : On le démontre sous une hypothèse plus faible, à savoir $A \in S_n^{++}(\mathbb{R})$ et $B \in S_n(\mathbb{R})$. On a que A définit canoniquement un produit scalaire sur $\mathbb{R}^n$ via $(x, y) \mapsto {}^txAy$: on peut prendre une base orthonormée pour ce produit scalaire, i.e. il existe $P \in \mathrm{GL}_n(\mathbb{R})$ telle que ${}^tPAP = \mathrm{I}_n$. Comme alors ${}^tPBP$ est symétrique réelle, le théorème spectral assure qu'il existe une matrice $Q \in O_n(\mathbb{R})$ telle que ${}^tQ{}^tPBPQ = D$ où D est une matrice diagonale réelle. En posant $C = (PQ)^{-1}$, on a le résultat attendu.

1.10.4 Remarques

— Bien faire attention à pourquoi l'on considère des bases orthonormées dans le lemme 1 : D serait mal défini sinon (au passage, l'utilité de prouver que $D(q)$ ne dépend que de q est que, lorsque q varie, la base orthonormée dans laquelle on va calculer son déterminant est fixée, et ainsi $D : q \mapsto D(q)$ est bien continue).

— La norme qui intervient au début de la preuve du théorème est bien définie, par continuité des formes quadratiques en dimension finie.

— Rappel de la preuve de l'inégalité de Minkowski lorsque q est (réelle) positive : on a l'inégalité de Cauchy-Schwarz (discriminant du polynôme $q(xt+y) \leq 0$), qui donne

$$\begin{aligned} \varphi(x,y) \leq \sqrt{q(x)}\sqrt{q(y)} &\Longrightarrow \frac{q(x+y)-q(x)-q(y)}{2} \leq \sqrt{q(x)}\sqrt{q(y)} \\ &\Longrightarrow \sqrt{q(x+y)} \leq \sqrt{q(x)}+\sqrt{q(y)} \end{aligned}$$

via la première identité remarquable.

— Fritz John : mathématicien allemand, 1910-1994

— Charles Loewner : mathématicien tchèque, 1863-1968

1.11 Partitions d'un entier en parts fixées

1.11.1 Développement

Théorème 11. *Soient $a_1, \dots, a_k \in \mathbb{N}^*$ premiers entre eux dans leur ensemble. Pour $n \in \mathbb{N}^*$, on note $u_n = |\{(x_1, \dots, x_k) \in \mathbb{N}^k \ ; \ a_1x_1 + \cdots + a_kx_k = n\}|$. Alors on a :*

$$u_n \sim \frac{1}{a_1 \dots a_k} \frac{n^{k-1}}{(k-1)!}.$$

Démonstration. Considérons le produit des k séries formelles $\sum_{x_i=0}^{+\infty} X^{a_i x_i}$, pour $i \in \{1, \dots, k\}$. On note $f(X)$ ce produit, il vient :

$$f(X) = \prod_{i=1}^{k} \Big(\sum_{x_i=0}^{+\infty} X^{a_i x_i} \Big) = \sum_{n=0}^{+\infty} \Big(\sum_{\substack{(x_1,\dots,x_k) \in \mathbb{N}^k \\ a_1x_1 + \cdots + a_kx_k = n}} 1 \Big) X^n = \sum_{n=0}^{+\infty} u_n X^n,$$

et on reconnaît la série génératrice de la suite (u_n). C'est une fraction rationnelle dont les pôles sont les racines a_i-ièmes de l'unité, car $f(X) = \prod_{i=1}^{k} \frac{1}{1-X^{a_i}}$. Effectuons sa décomposition en éléments simples : le pôle 1 est de multiplicité k [14], et soit ω un autre pôle de $f(X)$. On a que ω est d'ordre inférieur ou égal à k [15] Supposons que ω soit d'ordre k : on a alors $\omega^{a_i} = 1$ pour tout $i \in \{1, \dots, k\}$, mais le théorème de Bézout fournit un $k-$uplet $(u_1, \dots, u_k)$ tel que $a_1u_1 + \cdots + a_ku_k = 1$, et alors $\omega = \omega^{\sum_{i=1}^{k} a_iu_i} = \prod_{i=1}^{k} (\omega^{a_i})^{u_i} = 1$, ce qui est contradictoire. On note $\mathcal{P} := \{\omega_1, \dots, \omega_p\}$ les pôles de $f(X)$, avec $\omega_1 = 1$. Par décomposition en éléments simples, il existe $\alpha \in \mathbb{C}$ et $c_{i,j} \in \mathbb{C}$ pour $(i,j) \in \{1, \dots, k\} \times \{1, \dots, k-1\}$ tels que

$$f(X) = \frac{\alpha}{(1-X)^k} + \sum_{\substack{1 \le i \le p \\ 1 \le j \le k-1}} \frac{c_{i,j}}{(\omega_i - X)^j}.$$

Développons à présent ces éléments simples en séries formelles : on obtient en effet que, pour $\omega \in \mathcal{P}$ et $j \in \{1, \dots, k\}$, que

$$\frac{1}{\omega - X} = \frac{1}{\omega} \frac{1}{1 - \frac{X}{\omega}} = \frac{1}{\omega} \sum_{n=0}^{+\infty} \Big(\frac{X}{\omega} \Big)^n = \sum_{n=0}^{+\infty} \frac{X^n}{\omega^{n+1}}.$$

Ensuite :

$$\Big(\frac{1}{\omega - X} \Big)^{(j-1)} = \frac{(j-1)!}{(\omega - X)^j} = \sum_{n=j-1}^{+\infty} \frac{n!}{(n-j+1)!} \frac{X^{n-j+1}}{\omega^{n+1}}.$$

14. Car racine des k polynômes $1 - X^{a_i}$ qui sont scindés à racines simples sur $\mathbb{C}$.
15. Pour la même raison.

Par conséquent,

$$\frac{1}{(\omega - X)^j} = \sum_{n=j-1}^{+\infty} \frac{n!}{(n-j+1)!(j-1)!} \frac{X^{n-j+1}}{\omega^{n+1}} = \sum_{n=0}^{+\infty} \frac{(n+j-1)!}{n!(j-1)!} \frac{X^n}{\omega^{n+j}}$$
$$= \sum_{n=0}^{+\infty} \binom{n+j-1}{n} \frac{X^n}{\omega^{n+j}}.$$

On écrit enfin

$$f(X) = \alpha \sum_{n=0}^{+\infty} \binom{n+k-1}{n} X^n + \sum_{\substack{1 \leq i \leq p \\ 1 \leq j \leq k-1}} c_{i,j} \Big(\sum_{n=0}^{+\infty} \binom{n+j-1}{n} \frac{X^n}{\omega_i^{n+j}} \Big).$$

Par unicité du développement en série formelle, on a alors que

$$u_n = \alpha \binom{n+k-1}{n} + \sum_{\substack{1 \leq i \leq p \\ 1 \leq j \leq k-1}} c_{i,j} \binom{n+j-1}{n} \frac{1}{\omega_i^{n+j}}.$$

Comme, pour $r \in \mathbb{N}^*$, on a que $\binom{n+r-1}{n} = \frac{(n+r-1)\ldots(n+1)}{(r-1)!} \sim \frac{n^{r-1}}{(r-1)!}$, et que pour $(i,j) \in \{1,\ldots,p\} \times \{1,\ldots,k-1\}$ on a que $c_{i,j}\binom{n+j-1}{n}\frac{1}{\omega^{n+j}} = o(n^{k-1})$ (les ω_i étant des racines de l'unité, donc de module 1), on obtient enfin que

$$u_n \sim \alpha \frac{n^{k-1}}{(k-1)!}.$$

Pour calculer α, on utilise la méthode du cache : on multiplie $f(X)$ par $(1-X)^k$ et on substitue 1 à X [16], ce qui donne

$$(1-X)^k f(X) = \prod_{i=1}^{k} \frac{1-X}{1-X^{a_i}} = \prod_{i=1}^{k} \frac{1}{1+X+\cdots+X^{a_i-1}},$$

et

$$\alpha = \frac{1}{a_1 \ldots a_n}.$$

□

1.11.2 Références

[FGN14b], pp. 197-199.

16. Notons que l'on substitue ici dans f exprimée sous forme de fraction rationnelle, en une valeur qui n'est pas un pôle de f : on ne se permettrait pas ce procédé sur des séries formelles.

1.11.3 Questions classiques

1. *Calculez le nombre de manières d'obtenir* 100 *euros en pièces de* 1 *et* 2 *et en billets de* 5 : Il s'agit de déterminer le coefficient de X^{100} dans le développement en série formelle de $\frac{1}{(1-X)(1-X^2)(1-X^5)}$. Après calculs, on trouve 541.

1.11.4 Remarques

—

1.12 Dénombrement des polynômes irréductibles sur $\mathbb{F}_q$

1.12.1 Développement

Théorème 12. *Soit $n \in \mathbb{N}^*$. On note $A(n,q)$ l'ensemble des polynômes irréductibles unitaires de degré n de $\mathbb{F}_q[X]$ et $I(n,q) = |A(n,q)|$. Alors :*

1. $X^{q^n} - X = \prod_{d|n} \prod_{P \in A(d,q)} P$,
2. $I(n,q) = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) q^d$ *(on a noté μ la fonction de Möbius),*
3. $I(n,q) \sim \frac{q^n}{n}$.

Démonstration. 1. Soient d un diviseur de n (on notera $n = dr$) et $P \in A(d,q)$. Soit x une racine de P dans un corps de décomposition. $\mathbb{F}_q(x)$ est un corps de rupture de P [17] et $[\mathbb{F}_q(x) : \mathbb{F}_q] = \deg(P) = d$. Par unicité des corps finis, on a donc $\mathbb{F}_q(x) \simeq \mathbb{F}_{q^d}$. Par construction, $\mathbb{F}_{q^d}$ est le corps de décomposition de $X^{q^d} - X$ (sur $\mathbb{F}_p$, avec $q = p^n$), i.e. l'ensemble des racines de $X^{q^d} - X$. En particulier, $x^{q^d} = x$ [18]. Ainsi, on a que

$$x^{q^n} = \underbrace{(((x^{q^d})^{q^d})\dots)^{q^d}}_{r \text{ fois}} = \underbrace{(((x^{q^d})^{q^d})\dots)^{q^d}}_{r-1 \text{ fois}} = \dots = x$$

et donc x est racine de $X^{q^n} - X$. On a alors que $P \mid X^{q^n} - X$ [19], et finalement $\prod_{d|n} \prod_{P \in A(d,q)} P \mid X^{q^n} - X$ par irréductibilité [20] (i.e. la valuation de chacun des P dans X^{q^n} est d'au moins 1).
Réciproquement, soit $P \in \mathbb{F}_q[X]$ irréductible divisant $X^{q^n} - X$. On note que $X^{q^n} - X$ est scindé à racines simples sur $\mathbb{F}_{q^n}$, ce sera donc aussi le cas de P. Notons x une racine de P dans $\mathbb{F}_{q^n} : \mathbb{F}_q(x)$ est un corps de rupture de P et est donc un corps intermédiaire entre $\mathbb{F}_q$ et $\mathbb{F}_{q^n}$ [21]. Le théorème de multiplicativité du degré donne

$$n = [\mathbb{F}_{q^n} : \mathbb{F}_q] \text{ [22]} = [\mathbb{F}_{q^n} : \mathbb{F}_q(x)][\mathbb{F}_q(x) : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(x)] \deg(P),$$

17. I.e. une extension monogène $K(\alpha)$ avec $P(\alpha) = 0$.
18. On exhibe l'isomorphisme et on calcule !
19. Car P n'a que des racines simples dans une extension : c'est en fait le polynôme minimal de x, qui divise $X^{q^d} - X$ (car il annule aussi x), et ce dernier est scindé à racines simples.
20. Ou encore, comme ces P sont deux-à-deux premiers entre eux, par le lemme d'Euclide.
21. Pour $\mathbb{F}_{q^n}$, on utilise le résultat que $\mathrm{Dec}_{\mathbb{F}_p}(X^q - X) = \mathbb{F}_p(x_1, \dots, x_q)$, avec les x_i des racines dans une clôture algébrique.
22. On se rappelle que les sous corps de $\mathbb{F}_{p^n}$ sont les $\mathbb{F}_{p^m}$ avec $m \mid n$, via le fait que $X^{p^m} - X \mid X^{p^n} - X \iff m \mid n$ et passage au corps de décomposition.

et donc $\deg(P) \mid n$. On a alors $X^{q^n} - X = \prod_{d|n} \prod_{P \in A(d,q)} P^{\mathrm{val}(P)}$. Comme les facteurs irréductibles de $X^{q^n} - X$ dans $\mathbb{F}_q[X]$ sont de valuation au plus 1 (sans quoi $X^{q^n} - X$ aurait des racines doubles dans $\mathbb{F}_{q^n}$), on en déduit finalement que

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in A(d,q)} P.$$

2. En prenant les degrés des deux polynômes obtenus, on obtient $q^n = \sum_{d|n} dI(d,q)$. En appliquant la formule d'inversion de Möbius à $f : n \mapsto q^n$ et $g : n \mapsto nI(n,q)$, on obtient que

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

3. On a de plus $I(n,q) = \frac{1}{n}\Big(q^n + \underbrace{\sum_{\substack{d|n \\ d \neq n}} q^d \mu(\frac{n}{d})}_{:=r_n}\Big)$, et la majoration [23]

$$|r_n| \leq \sum_{d=1}^{\lfloor \frac{n}{2} \rfloor} q^d = q\frac{q^{\lfloor \frac{n}{2} \rfloor} - 1}{q-1} = o(q^n)$$

assure que $I(n,q) \sim \frac{q^n}{n}$.

□

On a du utiliser les résultats suivants :

Lemme 15 (Fonction de Möbius)**.** *On définit la fonction de Möbius $\mu : \mathbb{N}^* \to \{-1, 0, 1\}$ par $\mu(1) = 1$, $\mu(n) = 0$ si n a un facteur carré et $\mu(p_1 \dots p_r) = (-1)^r$, où les $p_1, \dots, p_r$ sont des nombres premiers distincts. On a alors que :*

1. *La fonction μ est multiplicative au sens où, pour tout $m, n \in \mathbb{N}^*$, $\mathrm{pgcd}(m,n) = 1 \Longrightarrow \mu(mn) = \mu(m)\mu(n)$,*
2. *$\sum_{d|n} \mu(d) = 1$ si $n = 1$, 0 sinon,*
3. *Si pour tout entier $n \in \mathbb{N}^*$, $g(n) = \sum_{d|n} f(d)$, alors $f(n) = \sum_{d|n} g(d)\mu(\frac{n}{d}) = \sum_{d|n} g(\frac{n}{d})\mu(d)$ (Formule d'inversion de Möbius).*

Démonstration. 1. Si m ou n vaut 1, le résultat est clair par définition de $\mu(1)$. C'est aussi clair lorsque m ou n possède un facteur carré. Enfin, comme on demande par hypothèse à ce que $\mathrm{pgcd}(m,n) = 1$, le cas restant est $m = p_1 \dots p_r$ et $n = q_1 \dots q_s$ avec les p_i et q_j des nombres premiers distincts. Alors $\mu(mn) = \mu(p_1 \dots p_r q_1 \dots q_s) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(m)\mu(n)$.

23. Qui vient du fait que si $d|n$ et $d \neq n$ alors $d \leq \lfloor \frac{n}{2} \rfloor$...

2. Le cas $n = 1$ est évident. Sinon, on écrit $n = p_1^{\alpha_1} \dots p_n^{\alpha_r}$, puis on a en considérant les diviseurs sans facteur carrés [24] que

$$\begin{aligned}\sum_{d|n} \mu(d) &= 1 + \sum_{i=1}^{r} \mu(p_i) + \sum_{i<j} \mu(p_i p_j) + \sum_{i<j<k} \mu(p_i p_j p_k) + \dots + \mu(p_1 \dots p_r) \\ &= \sum_{k=0}^{r} \binom{r}{k} (-1)^k \\ &= (1-1)^r \\ &= 0.\end{aligned}$$

3. On a que

$$\sum_{d|n} g\left(\frac{n}{d}\right)\mu(d) = \sum_{d|n} \sum_{d'|\frac{n}{d}} f(d')\mu(d) = \sum_{dd'|n} f(d')\mu(d) = \sum_{d'|n} \sum_{d|\frac{n}{d'}} f(d')\mu(d) = f(n),$$

où l'on a réindexé la somme pour les deux avant-dernières égalités, et le point 2. pour la dernière égalité. Un changement d'indice donne le dernier point.

□

1.12.2 Références

[FG97], pp. 93-94, 189-191.

1.12.3 Questions classiques

1. *Montrez qu'un corps K de caractéristique p sur lequel le morphisme de Frobenius est surjectif est parfait, i.e. que tout polynôme irréductible P est scindé à racine simple dans un corps de décomposition* : Supposons par l'absurde que x soit racine double de $P \in K[X]$, irréductible, dans un corps de décomposition L. On a par invariance du pgcd par extension de corps que nécessairement $\text{pgcd}_L(P, P') = \text{pgcd}_K(P, P') = P$, car P est irréductible (ses diviseurs sont 1 - contradictoire avec la racine double dans l'extension L - ou P). On a un problème de degré, sauf si $P' = 0$: mais dans ce cas, on aurait que $P = Q(X^p) = \sum \alpha_i X^{\beta_i p} = \sum \tilde{\alpha}_i^p X^{\beta_i p} = \left(\sum \tilde{\alpha}_i X^{\beta_i}\right)^p$ par morphisme de Frobenius - surjectivité dans le corps K, puis morphisme dans le corps $K(X)$ - et ceci est contradictoire à nouveau par irréductibilité de P. L'invariance du pgcd par extension de corps est ici utilisée "dans les deux

24. Proprement, on ferait une récurrence forte sur le nombre de facteurs premiers de n.

sens" : on utilise d'une part le fait que P n'admette pas de racine double dans l'extension L et d'autre part son irréductibilité dans le corps K. La preuve expose un argument plus simple dans le cas d'un corps fini, où le morphisme de Frobenius est bien sûr surjectif.

1.12.4 Remarques

— L'idée qui fait marcher la preuve est une idée féconde en algèbre : "on ne sait pas caractériser individuellement chaque élément, alors étudions un nouvel élément formé à partir des précédents via des opérations algébriques" (séries génératrices, etc.).

1.13 Décomposition de Dunford

1.13.1 Développement

Soit E un espace vectoriel de dimension finie.

Lemme 16 (Lemme des noyaux)**.** *Soient $n \geq 2$ et $P_1, \ldots, P_m$ une famille de polynômes deux à deux premiers entre eux et soit $f \in \mathrm{L}(E)$. Alors*

$$\ker\Big(\prod_{k=1}^{m} P_k\Big)(f) = \oplus_{k=1}^{m} \ker P_k(f).$$

De plus, les projecteurs de $\ker\left(\prod_{k=1}^{m} P_k\right)(f)$ *sur l'un de ces sous-espaces parallèlement à la somme des autres est un polynôme en f.*

Démonstration. On le montre par récurrence sur l'entier m.

1. Initialisons en prouvant le cas $m = 2$. Si P_1 et P_2 sont premiers entre eux, le théorème de Bézout donne deux polynômes U_1 et U_2 tels que $U_1P_1 + U_2P_2 = 1$, i.e. $U_1(f) \circ P_1(f) + U_2(f) \circ P_2(f) = \mathrm{id}$. D'où, pour tout $x \in \ker(P_1P_2)(f)$, $x = U_1(f) \circ P_1(f)(x) + U_2(f) \circ P_2(f)(x)$, avec $U_1(f) \circ P_1(f)(x) \in \ker P_2(f)$ et $U_2(f) \circ P_2(f)(x) \in \ker P_1(f)$, en utilisant le fait que deux polynômes en f commutent. Par ailleurs, si $x \in \ker P_1(f) \cap \ker P_2(f)$, alors $x = U_1(f) \circ P_1(f)(x) + U_2(f) \circ P_2(f)(x) = 0$. On déduit de ces résultats que $\ker P_1(f)$ et $\ker P_2(f)$ sont supplémentaires dans $\ker(P_1P_2)(f)$.
2. Établissons la récurrence. Soit $m \geq 2$. On suppose que le résultat est établi pour toute famille de m polynômes deux à deux premiers entre eux. Soit $P_1, \ldots, P_{m+1}$ une famille de polynômes deux à deux premiers entre eux. Alors $\prod_{k=1}^{m} P_k$ et P_{m+1} sont premiers entre eux, et l'initialisation permet d'écrire

$$\ker\Big(\prod_{k=1}^{m+1} P_k\Big)(f) = \ker\Big(\prod_{k=1}^{m} P_k\Big)(f) \oplus \ker P_{m+1}(f).$$

   On conclut en appliquant l'hypothèse de récurrence.

Montrons maintenant que les projections sont des polynômes en f : soit $P_1, ..., P_m$ une famille de polynômes deux à deux premiers entre eux, et soit $j \in \{1, \ldots, m\}$. Comme P_j et $\prod_{k=1,k\neq j}^{m} P_k$ sont premiers entre eux, il existe des polynômes U_j et V_j tels que $U_jP_j + V_j \prod_{k=1,k\neq j}^{m} P_k = 1$. Posons $p_j = (V_j \prod_{k=1,k\neq j}^{m} P_k)(f)$ et vérifions que p_j est bien le projecteur de $\ker P_j(f)$ parallèlement à $\oplus_{k=1,k\neq j}\ker P_k(f)$. En effet, tout élément $x \in \ker P_j(f)$ vérifie $x = (U_jP_j)(f)(x) + (V_j \prod_{k=1,k\neq j}^{m} P_k)(f)(x) =$

$p_j(x)$, et tout élément $x \in \oplus_{k=1,k\neq j}\ker P_k(f)$ de l'image de $P_j(f)$ satisfait $p_j(x) = (V_j \prod_{k=1,k\neq j} P_k)(f)(x) = 0$[25], et p_j coïncide avec le projecteur recherché sur deux sous-espaces supplémentaires, donc ces deux endomorphismes sont égaux. □

Théorème 13 (Décomposition de Dunford)**.** *Soit $f \in \mathcal{L}(E)$ annulé par un polynôme scindé P. Alors il existe un unique couple d'endomorphisme (d, n) tel que :*

1. *$f = n + d$,*
2. *n et d commutent,*
3. *n soit nilpotent,*
4. *d soit diagonalisable.*

De plus, n et d sont des polynômes en f.

Démonstration du théorème.

1. Démontrons l'existence d'un tel couple. En écrivant $P = \prod_{k=1}^{m}(X - \lambda_k)^{\alpha_k}$, on a par application du lemme des noyaux que $E = \oplus_{k=1}^{m}\ker(f - \lambda_k \mathrm{id})^{\alpha_k} = \oplus_{k=1}^{m} F_{\lambda_k}$. Sur chacun de ces sous-espaces stables par f (car noyaux de polynômes en f), les endomorphismes $f|_{F_{\lambda_j}} = \lambda_j \mathrm{id}|_{F_{\lambda_j}} + (f - \lambda_j \mathrm{id})_{F_{\lambda_j}}$ sont sommes d'une homothétie et d'un endomorphisme nilpotent. On note p_j les projecteurs définis comme dans le lemme. Posons $d = \sum_{k=1}^{m} \lambda_k p_k$ et $n = f - d$: ce sont des polynômes en f. On a :
   (a) $f = d + n$,
   (b) d est un polynôme en f et commute donc avec les polynômes en f, en particulier avec $n = f - d$,
   (c) n est nilpotent, car l'endomorphisme induit par n sur chacun des sous-espaces F_{λ_j} est nilpotent,
   (d) d est diagonalisable, car somme de projections (donc diagonalisables, car annulant le polynôme $X(X-1)$) qui commutent deux à deux, et sont donc simultanément diagonalisables.
2. Démontrons à présent l'unicité d'un tel couple. Soit (d, n) le couple construit précédemment et $(\tilde{d}, \tilde{n})$ un couple satisfaisant aux conditions de la proposition. Comme $\tilde{d}$ commute avec $\tilde{n}$, et donc avec $f = \tilde{d} + \tilde{n}$, il commute avec tous les polynômes en f, par conséquent avec d. De même, $\tilde{n}$ commute avec n. On a alors $d - \tilde{d} = \tilde{n} - n$, et comme $d - \tilde{d}$ est diagonalisable par diagonalisation simultanée et $\tilde{n} - n$ est nilpotent par la formule du binôme de Newton, chacun de ces endomorphismes est diagonalisable et nilpotent. Ils sont donc tous les deux nuls, et alors $d = \tilde{d}$ et $n = \tilde{n}$.

□

25. À nouveau, faire commuter les polynômes en f...

1.13.2 Références

[Mar07], pp. 7-8, 22.

1.13.3 Questions classiques

1. *Comment prouvez-vous le résultat sur la diagonalisation simultanée :* Par récurrence forte sur la dimension de l'espace. Pour $n = 1$, n'importe quelle base convient. Si $n \geq 1$, on distingue deux cas : soit tous les endomorphismes sont des homothéties, et dans ce cas n'importe quel base convient, soit il existe un endomorphisme qui n'est pas une homothétie. On le diagonalise, et on considère que $E = E_{\lambda_1} \oplus (\oplus_{k=2}^{r}) E_{\lambda_k} = E_{\lambda_1} \oplus F$, avec λ_1 une valeur propre de notre endomorphisme et F de dimension non-nulle. Comme sur chacun des deux sous-espaces supplémentaires sont stables par tous les endomorphismes (en tant que noyaux de polynômes en un des endomorphismes), on peut considérer leur restriction à ces sous-espaces. En remarquant enfin qu'un endomorphisme diagonalisable reste diagonalisable lorsque l'on considère sa restriction à un sous-espace stable (via le fait que u diagonalisable implique qu'il existe P scindé à racines simples tel que $P(u) = 0$, et donc $P(u|_E) = P(u)|_E = 0$, ce qui prouve que $u|_E$ est diagonalisable), on peut appliquer l'hypothèse de récurrence et conclure en concaténant les deux bases ainsi obtenues.

1.13.4 Remarques

— Si l'on a le temps, on peut faire en application le lemme qui initialise le théorème de Liapounov.

— Le lemme des noyaux reste valable en dimension infinie.

— Nelson Dunford : mathématicien américain, 1906-1986.

1.14 Réduction des endomorphismes normaux

1.14.1 Développement

Théorème 14. *Soit E un espace euclidien et $u \in \mathcal{L}(E)$ un endomorphisme normal. Alors il existe une base orthonormée $\mathcal{B}$ de E telle que*

$$[u]_{\mathcal{B}} = \begin{pmatrix} \lambda_1 & & & & & \\ & \ddots & & & 0 & \\ & & \lambda_r & & & \\ & & & \tau_1 & & \\ & 0 & & & \ddots & \\ & & & & & \tau_s \end{pmatrix},$$

où pour tout $i \in \{1, \dots, n\}$ on a $\lambda_i \in \mathbb{R}$ et pour tout $j \in \{1, \dots, s\}$ on a $\tau_j = \begin{pmatrix} a_j & -b_j \\ b_j & a_j \end{pmatrix} \in \mathscr{M}_2(\mathbb{R})$.

Lemme 17. *Soit $u \in \mathcal{L}(E)$ et soit F un sous-espace vectoriel stable par u. Alors $F^\perp$ est stable par u^*. Si de plus u est normal et E_λ est un sous-espace propre de u (associé à une valeur propre λ), alors $E_\lambda^\perp$ est stable par u.*

Démonstration du lemme. Soit $y \in F^\perp$. Soit $x \in F$ quelconque. On a que

$$\langle x, u^*(y) \rangle = \langle u(x), y \rangle = 0$$

par hypothèse sur u. Si de plus u est normal, u et u^* commutent et E_λ est stable par u^* [26], et donc $E_\lambda^\perp$ est stable par $(u^*)^* = u$. □

Lemme 18. *On suppose que* $\dim E = 2$. *Soit $u \in \mathcal{L}(E)$ un endomorphisme normal n'admettant pas de valeurs propres réelles. Dans toute base $\mathcal{B}$ orthonormale de E, la matrice de u est de la forme*

$$[u]_{\mathcal{B}} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \text{ avec } b \neq 0.$$

Démonstration du lemme. Écrivons

$$M = [u]_{\mathcal{B}} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

26. On se rappelle que E_λ est le noyau d'un polynôme en u.

On a $b \neq 0$ puisque u est sans valeur propre réelle. Comme u est normal, $M^tM = {}^tMM$. Parmi les équations dérivant de cette égalité, on trouve $a^2 + c^2 = a^2 + b^2$ et $ab + cd = ac + bd$. La première de ces égalités entraîne $b = c$ ou $b = -c$. Si $b = c$, alors M est symétrique et donc diagonalisable, ce qui est impossible à nouveau car u est sans valeur propre réelle. Donc $b = -c$: la deuxième égalité se réécrit comme $2(a-d)b = 0$, et comme $b \neq 0$ on a $a = d$, et la matrice a bien la forme annoncée. □

Démonstration du théorème. On procède par récurrence forte sur $n = \dim E$. Pour $n = 1$, c'est évident. Supposons que le résultat est vrai jusqu'au rang $n-1$ et montrons le au rang n. Deux cas se présentent :

1. Si u admet une valeur propre réelle λ, on pose $E_\lambda = \ker(u - \lambda \mathrm{id}_E)$. Le sous-espace vectoriel $F = E_\lambda^\perp$ est stable par u et par u^*. Comme $u|_F$ et $u|_F^* = u^*|_F$ commutent et que $\dim F \leq n-1$, il existe d'après l'hypothèse de récurrence une base orthonormée $\mathcal{B}_1$ de F telle que $[u|_F]_{\mathcal{B}_1}$ a la forme demandée. Si $\mathcal{B}_2$ désigne une base orthonormée de E, on a que $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ est une base orthonormée de E dans laquelle $[u]_{\mathcal{B}}$ a la forme demandée.

2. Si u n'admet pas de valeurs propres réelles, on note $Q = X^2 - 2\alpha X + \beta$ un facteur irréductible du polynôme caractéristique de u (i.e. $\alpha^2 - \beta < 0$), et $N = \ker Q(u)$.
   On a $N \neq \{0\}$. En effet, comme Q est irréductible dans $\mathbb{R}$, on peut écrire $Q = (X-\lambda)(X-\overline{\lambda})$, où $\lambda \in \mathbb{C}$. Soit M la matrice de u dans une base de E. Le nombre complexe λ est racine de Q, et comme Q divise le polynôme caractéristique de M, on a $\det(M - \lambda \mathrm{I}_n) = 0$. Donc

$$\det Q(u) = \det Q(M) = \det(M - \lambda \mathrm{I}_n) \det(M - \overline{\lambda}\mathrm{I}_n) = 0,$$

   ce qui prouve que $N = \ker Q(u) \neq \{0\}$.
   Comme N est stable par u en tant que noyau d'un polynôme en u, et stable par u^* comme u et u^* commutent, on peut considérer $v = u|_N$. On a $v^* = u^*|_N$, de sorte que l'endomorphisme $v^*v = (u^*u)|_N$ est symétrique et admet donc une valeur propre $\mu \in \mathbb{R}$ [27]. Soit un $x \in N \setminus \{0\}$ un vecteur propre associé à la valeur μ, i.e. tel que $v^*v(x) = \mu x$. Posons $F = \mathrm{vect}(x, u(x))$. Comme u n'admet pas de valeur propre réelle, x et $u(x)$ forment une famille libre donc $\dim F = 2$. Le sous-espace vectoriel F est stable par u puisque comme $x \in N$, on a $u^2(x) = 2\alpha u(x) - \beta x$.

27. Car, en considérant une valeur propre complexe λ et un vecteur propre (a priori à coefficients complexes) X, on a en considérant la matrice d'un tel endomorphisme dans une base orthonormée que $\lambda {}^tX\overline{X} = {}^t\overline{X}MX = t({}^tX{}^tM\overline{X})$. Or $M\overline{X} = \overline{\lambda X}$ car M est à coefficients réels, et on peut simplifier par ${}^t\overline{X}X = {}^tX\overline{X} = \sum |x_i|^2 \neq 0$, d'où $\lambda = \overline{\lambda}$ et $\lambda \in \mathbb{R}$.

Nous allons montrer que F est également stable par u^*. Remarquons tout d'abord que l'égalité précédente entraîne $F = \text{vect}(u(x), u^2(x))$ (ceci car $\beta \neq 0$, Q étant irréductible sur $\mathbb{R}$). On écrit maintenant

$$u^*[u(x)] = v^*v(x) = \mu x \in F,$$

et comme u et u^* commutent,

$$u^*[u^2(x)] = u \circ u^*[u(x)] = u(\mu x) = \mu u(x) \in F,$$

ce qui achève de montrer que F est stable par u^*.
Comme $(u|_F)^* = (u^*)|_F$, $u|_F$ est un endomorphisme normal. D'après le second lemme, dans une base orthonormée $\mathcal{B}_2$ de F, la matrice de $u|_F$ est de la forme

$$\tau = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Maintenant, on a vu que F est stable par u^*, donc $F^\perp$ est stable par $(u^*)^* = u$ d'après le premier lemme. On a aussi que, F étant stable par u, $F^\perp$ est stable par u^*. Donc $(u|_{F^\perp})^* = (u^*)|_{F^\perp}$, ce qui prouve que $u_{F^\perp}$ est normal. Comme $\dim F^\perp = n - 2 < n$, l'hypothèse de récurrence assure l'existence d'une base $\mathcal{B}_1$ orthonormée dans laquelle la matrice de $u|_{F^\perp}$ a la bonne forme. La base $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ est alors une base orthonormée dans laquelle la matrice de u a la forme demandée.

□

1.14.2 Références

[Gou09], pp. 258-260.

1.14.3 Questions classiques

1.

1.14.4 Remarques

—

1.15 Générateurs de $\mathrm{GL}_n(K)$ et de $\mathrm{SL}_n(K)$

1.15.1 Développement

Proposition 9. *Soit $n \geq 2$ et K un corps commutatif.*

1. *On appelle matrice de transvection toute matrice de la forme $T_{ij}(\lambda) = \mathrm{I}_n + \lambda E_{ij}$, où $i \neq j$ et $\lambda \in K$. On appelle matrice de dilatation toute matrice de la forme $D_i(\alpha) = \mathrm{I}_n + (\alpha - 1)E_{ii}$ avec $\alpha \in K^*$. Alors l'ensemble des matrices de transvection engendre le groupe $\mathrm{SL}_n(K)$ tandis que l'ensemble des matrices de transvection et de dilatation engendre le groupe $\mathrm{GL}_n(K)$.*
2. *Si $\operatorname{car} K = 0$, $\mathrm{GL}_n(K)$ est engendré par l'ensemble des matrices inversibles diagonalisables.*
3. ***Application :** Si $K = \mathbb{R}$ ou $\mathbb{C}$, $\mathrm{SL}_n(K)$ est connexe par arcs.*

Démonstration. 1. Notons que toutes les matrices de transvection sont de déterminant 1. Le groupe qu'elles engendrent est donc inclus dans $\mathrm{SL}_n(K)$. La multiplication à gauche (resp. à droite) par une matrice de transvection élémentaire $T_{ij}(\lambda)$ revient à effectuer l'opération élémentaire $L_i \leftarrow L_i + \lambda L_j$ (resp. $C_j \leftarrow C_j + \lambda C_i$). Notons qu'il est possible de réaliser l'échange de deux lignes (ou de deux colonnes) uniquement à l'aide de transvections modulo un changement de signe : en effet, la matrice $T_{ij}(1)T_{ji}(-1)T_{ij}(1)$ a pour effet (par multiplication à gauche) de remplacer L_i par L_j et L_j par $-L_j$, les autres lignes étant invariantes. Il n'est évidemment pas possible de réaliser l'échange de deux lignes sans apparition de ce signe moins puisque cette opération change le signe du déterminant.
Soit $A \in \mathrm{GL}_n(K)$. En appliquant le pivot de Gauss, nous allons transformer A en une matrice de dilatation uniquement en utilisant des matrices de transvection. Comme A est inversible, sa première colonne n'est pas nulle. Si $a_{i1} \neq 0$ avec $i \geq 2$, l'opération $L_1 \leftarrow L_1 - \frac{a_{11}-1}{a_{i1}}$ permet de mettre un 1 en position $(1,1)$. Si tous les coefficients a_{i1} pour $i \geq 2$ sont nuls, on effectue l'échange de lignes $L_1 \leftarrow L_2$ et $L_2 \leftarrow -L_1$ pour se ramener au cas précédent. En utilisant le coefficient $(1,1)$ comme pivot, une succession 'opérations sur les lignes puis sur les colonnes permet d'annuler tous les autres coefficients de la première ligne et de la première colonne. Autrement dit, il existe des matrices de transvection $M_1, \ldots, M_p$ et $N_1, \ldots, N_q$ telles que

$$M_p \ldots M_1 A N_1 \ldots N_q = \begin{pmatrix} 1 & 0 \\ 0 & A_1 \end{pmatrix},$$

où $A_1 \in \mathrm{GL}_{n-1}(K)$.
On recommence le même algorithme sur la matrice A_1, et ainsi de suite.

On aboutit à la fin de cet algorithme à une matrice diagonale $\mathrm{diag}(1,\dots,1,\alpha)$, où le scalaire α n'est autre que $\det A$. On vient donc de montrer que pour toute matrice inversible A, il existe des matrices de transvection $U_1,\dots,U_r$ et $V_1\dots,V_s$ telles que

$$A = U_r \dots U_1 D_n(\det A) V_1 \dots V_s.$$

Ceci permet de répondre à la question : toute matrice $A \in \mathrm{SL}_n(K)$ s'écrit comme produit de matrices de transvection [28] et toute matrice $A \in \mathrm{GL}_n(K)$ est produit de matrices de transvection et de dilatation.

2. Comme on sait à présent que $\mathrm{GL}_n(K)$ est engendré par les matrices de dilatation et de transvection, montrons que ces deux types de matrices sont engendrés par des matrices inversibles diagonalisables. Les premières sont diagonales inversibles. Pour T une matrice de transvection, il suffit d'écrire $M = D^{-1}(DM)$ où D est la matrice diagonale $\mathrm{diag}(1,\dots,n)$: la matrice D^{-1} est diagonale inversible et la matrice DM est triangulaire avec la même diagonale que D : il s'en suit qu'elle est diagonalisable [29], et l'ensemble des matrices diagonalisables inversibles engendre donc tout le groupe $\mathrm{GL}_n(\mathbb{R})$.
3. Montrons que toute matrice $A \in \mathrm{SL}_n(K)$ est reliée par un arc continu à l'identité I_n. D'après le premier point, il existe une partie X contenue dans l'ensemble des couples $(i_j) \in \{1,\dots,n\}^2$ avec $i \neq j$ et une famille $(\lambda_C)_{C\in X}$ de K telle que A soit le produit des transvections $T_C(\lambda_C)$:

$$A = \prod_{C\in X} T_c(\lambda_C).$$

On pose alors $\varphi : t \in [0,1] \mapsto A_t = \prod_{C\in X} T_C(t\lambda_C)$. On obtient un arc continu (car polynomial) qui relie $\varphi(0) = \mathrm{I}_n$ à $\varphi(1) = A$ dans $\mathrm{SL}_n(K)$, qui est ainsi connexe par arcs.

□

1.15.2 Références

[FGN09], pp. 177-179.

1.15.3 Questions classiques

1. *Que peut-on dire à propos de la connexité par arcs de* $\mathrm{GL}_n(\mathbb{C})$ *et de* $\mathrm{GL}_n(\mathbb{R})$: Pour $\mathrm{GL}_n(\mathbb{C})$, on décompose $A = \prod_{(C\in X, C'\in X'} T_C(\lambda_C) D_{C'}(\lambda_{C'})$ et on utilise la connexité par arcs de $\mathbb{C}^*$ pour relier les $\lambda_{C'}$ à 1 sans passer par 0.

28. Car $D_n(1) = \mathrm{I}_n$.
29. Car son polynôme caractéristique est scindé à racines simples.

Pour $\mathrm{GL}_n(\mathbb{R})$, on suppose par l'absure qu'il est connexe par arcs : il est alors connexe, et sont image par det est connexe. Or $\det(\mathrm{GL}_n(\mathbb{R})) = \mathbb{R}^*$, d'où la contradiction.

1.15.4 Remarques

— On a adapté la preuve du second point pour l'étendre à tout corps de caractéristique nulle.

— La topologie mise en jeu dans le troisième point est celle issue d'une norme quelconque sur $\mathscr{M}_n(K)$, par exemple $||M|| = \sup_{i,j\in\{1,\dots,n\}^2} |a_{ij}|$.

1.16 Théorème de Kronecker

1.16.1 Développement

Théorème 15. *On pose, pour $n \in \mathbb{N}^*$,*

$$\Omega_n := \{P \in \mathbb{Z}[X] \ ; \ P \text{ unitaire}, \deg P = n, z \in Z(P) \Longrightarrow 0 < |z| \leq 1\},$$

où $Z(P)$ désigne l'ensemble des racines complexes du polynôme P. Si $P \in \Omega_n$, alors les racines de P sont des racines de l'unité.

Démonstration. Montrons que Ω_n est fini. Soit $P = X^n + a_1 X^{n-1} + \cdots + a_n = (X - z_1)\dots(X - z_n) \in \Omega_n$. Remarquons que l'on doit avoir $a_n \neq 0$ et $0 < |z_i| \leq 1$. On note $\sigma_1, \dots, \sigma_n$ les fonctions symétriques élémentaires[30] évalués en $(z_1, \dots, z_n)$. La relation coefficients-racines, affirmant que $a_p = (-1)^p \sigma_p$[31], assure que

$$|a_p| = |\sigma_p| = |\sum_{i_1 < \cdots < i_p} z_{i_1} \dots z_{i_p}| \leq \sum_{i_1 < \cdots < i_p} 1 = \binom{n}{p}.$$

Ainsi, P n'admet qu'un nombre fini de coefficients possibles et Ω_n est fini.
Notons à présent, pour $k \in \mathbb{N}^*$, $P_k = (X - z_1^k)\dots(X - z_n^k)$. Remarquons que $P = P_1$. On va montrer que $P_k \in \Omega_n$: soit $k \geq 2$. On a que P_k est unitaire de degré n et que $0 < |z_i^k| \leq 1$. Montrons que ses coefficients sont entiers : on pose $Q_k = X^k - Y \in \mathbb{Z}[X, Y]$ et

$$R_k = \mathrm{Res}_X(P, Q_k) = \begin{vmatrix} 1 & & & & 1 & & \\ a_1 & \ddots & & & 0 & \ddots & \\ \vdots & \ddots & \ddots & & \vdots & \ddots & 1 \\ a_n & & \ddots & 1 & 0 & & 0 \\ & \ddots & & a_1 & Y & \ddots & \vdots \\ & & \ddots & \vdots & & \ddots & 0 \\ & & & a_n & & & Y \end{vmatrix}$$

Comme $Q \in \mathbb{Z}[X, Y]$ et $P \in \mathbb{Z}[X] \subset \mathbb{Z}[X, Y]$, on a que $R_k \in \mathbb{Z}[Y]$. Exprimons à présent le résultant en fonction des racines de P : la formule donne

$$R_k = \mathrm{Res}_X(P, Q_k) = \prod_{i=1}^{n} Q_k(z_i) = \prod_{i=1}^{n} (z_i^k - Y) = (-1)^n P_k(Y).$$

30. On a $\sigma_1(X_1, \dots, X_n) = X_1 + \cdots + X_n, \sigma_2(X_1, \dots, X_n) = \sum_{i<j} X_1 X_2, \dots, \sigma_n(X_1, \dots, X_n) = X_1 \dots X_n$.

31. Et se démontrant par récurrence sur p.

Finalement, $P_k = (-1)^n R_k \in \mathbb{Z}[X]$ et $P_k \in \Omega_n$.
Achevons de prouver le théorème : comme Ω_n est fini, il en est de même de l'ensemble $Z_n = \cup_{Q \in \Omega_n} Z(Q)$, un polynôme non-nul ayant un nombre fini de racines par division euclidienne. D'après ce qui précède, cet ensemble contient tout les z_i^k : l'application

$$\varphi_i : \begin{array}{ccc} \mathbb{N} & \longrightarrow & Z_n \\ k & \longmapsto & z_i^k \end{array}$$

étant bien définie et ne pouvant être injective, on en déduit l'existence de $p > q$ tels que $z_i^p = z_i^q$, et comme z_i est non-nul on obtient finalement $z_i^{p-q} = 1$. □

Corollaire 4. *Si on suppose de plus P irréductible, alors P est un polynôme cyclotomique.*

Démonstration. On a d'après le théorème que les racines de P sont des racines de l'unité. Comme P est irréductible, ses racines complexes sont simples, sinon on aurait que $\text{pgcd}(P, P') = P$ par irréductibilité, puis nécessairement $P' = 0$ et donc $P = 1$, mais on a supposé P irréductible (et donc non inversible par définition), d'où la contradiction. On a alors $P \mid X^N - 1$ pour N le ppcm des ordres des racines de l'unité impliquées. Enfin, comme $X^N - 1 = \prod_{d|n} \Phi_d$ avec Φ_d le $d-$ième polynôme cyclotomique, à coefficients dans $\mathbb{Z}$ et irréductible, on a notre résultat. □

Corollaire 5. *Tout polynôme de $\mathbb{Z}[X]$ ayant ses racines dans $D(0,1)$ est un produit de polynômes cyclotomiques et de puissances de X.*

1.16.2 Références

[Szp09], p. 573.

1.16.3 Questions classiques

1.

1.16.4 Remarques

— Le théorème est que ces racines sont des racines de l'unité : le fait qu'elles soient de norme 1 n'est pas étonnant car on a $P(0) = \lambda_1 \dots \lambda_n \in \mathbb{Z} \setminus \{0\}$ où les $0 < |\lambda_i| \leq 1$ sont les racines de P, et donc $P(0) = |\lambda_1| \dots |\lambda_n| = 1$, donc chacune des racines est de norme 1.

— Dans la seconde partie de la preuve, on retrouve P_k comme un polynôme en Y alors qu'on l'a introduit comme un polynôme en X : ne pas se laisser embrouiller.

— Leopold Kronecker : mathématicien et logicien allemand, 1823-1891.

1.17 Loi de réciprocité quadratique

1.17.1 Développement

Théorème 16. *Soient p et q deux nombres impairs distincts. On a :*

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

On aura besoin du lemme suivant :

Lemme 19. *Soit p un premier impair et $a \in \mathbb{F}_p^*$. On a :*

$$|\{x \in \mathbb{F}_p \ ; \ ax^2 = 1\}| = 1 + \left(\frac{a}{p}\right).$$

Démonstration du lemme. Par définition, $(\frac{a}{p}) = a^{\frac{p-1}{2}}$. On a que $(a^{\frac{p-1}{2}})^2 = 1$ par le théorème de Lagrange, donc $a^{\frac{p-1}{2}}$ est racine de $X^2 - 1 \in \mathbb{F}_p[X]$ et vaut donc ± 1. Or, on a que $\mathbb{F}_p^{*2} = \{x \in \mathbb{F}_p^* \ ; \ x^{\frac{p-1}{2}} = 1\}$: le premier ensemble est inclus dans le second, qui est de cardinal au plus $\frac{p-1}{2}$, alors que le morphisme surjectif $\mathbb{F}_p^* \longrightarrow \mathbb{F}_p^{*2}$ défini par $x \mapsto x^2$ est de noyau $\{-1, +1\}$ qui est de cardinal 2 car $p > 2$. Par le théorème d'isomorphisme, cet ensemble est de cardinal $\frac{p-1}{2}$ et on a bien égalité. Finalement,

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ si } a \text{ est un carré dans } \mathbb{F}_p^* \\ -1 \text{ si } a \text{ n'est pas un carré dans } \mathbb{F}_p^* \end{cases},$$

et le leme en découle. □

Démonstration du théorème. L'idée est de calculer de deux façons différentes le cardinal de la "sphère"

$$X = \{(x_1, \ldots, x_p) \in \mathbb{F}_q^p \ ; \ \sum_{i=1}^{p} x_i^2 = 1\}.$$

1. Première méthode : Faisons agir $\mathbb{Z}/p\mathbb{Z}$ par permutation circulaire sur $\mathbb{F}_q^p$:

   $$\forall k \in \mathbb{Z}/p\mathbb{Z}, \forall (x_1, \ldots, x_p) \in \mathbb{F}_q^p, k \cdot (x_1, \ldots, x_p) = (x_{1+k}, \ldots, x_{n+k}),$$

   où les indices sont vus modulos p : $x_{l+p} = x_l$ pour tout p. Les orbites de $\mathbb{Z}/p\mathbb{Z}$ dans X sont de deux types : les singletons $\{(x, \ldots, x)\}$, où $x \in \mathbb{F}_q$, dont les stabilisateurs sont égaux à $\mathbb{Z}/p\mathbb{Z}$, et toutes les autres qui ont

nécessairement un stabilisateur trivial[32] et sont alors de cardinal p par la formule des classes. Le nombre d'orbites-singletons est le nombre de solutions de l'équation $px^2 = 1$ dans $\mathbb{F}_q$, qui par le lemme vaut $1 + (\frac{p}{q})$. En réduisant modulo p, il vient

$$|X| \equiv 1 + \left(\frac{p}{q}\right) \mod p.$$

2. Deuxième méthode : Les matrices $p \times p$ à coefficients dans $\mathbb{F}_q$, I_p et

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

avec $a = (-1)^{\frac{p-1}{2}} =: (-1)^d$, sont symétriques et ont même rang p ainsi que même déterminant 1 (donc même discriminant) : elles sont donc congruentes. Un changement de variables linéaire identifie X à l'ensemble

$$X' = \{(y_1, \dots, y_d, z_1, \dots, z_d, t) \in \mathbb{F}_q^p \ ; \ 2(y_1 z_1 + \cdots + y_d z_d) + at^2 = 1\}$$ [33].

Dénombrons les points de X' :

(a) Si $y_1 = \cdots = y_d = 0$: chaque valeur de t telle que $at^2 = 1$ détermine q^d tels points, ce qui par le lemme donne $q^d(1 + (\frac{a}{q}))$ points en tout,

(b) Si l'un des y_i est non-nul, alors à $(y_1, \dots, y_d)$ et t fixés, il reste à choisir $(z_1, \dots, z_d)$ dans un hyperplan affine de $\mathbb{F}_q^d$: il y a

$$\underbrace{(q^d - 1)}_{\substack{\text{nombre de } (y_1,\dots,y_n) \\ \text{convenant}}} \quad \underbrace{q}_{\substack{\text{nombre de } t \\ \text{convenant}}} \quad \underbrace{q^{d-1}}_{\substack{\text{nombre de } (z_1,\dots,z_n) \\ \text{convenant}}}$$

tels points en tout.

Finalement, $|X| = q^d(q^d + (\frac{a}{q}))$.

En comparant les deux méthodes, on a obtenu

$$|X| = q^{\frac{p-1}{2}}\left(q^{\frac{p-1}{2}} + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right) \equiv 1 + \left(\frac{p}{q}\right) \mod p,$$

ce qui donne la loi de réciprocité quadratique après simplification. □

32. Les seuls sous-groupes de $\mathbb{Z}/p\mathbb{Z}$ étant $\{0\}$ et $\mathbb{Z}/p\mathbb{Z}$.

33. I.e. en notant u l'endomorphisme tel que $q(x) = q'(u(x))$, on a que u induit une bijection entre X et X'.

1.17.2 Références

[CG13], pp. 182-186.

1.17.3 Questions classiques

1.

1.17.4 Remarques

— On a défini le symbole de Legendre sur les $\mathbb{F}_p$: on aurait pu le définir sur $\mathbb{Z}$, mais on aurait du travailler modulo quelque chose tout le long de la preuve.

1.18 Groupes des K-automorphismes de $K(X)$

1.18.1 Développement

Théorème 17. *L'application qui associe à une matrice* $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *la substitution*

$$\sigma_M : \begin{array}{ccc} K(X) & \longrightarrow & K(X) \\ F & \longmapsto & F\left(\frac{dX-b}{-cX+a}\right) \end{array}$$

définit un morphisme de groupes $\sigma : \mathrm{GL}_2(K) \to \mathrm{Aut}_K(K(X))$. *De plus, ce morphisme se factorise en un isomorphisme* $\tilde{\sigma} : \mathrm{PGL}_2(K) \to \mathrm{Aut}_K(K(X))$.

Démonstration. Considérons un produit de matrices

$$MM' = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}.$$

Il lui est associé la substitution $\sigma_{MM'}$ qui a pour action

$$F \mapsto F\Big(\frac{(cb'+dd')X-(ab'+bd')}{-(ca'+dc')X+(aa'+bc')}\Big).$$

Par ailleurs, $\sigma_{M'}(F) = F(\frac{d'X-b'}{-c'X+a'})$ et

$$\sigma_M(\sigma_{M'}(F)) = F\Big(\frac{d'\frac{dX-b}{-cX+a}-b'}{-c'\frac{dX-b}{-cX+a}+a'}\Big) = F\Big(\frac{(cb'+dd')X-(ab'+bd')}{-(ca'+dc')X+(aa'+bc')}\Big).$$

On obtient donc que $\sigma_{MM'} = \sigma_M \circ \sigma_{M'}$. En particulier, $\sigma_M \circ \sigma_{M^{-1}} = \sigma_{M^{-1}} \circ \sigma_M = \sigma_{\mathrm{I}_2} = \mathrm{id}_{K(X)}$, ce qui montre que σ_M est un K-automorphisme de $K(X)$. De plus, σ est un morphisme de groupes.

Montrons à présent que ce morphisme se factorise sur $\mathrm{PGL}_2(K)$, i.e. que son noyau est constitué du groupe des homothéties et qu'il est surjectif.

Il est clair que $\sigma_{\lambda \mathrm{I}_2} = \mathrm{id}_{K(X)}$ pour tout $\lambda \in K^*$. Réciproquement, si σ_M est l'identité, alors en particulier $X = \frac{dX-b}{-cX+a}$. Ainsi $-cX^2 + aX = dX - b$ et cette égalité entre polynômes implique $b = c = 0$ et $a = d$, donc M est une homothétie.

Ensuite, soit $\varphi : K(X) \to K(X)$ un K-automorphisme de corps. La fraction rationnelle $A = \varphi(X)$ détermine entièrement φ, car, d'après les propriétés

d'un K-morphisme de corps, pour toute fraction rationnelle $F = F(X)$ on a $\varphi(F(X)) = F(\varphi(X)) = F(A)$. On portera notre attention sur le sous-anneau $K[A]$ et le sous-corps $K(A)$ de $K(X)$ engendrés par A, et les inclusions $K \subset K(A) \subset K(X)$. En fait $K(A) = K(X)$, car c'est l'image de φ qui est bijectif. En particulier, A est non-constante. On peut écrire $A = \frac{P}{Q}$ où P et Q sont des polynômes en X non-nuls et premiers entre eux : l'objectif est de montrer que $\deg(P), \deg(Q) \leq 1$. On introduit pour cela une nouvelle indéterminée et le polynôme non-nul

$$\Phi = Q(T)A - P(T) \in K(A)[T].$$

On note $n = \max(\deg(P), \deg(Q))$ son degré. Ce polynôme annule X, par définition de A : montrons que c'est le polynôme minimal de X sur $K(A)$, et on aura ainsi $n = \deg(\Phi) = [K(X) : K(A)] = [K(X) : K(X)] = 1$.

Comme X est algébrique sur $K(A)$, on a que $K(X)$ est de dimension finie sur $K(A)$, et ainsi par multiplicativité des degrés que $K(A)$ est de dimension infinie sur K (l'extension $K \subset K(A)$ est transcendante). Ainsi, $K(A)$ est isomorphe à un corps de fractions rationnelles en une indéterminée. Par suite, $K[A]$ est isomorphe à un anneau de polynômes en une indéterminée.

Vu comme polynôme en A à coefficients dans $K(T)$, le polynôme Φ est irréductible car de degré 1. De plus, Φ est en fait à coefficients dans $K[T]$ est son contenu vaut 1, par choix de P et de Q. Le théorème de Gauss assure que Φ est un irréductible de $K[T][A]$, donc par isomorphisme de $K[A][T]$ et à nouveau par le théorème de Gauss de $K(A)[T]$: c'est bien le polynôme minimal de X sur $K(A)$.

On écrit finalement $A = \frac{dX-b}{-cX+d}$, et comme A est non-constante, il vient $ad - bc \neq 0$. Ainsi $\varphi = \sigma_M$ avec

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

□

[Szp09], pp. 607-608.

1.18.2 Questions classiques

1. *Pourquoi le polynôme $\Phi \in K[A][T]$ est-il non-nul* : S'il était nul, chacun de ses coefficients seraient nuls dans $K[A]$. En particulier pour un coefficient non-nul q de Q on aurait $Aq = p$ et ainsi $A \in K$, ce qui est contradictoire avec A non-constante.

1.18.3 Remarques

— On sait déjà que la substitution est un endomorphisme, exhiber un inverse suffit à montrer que σ est bien définie.

— Le fait que l'on définisse la substitution à l'aide de la transposée de la comatrice de M permet d'avoir affaire à un morphisme et non à un anti-morphisme.

— En tant que K-automorphisme, on s'attend à ce que φ "envoie une indéterminée sur une indéterminée".

1.19 L'hexagone et les représentations de D_6

1.19.1 Développement

On se propose de caractériser les sous-groupes distingués à l'aide de la table de caractères, et de retrouver de cette manière les sous-groupes distingués de D_6.

Proposition 10. *Soit G un groupe fini de caractères irréductibles $\chi_1, \dots, \chi_m$. Alors les sous-groupes distingués H de G sont de la forme*

$$H = \cap_{i \in I} \ker \chi_i, \text{ où } I \subset \{1, \dots, m\}.$$

Démonstration. On commence par montrer que, si $\rho : G \to \mathrm{GL}(V)$ est une représentation, alors $\ker \chi := \{g \in G \ ; \ \chi(g) = \dim V\} = \ker \rho$. En effet, comme G est fini, le polynôme $X^{|G|} - 1$ annule tous les $\rho(g)$: les racines λ de ces endomorphismes sont donc des racines de l'unité. En particulier, on a que

$$\chi(g) = \dim V \Longrightarrow \sum_{i=1}^{\dim V} \lambda_i = \dim V,$$

et en passant au module on est dans le cas d'égalité de l'inégalité triangulaire, et on en déduit que tous les λ_i valent 1. Ceci signifie que $\rho(g) = \mathrm{I}_{\dim(V)}$, et l'égalité est ainsi établie. Passons à la preuve du théorème : il est clair par ce qui précède que les intersections des noyaux des caractères sont bien des sous-groupes distingués. Pour l'inclusion réciproque, on considère H un sous-groupe distingué de G. La représentation régulière $\rho_{G/H}$ de G/H est en particulier fidèle, et en composant avec la projection canonique π on obtient une représentation $\rho = \rho_{G/H} \circ \pi$ de noyau

$$\ker \rho = \ker \rho_{G/H} \circ \pi = \ker \pi = H.$$

En décomposant ρ en somme de sous-représentations irréductibles, on obtient finalement le résultat. □

Appliquons ceci au groupe diédral D_6 : déterminons sa table de caractères.

1. Caractères de degré 1 : ce sont les morphismes $\psi : D_6 \to \mathbb{C}^*$. En notant s la symétrie d'axe Ox et r la rotation d'angle $\frac{\pi}{3}$, on remarque que l'on doit avoir $\psi(s)^2 = 1$, donc $\psi(s) = \pm 1$, puis $\psi(sr)^2 = 1$, donc $\psi(r) = \pm 1$.[34] On obtient donc quatre candidats à être des représentations, dont on vérifie qu'ils conviennent.

34. Si n était impair, la relation $\psi(r)^n$=1 forçait l'égalité $\psi(r) = 1$.

2. Caractères de degrés supérieurs : la relation $|D_6| = \sum_{i\in I} n_i^2$ qui se reformule ici en $8 = \sum_{j\in J} n_j^2$ avec $n_j > 1$ indique qu'il reste deux caractères irréductibles de degré 2 à exhiber. En considérant l'écriture de D_6 à l'aide des matrices de rotations et de symétries complexes, i.e. en posant

$$\rho_h(r) = \begin{pmatrix} \omega^h & 0 \\ 0 & \overline{\omega}^h \end{pmatrix} \text{ puis } \rho_h(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

avec $h \in \{1,2\}$ et $\omega = e^{\frac{i\pi}{3}}$, on réalise (le verifier à nouveau) deux représentations de caractère associé χ_h. Vérifions qu'elles sont bien irréductibles : on a [35]

$$\langle \chi_h, \chi_h \rangle = \frac{1}{12}\sum_{k=0}^{5} (\chi_h(r^k))^2 + (\chi_h(sr^k))^2 = \frac{1}{12}\sum_{k=0}^{5} (\omega^{hk} + \overline{\omega}^{hk})^2,$$

via le fait que la composition par $\rho_h(s)$ envoie $\rho_h(r)^k$ sur une matrice à trace nulle, puis

$$\langle \chi_h, \chi_h \rangle = \frac{1}{12}\sum_{k=0}^{5} (\omega^{2hk} + 2 + \overline{\omega}^{2hk}) = \frac{2\times 6}{12} = 1,$$

en reconnaissant que $\omega^2 = j$. Ces représentations sont bien irréductibles, et on obtient finalement

D_6	r^k	sr^k
ψ_1	1	1
ψ_2	1	-1
ψ_3	$(-1)^k$	$(-1)^k$
ψ_4	$(-1)^k$	$(-1)^{k+1}$
χ_1	$2\cos(\frac{k\pi}{3})$	0
χ_2	$2\cos(\frac{2k\pi}{3})$	0

Les sous-groupes distingués de D_6 sont donc D_6, $\langle r\rangle$, $\langle r^2, s\rangle$, $\langle r^2, sr\rangle$, $\{\mathrm{id}\}$, $\langle r^3\rangle$ et $\langle r^2\rangle$ (intersection des noyaux de ψ_2 et ψ_3).

1.19.2 Références

[Pey04], pp. 227-228, 231-232, , p. 493.

35. On devrait prendre *a priori* le module de $\chi_h(g)$ dans ce qui suit, mais les traces des matrices considérées sont sommes de nombres complexes conjugués, et sont donc réelles.

1.19.3 Questions classiques

1.

1.19.4 Remarques

— La matrice de la symétrie n'est pas

$$\rho_h(s) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

car on ne travaille pas dans la base canonique mais dans la base $((1,i),(1,-i))$.

— Si on veut donner la table de caractères "classique", i.e. dont les colonnes correspondent aux classes de conjugaison, on rappelle que les classes de conjugaisons de D_n sont :

1. Si $n = 2m$ est pair : $\{\mathrm{id}\}, \{r^{\frac{n}{2}}\}, \{s, sr^2, \ldots, sr^{2m-2}\}, \{sr, sr^3, \ldots, sr^{2m-1}\}$ et les $\{r^h, r^{-h}\}$ pour $0 < h < m$,
2. Si n est impair : $\{\mathrm{id}\}, \{s, sr, sr^2, \ldots, sr^{n-1}\}$ et les $\{r^h, r^{-h}\}$ pour $0 < h \leq \frac{n-1}{2}$.

Chapitre 2

Développements d'Analyse

2.1 Lemme de Morse

2.1.1 Développement

Lemme 20 (Lemme de Morse)**.** *Soit $U \subset \mathbb{R}^n$ un ouvert contenant 0, $f \in C^3(U)$ telle que $f(0) = 0, \mathrm{d}f(0) = 0_{\mathcal{L}(\mathbb{R}^n,\mathbb{R})}$ et telle que $\mathrm{d}^2 f(0)$ soit non-dégénérée de signature $(p, n-p)$. Alors il existe un C^1-difféomorphisme Φ entre deux voisinages U et V de 0 dans $\mathbb{R}^n$ tel que $\Phi(0) = 0$ et*

$$\forall x \in U, f(x) = u_1^2 + ... + u_p^2 - u_{p+1}^2 - ... - u_n^2,$$

où l'on a noté $(u_1, ..., u_n) := \Phi(x)$.

La preuve de ce résultat repose sur deux points. Tout d'abord, la formule de Taylor avec reste intégral que l'on admettra :

Lemme 21. *Soit $U \subset \mathbb{R}^n$ un ouvert et soit $f \in C^{k+1}(U, \mathbb{R})$. Alors, pour tout a et h de U tels que $[a, a+h]$ soit inclus dans U, on a*

$$f(a+h) = f(a) + \sum_{i=1}^{k} \frac{1}{i!} d^i f(a)(h)^i + \int_0^1 \frac{(1-t)^k}{k!} d^{k+1} f(a+th)(h)^{k+1} dt.$$

Ensuite, le lemme suivant que l'on va démontrer :

Lemme 22. *Soit $A_0 \in S_n(\mathbb{R}) \cap \mathrm{GL}_n(\mathbb{R})$. Alors il existe un voisinage W de A_0 dans $S_n(\mathbb{R})$ et $\varphi \in C^1(W, \mathrm{GL}_n(\mathbb{R}))$ tels que*

$$\forall A \in W, A = {}^t\varphi(A) A_0 \varphi(A).$$

Démonstration. Considérons l'application

$$\phi : \begin{array}{ccc} \mathscr{M}_n(\mathbb{R}) & \longrightarrow & S_n(\mathbb{R}) \\ M & \longmapsto & {}^tMA_0M \end{array}.$$

Cette application est polynomiale et en particulier C^1. Calculons sa différentielle en l'identité : il vient que

$$\phi(\mathrm{I}_n + H) = \phi(\mathrm{I}_n) + A_0H + {}^t(A_0H) + {}^tHA_0H.$$

Quitte à prendre une norme sous-multiplicative pour s'assurer que $(H \mapsto {}^tHA_0H) = o(H)$, on obtient que $\mathrm{D}\phi(\mathrm{I}_n)(H) = A_0H + {}^t(A_0H)$. Le noyau de cette différentielle est donné par

$$\ker \mathrm{D}\phi(\mathrm{I}_n) = \{H \in \mathscr{M}_n(\mathbb{R}) \ ; \ A_0H \in A_n(\mathbb{R})\},$$

et de la remarque que $\mathscr{M}_n(\mathbb{R}) = S_n(\mathbb{R}) \oplus A_n(\mathbb{R})$, et donc par inversibilité de A_0 [1] $\mathscr{M}_n(\mathbb{R}) = A_0^{-1}\mathscr{M}_n(\mathbb{R}) = A_0^{-1}S_n(\mathbb{R}) \oplus A_0^{-1}A_n(\mathbb{R})$, se dégage un supplémentaire naturel de $\ker \mathrm{D}\phi(\mathrm{I}_n)$, à savoir $F = \{H \in \mathscr{M}_n(\mathbb{R}) \ ; \ A_0H \in S_n(\mathbb{R})\}$. En notant alors $\psi := \phi|_F$, on a que $\mathrm{D}\psi(\mathrm{I}_n) = \mathrm{D}\phi(\mathrm{I}_n)|_F$ et est donc injective. Cette différentielle est de plus surjective, car toute matrice $A \in S_n(\mathbb{R})$ est atteinte par $\mathrm{D}\psi(\mathrm{I}_n)(\frac{1}{2}A_0^{-1}A)$, la matrice $\frac{1}{2}A_0^{-1}A$ étant bien dans F (ou pour une raison de dimensions). De plus I_n appartient à F. En appliquant le théorème d'inversion locale à ψ en l'identité, on obtient un voisinage ouvert de I_n dans F que l'on peut supposer contenu dans l'ouvert des matrices inversibles et un voisinage W de $\psi(\mathrm{I}_n) = A_0$ dans $S_n(\mathbb{R})$ tel que ψ réalise un C^1-difféomorphisme entre ces deux voisinages. On a alors :

$$\forall A \in W, A = {}^t\psi^{-1}(A)A_0\psi^{-1}(A),$$

et $\varphi := \psi^{-1}$ est alors l'objet que nous cherchions. □

Démontrons finalement le lemme de Morse :

Démonstration. Pour x au voisinage de 0, appliquons la formule de Taylor avec reste intégral à f. On obtient l'égalité

$$f(x) = {}^txQ(x)x,$$

où l'on a noté $Q(x) := \int_0^1 (1-t)d^2f(tx)dt$. Le théorème de continue différentiabilité sous le signe somme nous permet d'affirmer que $x \mapsto Q(x)$ est une

1. Un isomorphisme envoie une base sur une base.

fonction de classe C^1. On remarque de plus qu'à x fixé, $Q(x)$ est un matrice symétrique, et que $Q(0) = \frac{1}{2}d^2f(0)$ est inversible et symétrique. Ces conditions réunies permettent d'appliquer le lemme précédent à $Q(0)$, ce qui nous donne une matrice inversible $M(x)$ fonction C^1 de x telle que

$$Q(x) = {}^tM(x)Q(0)M(x),$$

d'où

$$f(x) = {}^tyQ(0)y$$

où l'on a noté $y := M(x)x$. En considérant un changement de coordonnées linéaire $A \in \mathrm{GL}_n(\mathbb{R})$ tel que

$${}^tAQ(0)A = \begin{pmatrix} \mathrm{I}_p & 0 \\ 0 & -\mathrm{I}_{n-p} \end{pmatrix},$$

on obtient finalement

$$f(x) = {}^tu{}^tAQ(0)Au = u_1^2 + ... + u_p^2 - u_{p+1}^2 - ... - u_n^2,$$

où l'on a noté $u := A^{-1}y = A^{-1}M(x)x$. En posant enfin $\Phi : x \mapsto A^{-1}M(x)x$ et en remarquant que $\Phi(0) = 0$, que Φ est C^1 et que $d\Phi(0) = A^{-1}M(0) \in \mathrm{GL}_n(\mathbb{R})$, le théorème d'inversion locale donne les deux voisinages cherchés. □

2.1.2 Références

[Rou09], pp. 209-211, 354-355.

2.1.3 Questions classiques

1. *Donnez une idée de la démonstration de la formule de Taylor* : La preuve se fait par récurrence sur la dimension de l'espace, l'initialisation étant la formule de Taylor classique et l'hérédité se montrant en utilisant le théorème de Fubini pour se ramener à un espace de dimension inférieure. La formule de Taylor classique se démontre elle aussi par récurrence, l'initialisation étant le théorème fondamental de l'analyse et l'hérédité reposant sur une intégration par parties.
2. *Pourquoi peut-on supposer le voisinage donné par le lemme inclus dans* $\mathrm{GL}_n(\mathbb{R})$: Comme le théorème d'inversion locale garantit l'existence d'un voisinage $V = U \cap F$ ouvert de I_n dans F (i.e. U est un voisinage ouvert de I_n dans $\mathscr{M}_n(\mathbb{R})$) tel que $\psi|_V^{\psi(V)} : V \to \psi(V)$ soit un C^1-difféomorphisme, il suffit de restreindre (puis de corestreindre...) cette application à $U \cap \mathrm{GL}_n(\mathbb{R}) \cap F$ pour obtenir ce que l'on souhaite.

2.1.4 Remarques

— Le lemme s'énonce clairement en Français : toute matrice symétrique assez proche d'une matrice symétrique non-dégénérée lui est congrue de manière continûment différentiable (ou toute forme quadratique assez proche d'une forme quadratique non-dégénérée lui est équivalente de manière continûment différentiable).

— Il est clair que ϕ ne saurait être un C^1-difféomorphisme, car $\dim \mathscr{M}_n(\mathbb{R}) \neq \dim S_n(\mathbb{R})$.

— Marston Morse : mathématicien américain, 1892-1977

2.2 Marche aléatoire sur $\mathbb{Z}$

2.2.1 Développement

Définition 3. Soit $(X_n)_{n\geq 1}$ une suite de variables aléatoires i.i.d. de loi μ à valeurs dans $\mathbb{Z}^d$, appelées pas . On appelle marche aléatoire sur $\mathbb{Z}^d$ centrée en 0 la suite de variables aléatoires $(S_n)_{n\geq 0}$, où

$$S_0 \equiv 0 \quad \text{et} \quad S_n = \sum_{k=1}^{n} X_k \ \text{ pour } \ n \geq 1.$$

On note $S = \sum_{k=0}^{\infty} \mathbf{1}_{\{S_k=0\}}$ le nombre de passages de la marche en zéro.

Proposition 11.

$$\mathbb{P}(S = +\infty) = \begin{cases} 0 & si \quad \sum_{k=0}^{\infty} \mathbb{P}(S_k = 0) < +\infty \\ 1 & si \quad \sum_{k=0}^{\infty} \mathbb{P}(S_k = 0) = +\infty \end{cases}$$

Dans le premier cas la marche est dite transiente, dans le second cas elle est dite récurrente.

Démonstration.

1. **Premier cas :** On a d'après le théorème de Tonelli que $\mathbb{E}(S) = \sum_{k=0}^{\infty} \mathbb{P}(S_k = 0)$. Par hypothèse, S est intégrable, et par conséquent S est fini presque sûrement. Ceci donne donc que $\mathbb{P}(S = +\infty) = 0$.

2. **Second cas :** On s'intéresse à l'évènement contraire de $\{S = +\infty\}$, i.e. $B = \{S < +\infty\}$. On va partitionner B en fonction de l'instant du dernier retour en 0 grâce à la variable aléatoire T, définie par $\{T = k\} = \{S_k = 0\} \cap \{\forall l > k, S_l \neq 0\}$. On a que :

$$\begin{aligned} B &= \cup_{k=0}^{\infty} \{T = k\} \\ &= \cup_{k=0}^{\infty} \{S_k = 0\} \cap \{\forall l > k, S_l \neq 0\} \\ &= \cup_{k=0}^{\infty} \{S_k = 0\} \cap \{\forall l > k, S_l - S_k \neq 0\} \\ &= \cup_{k=0}^{\infty} \{S_k = 0\} \cap \{\forall i > 0, S_{k+i} - S_k \neq 0\} \\ &= \cup_{k=0}^{\infty} \{S_k = 0\} \cap \{\forall i > 0, X_{k+1} + X_{k+2} + ... + X_{k+i} \neq 0\}. \end{aligned}$$

Cette dernière écriture permet de voir chaque intersection comme intersection de deux évènements indépendants. La réunion étant disjointe, on

a alors

$$\begin{aligned}\mathbb{P}(B) &= \sum_{k=0}^{\infty} \mathbb{P}(S_k = 0)\mathbb{P}(\forall i > 0, X_{k+1} + X_{k+2} + ... + X_{k+i} \neq 0) \\ &= \sum_{k=0}^{\infty} \mathbb{P}(S_k = 0)\mathbb{P}(\forall i > 0, X_1 + X_2 + ... + X_i \neq 0) \\ &= \sum_{k=0}^{\infty} \mathbb{P}(S_k = 0)\mathbb{P}(\forall i > 0, S_i \neq 0) \\ &= \Big(\sum_{k=0}^{\infty} \mathbb{P}(S_k = 0)\Big)\mathbb{P}(T = 0),\end{aligned}$$

la deuxième égalité découlant de l'hypothèse i.i.d. sur les pas. Remarquons à présent que si $\mathbb{P}(T = 0) > 0$, on a par hypothèse que $\mathbb{P}(B) = +\infty$. Ceci étant absurde, il vient que $\mathbb{P}(T = 0) = 0$ et alors $\mathbb{P}(B) = 0$. Ceci donne que $\mathbb{P}(S = +\infty) = 1$.

□

On s'intéresse maintenant à un cas particulier de marche aléatoire, la marche aléatoire symétrique sur $\mathbb{Z}$ centrée en 0, qui consiste à fixer la loi des pas comme étant $\mu = \frac{1}{2}(\delta_{-1} + \delta_1)$. On a le résultat suivant :

Théorème 18. *La marche aléatoire symétrique sur $\mathbb{Z}$ centrée en 0 est récurrente.*

Démonstration. La proposition précédente nous amène à étudier la convergence de la série $\sum_{k=0}^{\infty} \mathbb{P}(S_k = 0)$. Pour cela calculons pour $k \in \mathbb{N}$ la quantité $\mathbb{P}(S_k = 0)$, avec discussion portant sur la parité de k :

- Si $k = 2n + 1$, on a que $\mathbb{P}(S_k = 0) = 0$ (par le fait que S_k est pair lorsque k est pair et impair lorsque k est impair).
- Si $k = 2n$, on a que $\mathbb{P}(S_k = 0) = \frac{1}{2^{2n}}\binom{2n}{n}$. Ceci peut se voir de deux manières différentes : la première possibilité consiste à voir qu'être en 0 après $2n$ pas revient à avoir fait autant de pas à gauche que de pas à droite. On dénombre alors $\binom{2n}{n}$ cas favorables sur 2^{2n} cas possibles, d'où le résultat. La seconde possibilité est de voir que pour tout entier i on a $\frac{1+X_i}{2} \sim \mathscr{B}(\frac{1}{2})$, et qu'alors $B_n = \frac{n+S_n}{2} \sim \mathscr{B}(n, \frac{1}{2})$. On a donc $\mathbb{P}(S_{2n} = 0) = \mathbb{P}(B_{2n} = n) = \binom{2n}{n}(\frac{1}{2})^{2n}$.

Pour conclure, on donne grâce à la formule de Stirling ($n! \sim \sqrt{2\pi n}(\frac{n}{e})^n$) un équivalent de $\mathbb{P}(S_{2n} = 0)$:

$$\mathbb{P}(S_{2n} = 0) = \frac{1}{2^{2n}}\binom{2n}{n} = \frac{1}{2^{2n}}\frac{(2n)!}{(n!)^2} \sim \frac{1}{2^{2n}}\frac{\sqrt{2\pi 2n}(\frac{2n}{e})^{2n}}{(\sqrt{2\pi n}(\frac{n}{e})^n)^2} = \frac{1}{\sqrt{\pi n}.}$$

Le critère de comparaison couplé au résultat sur les séries de Riemann nous donne enfin que $\sum_{k=0}^{\infty} \mathbb{P}(S_k = 0) = +\infty$, et que la marche aléatoire est bien récurrente. □

2.2.2 Références

[GK11], pp. 227-229.

2.2.3 Questions classiques

1. *Que peut-on dire lorsque l'on établit le même type de marche sur $\mathbb{Z}^d$, avec $d \geq 2$:* On distingue le premier cas $d = 2$, où la marche reste récurrente, et le cas $d > 2$ où la marche devient transiente.

2.2.4 Remarques

— Le premier cas du lemme est aussi le premier cas du lemme de Borel-Cantelli.

— On ne peut pas appliquer le second cas du lemme de Borel-Cantelli au second cas de notre lemme, car les variables S_n ne sont pas indépendantes.

— On rappelle le lemme de Borel-Cantelli : Soit (A_n) une suite d'évènements sur un espace probabilisé $(\Omega, \mathcal{A}, \mathbb{P})$. On note A i.s. $= \{A$ a lieu une infinité de fois$\}$. Alors :

1. Si $\sum_{k=0}^{+\infty} < +\infty$ alors $\mathbb{P}(A \text{ i.s.}) = 0$,
2. Si la suite (A_n) est indépendante et si $\sum_{k=0}^{+\infty} = +\infty$ alors $\mathbb{P}(A \text{ i.s.}) = 1$.

2.3 Théorème de Cartan-von Neumann

2.3.1 Développement

Théorème 19 (Théorème de Cartan-von Neumann)**.** *Tout sous-groupe fermé G de $\mathrm{GL}_n(\mathbb{R})$ est une sous-variété de $\mathscr{M}_n(\mathbb{R})$.*

Pour prouver ce théorème, il va nous falloir exhiber un sous-espace vectoriel F de $\mathscr{M}_n(\mathbb{R})$ tel que pour tout $M \in G$, il existe un voisinage U de 0 dans $\mathscr{M}_n(\mathbb{R})$, un voisinage V de M dans $\mathscr{M}_n(\mathbb{R})$ et un C^1-difféomorphisme $\Phi_M : U \to V$ tel que $\Phi(U \cap F) = V \cap G$. Un premier lemme va nous simplifier la tâche.

Lemme 23. *Il suffit de vérifier la condition précédente pour $M = \mathrm{I}_n$.*

Démonstration. En effet, une fois exhibé $\Phi_{\mathrm{I}_n} : U \to V$, il ne restera pour $M \in G$ quelconque qu'à composer avec le C^1-difféomorphisme

$$\Psi_M : \begin{array}{ccc} \mathscr{M}_n(\mathbb{R}) & \longrightarrow & \mathscr{M}_n(\mathbb{R}) \\ N & \longmapsto & MN \end{array},$$

qui envoie un voisinage V de I_n sur un voisinage $\Psi_M(V)$ de M. On obtient alors

$$\Phi_M(U \cap F) := (\Psi_M \circ \Phi_{\mathrm{I}_n})(U \cap F) = \Psi_M(V \cap G) = \Psi_M(V) \cap G,$$

la dernière égalité provenant du fait que G est un sous-groupe. □

L'idée est d'alors trouver le bon sous-espace vectoriel de $\mathscr{M}_n(\mathbb{R})$ pour paramétrer G à partir de l'exponentielle de matrices. Le lemme suivant décrit ce sous-espace vectoriel :

Lemme 24. *Soit $F := \{M \in \mathscr{M}_n(\mathbb{R}) \ ; \ \forall t \in \mathbb{R}, e^{tM} \in G\}$. On a que F est un sous-espace vectoriel de $\mathscr{M}_n(\mathbb{R})$.*

Démonstration. Il est évident que $0 \in F$ et que F est stable par multiplication scalaire. Il reste à voir que F est stable par addition. Ceci découle du résultat que, pour A et B dans $\mathscr{M}_n(\mathbb{R})$, $e^{A+B} = \lim_{k\to\infty}(e^{A/k}e^{B/k})^k$.[2] On peut alors écrire, pour A, B dans F et $t \in \mathbb{R}$ quelconque, que $e^{t(A+B)} = \lim_{k\to\infty}(e^{\frac{t}{k}A}e^{\frac{t}{k}B})^k$. Comme par hypothèse on a que $e^{\frac{t}{k}A}$ et $e^{\frac{t}{k}B}$ sont des éléments de G pour tout $t \in \mathbb{R}$ et tout $k \in \mathbb{N}^*$, et comme de plus G est supposé fermé, alors $e^{t(A+B)} \in G$ par passage à la limite et donc $A + B \in F$.[3] □

2. On le démontre dans la partie *Questions classiques* , dans le but de gagner du temps sur ce long développement.

3. Dans toutes les leçons concernées sauf la 156, on pourra simplement résumer ce qui a été fait jusque-là pour pouvoir travailler plus en détail sur la suite de la preuve.

Ce lemme étant prouvé, on peut considérer F' un supplémentaire de F dans $\mathscr{M}_n(\mathbb{R})$ et définir

$$\Phi : \begin{array}{ccc} \mathscr{M}_n(\mathbb{R}) = F \oplus F' & \longrightarrow & \mathrm{GL}_n(\mathbb{R}) \\ N = A + B & \longmapsto & e^A e^B \end{array} .$$

On a que Φ est C^1 en tant que composée de fonctions C^1 (ceci se voit en écrivant plus justement $e^A e^B$ comme $e^{\pi_F(N)} e^{\pi_{F'}(N)}$ où π_F est la projection – linéaire donc C^1 – sur F parallèlement à F' et où $\pi_{F'}$ est définie analoguement). On a aussi que $\Phi(0) = \mathrm{I}_n$ et que $\mathrm{D}\Phi(0) = \mathrm{id}_{\mathscr{M}_n(\mathbb{R})}$. Le théorème d'inversion locale assure l'existence d'un voisinage U de 0 dans $\mathscr{M}_n(\mathbb{R})$ et d'un voisinage $V = \Phi(U)$ de I_n dans $\mathscr{M}_n(\mathbb{R})$ tel que $\Phi : U \to V$ soit un C^1-difféomorphisme. Il nous reste à montrer que $\Phi(U \cap F) = V \cap G$, l'inclusion de gauche à droite étant immédiate étant donné la définition de F. Pour celle de droite à gauche on se sert du dernier lemme :

Lemme 25. *Il n'existe pas de suite (M_k) d'éléments de $F'\backslash\{0\}$ telle que $\lim_{k\to\infty} M_k = 0$ et $\forall k \in \mathbb{N}, e^{M_k} \in G$.*

En effet, une fois ce résultat prouvé, on peut voir que, quitte à restreindre U, tout élément P de $\Phi(U) \cap G$ est dans $\Phi(U \cap F)$: si ce n'était pas le cas on pourrait choisir deux suites (A_k) de F et (B_k) de $F'\backslash\{0\}$ de limite nulle telles que pour tout $k \in \mathbb{N}$, $\Phi(A_k + B_k) \in G$ (ce qui traduit l'existence d'un P qui nous contredit pour tout voisinage de 0). En écrivant $e^{B_k} = e^{-A_k}\Phi(A_k + B_k) \in G$, on entre alors en contradiction avec le résultat précédent. Démontrons finalement le lemme :

Démonstration. Par l'absurde : supposons qu'il existe une suite de matrices non-nulles (M_k) de F' telle que $\lim_{k\to\infty} M_k = 0$ et telle que $e^{M_k} \in G$ pour tout $k \in \mathbb{N}$. En posant $\varepsilon_k := \frac{M_k}{||M_k||} \in S \cap F'$ où S est la sphère unité de $\mathscr{M}_n(\mathbb{R})$, on peut extraire une sous-suite toujours notée (ε_k) telle que $\lim_{k\to\infty} \varepsilon_k = \varepsilon \in S$ par compacité de la sphère unité. Comme F' est fermé en tant que sous-espace vectoriel de $\mathscr{M}_n(\mathbb{R})$, on a alors que $\varepsilon \in S \cap F'$. On a de plus par continuité de l'exponentielle que, pour $t \in \mathbb{R}$ quelconque,

$$e^{t\varepsilon} = \lim_{k\to\infty} e^{t\frac{M_k}{||M_k||}}.$$

En écrivant $\frac{t}{||M_k||} = \lambda_k + \mu_k$ où $\lambda_k \in \mathbb{Z}$ et la partie entière et $\mu_k \in [0, 1[$ la partie décimale de $\frac{t}{||M_k||}$, on a finalement

$$e^{t\frac{M_k}{||M_k||}} = e^{\lambda_k M_k} e^{\mu_k M_k} \Longrightarrow (e^{M_k})^{\lambda_k} = \underbrace{e^{t\varepsilon_k}}_{\to e^{t\varepsilon}} \underbrace{e^{-\mu_k M_k}}_{\to \mathrm{I}_n} \underset{k\to\infty}{\longrightarrow} e^{t\varepsilon}.$$

Comme $e^{M_k} \in G$ et G est fermé, $e^{t\varepsilon} \in G$ pour tout $t \in \mathbb{R}$, i.e. $\varepsilon \in F$. Alors $\varepsilon \in F \cap F' = \{0\}$ et $||\varepsilon|| = 1$, d'où la contradiction et le lemme. □

2.3.2 Références

[GT98], pp. 83-84.

2.3.3 Questions classiques

1. *Montrez que* $e^{A+B} = \lim_{k\to\infty}(e^{A/k}e^{B/k})^k$: On développe e en série entière et l'on voit que $e^H = \mathrm{I}_n + H + o(H)$, ce qui nous donne $\mathrm{D}e(0) = \mathrm{id}_{\mathscr{M}_n(\mathbb{R})}$. D'après le théorème d'inversion locale, e réalise un C^1-difféomorphisme d'un voisinage ouvert de 0 sur un voisinage ouvert de I_n. Notons L sa réciproque : on a en particulier que $L(\mathrm{I}_n + H) = H + o(H)$. Pour k assez grand, et grâce au fait que $(e^{\frac{A}{k}}e^{\frac{B}{k}}) = \mathrm{I}_n + \frac{A+B}{k} + o(\frac{1}{k})$, on écrit alors :

$$\begin{aligned}(e^{\frac{A}{k}}e^{\frac{B}{k}})^k &= e^{L(e^{\frac{A}{k}}e^{\frac{B}{k}})^k} \\ &= e^{kL(\mathrm{I}_n+\frac{A+B}{k}+o(\frac{1}{k}))} \\ &= e^{(}A + B + o(1)) \underset{k\to\infty}{\longrightarrow} e^{(}A + B).\end{aligned}$$

2. *Expliquez pourquoi* $\mathrm{D}\Phi(0) = \mathrm{id}_{\mathscr{M}_n(\mathbb{R})}$: On a vu que Φ était C^1, on va donc exhiber sa différentielle en calculant ses différentielles partielles selon F et F' en 0. On a que $\Phi|_F = e|_F$ d'où pour $H = H_F + H_{F'}$

$$\mathrm{D}_F\Phi(0)(H_F) = \underbrace{(\mathrm{D}e(0))|_F}_{=\mathrm{id}_{\mathscr{M}_n(\mathbb{R})}|_F}(H_F) = H_F.$$

   De même on trouve $\mathrm{D}_{F'}\Phi(0)(H_{F'}) = H_{F'}$, d'où enfin $\mathrm{D}\Phi(0)(H) = \mathrm{D}_F\Phi(0)(H_F) + \mathrm{D}_{F'}\Phi(0)(H_{F'}) = H_F + H_{F'} = H$, qui donne $\mathrm{D}\Phi(0) = \mathrm{id}_{\mathscr{M}_n(\mathbb{R})}$.
3. *Quel est le plan tangent à* G *en* I_n : Le plan tangent à G en I_n est F : on a en effet que $t \mapsto e^{tM}$ est une courbe tracée sur G qui vaut I_n en 0 et est dérivable, sa dérivée $t \mapsto Me^{tM}$ valant M en 0. Ceci nous indique que $F \subset T_{\mathrm{I}_n}G$, et le développement montre $\dim F = \dim T_{\mathrm{I}_n}G$. Finalement, $F = T_{\mathrm{I}_n}G$. Par exemple, si $G = \mathrm{SL}_n(\mathbb{R})$, on a

$$\begin{aligned}T_{\mathrm{I}_n}\mathrm{SL}_n(\mathbb{R}) &= \{M \in \mathscr{M}_n(\mathbb{R}) \ ; \ \forall t \in \mathbb{R}, e^{tM} \in \mathrm{SL}_n(\mathbb{R})\} \\ &= \{M \in \mathscr{M}_n(\mathbb{R}) \ ; \ \forall t \in \mathbb{R}, \det(e^{tM}) = 1\} \\ &= \{M \in \mathscr{M}_n(\mathbb{R}) \ ; \ \forall t \in \mathbb{R}, e^{\mathrm{Tr}(tM)} = 1\} \\ &= \{M \in \mathscr{M}_n(\mathbb{R}) \ ; \ \mathrm{Tr}(M) = 0\}.\end{aligned}$$

On peut ainsi affirmer que $\mathrm{SL}_n(\mathbb{R})$ est une sous variété de dimension $n^2 - 1$ de $\mathscr{M}_n(\mathbb{R})$. Pour l'espace tangent en un autre point, il suffit de composer à nouveau par la translation $\psi_M : N \mapsto MN$.

2.3.4 Remarques

— Élie Cartan : mathématicien et physicien français, 1869-1951

— John von Neumann : mathématicien et physicien américano-hongrois, 1903-1957

2.4 Théorème de Liapounov

2.4.1 Développement

Théorème 20 (Théorème de Liapounov)**.** *Soit $f : \mathbb{R}^n \to \mathbb{R}^n$ de classe C^1 telle que $f(0) = 0$ et telle que les valeurs propres de $A = \mathrm{D}f(0)$ sont de partie réelle strictement négative. On considère le problème de Cauchy $y' = f(y), y(0) = x \in \mathbb{R}^n$. Alors pour x proche de 0 la solution y tend exponentiellement vers 0 lorsque t tend vers $+\infty$.*

Démonstration. On établit un premier lemme sur le problème linéarisé en 0 :

Lemme 26. *On considère le problème de Cauchy $z' = Az, z(0) = x \in \mathbb{R}^n$. Alors il existe $C > 0$ et $a > 0$ tels que, pour tout $t \in \mathbb{R}$, $||z(t)|| \leq Ce^{-at}||x||$.*

Démonstration. Soit $|||.|||$ une norme subordonnée usuelle sur $\mathscr{M}_n(\mathbb{C})$. Le flot du problème de Cauchy est donné par $z(t) = e^{tA}x$. En considérant que A s'écrit $D + N$ selon sa décomposition de Dunford, il vient

$$|||e^{tA}||| \leq |||e^{tD}||| \times |||e^{tN}||| \leq |||e^{tD}||| \times \Big(\sum_{k=0}^{n} \frac{|t|^k |||N^k|||}{k!} \Big) \leq Ke^{t \sup \mathrm{Re}(\lambda)}(1 + |t|^n).$$

Par hypothèse, il existe $a > 0$ tel que $\sup \mathrm{Re}(\lambda) < -a$. On a alors que $e^{t \sup \mathrm{Re}(\lambda) + at}(1 + |t|^n) \underset{t \to \infty}{\longrightarrow} 0$ par croissance comparée. En particulier cette fonction est bornée par une certaine constante M et donc $Ke^{t \sup \mathrm{Re}(\lambda)}(1 + |t|^n) \leq \underbrace{KM}_{:=C} e^{-at}$. Par conséquent

$$||z(t)|| = ||e^{tA}x|| \leq |||e^{tA}||| \times ||x|| \leq Ce^{-at}||x||.$$

□

Considérons à présent pour $x, y \in \mathbb{R}^n$ la quantité $\langle e^{tA}x, e^{tA}y \rangle$. Le lemme précédent et l'inégalité de Cauchy-Schwarz nous permettent d'affirmer que $|\langle e^{tA}x, e^{tA}y \rangle| \leq ||e^{tA}x|| \times ||e^{tA}y|| \leq C^2 e^{-2at}||x|| \times ||y||$, qui est intégrable sur $\mathbb{R}^+$. On peut donc définir la fonction $b : (x, y) \mapsto \int_0^{+\infty} \langle e^{tA}x, e^{tA}y \rangle dt$, et on vérifie rapidement que c'est une forme bilinéaire symétrique. De plus,

$$q(x) := b(x, x) = \int_0^{+\infty} ||e^{tA}x||^2 \, dt$$

est positif pour tout x, et s'annule si et seulement si la fonction continue positive sous l'intégrale est identiquement nulle, i.e. $x = 0$. Donc q est définie positive. La règle de dérivation d'une forme quadratique[4] donne que $\mathrm{D}q(x)(y) =$

4. Obtenue par $q(x + h) = q(x) + 2b(x, h) + q(h)$.

$2b(x,y)$. En particulier on a

$$\langle \nabla q(x), Ax\rangle = 2b(x,Ax) = \int_0^{+\infty} 2\langle e^{tA}x, Ae^{tA}x\rangle\, dt,$$

où l'intégrande est la dérivée par rapport à t de $\langle e^{tA}x, e^{tA}x\rangle$, d'où finalement par le lemme

$$\langle \nabla q(x), Ax\rangle = \lim_{T\to+\infty} [||e^{tA}x||^2]_{t=0}^{t=T} = -||x||^2.$$

Revenons à présent au problème initial en considérant une solution maximale y, avec $y' = f(y) = Ay + r(y)$. On a par la règle de la chaîne que :

$$\begin{aligned} q(y)' = \mathrm{D}q(y)(y') &= 2b(y,y') \\ &= 2b(y,Ay) + 2b(y,r(y)) \\ &= -||y||^2 + 2b(y,r(y)). \end{aligned}$$

Notons que l'on aurait simplement $q(z)' = -||z||^2$ pour le système linéarisé : on veut montrer que, r étant petit, les fonctions $q(y)$ et $q(z)$ auront à peu près le même comportement pour t grand [5]. On va travailler par commodité avec la norme donnée par $\sqrt{q}$ [6] : majorons ainsi $b(y,r(y))$, il vient

$$|b(y,r(y))| \leq \sqrt{q(y)}\sqrt{q(r(y))}.$$

En remarquant que $r(y) = f(y) - f(0) - \mathrm{D}f(0)(y) = o(y)$ par définition de la différentielle, on a l'assertion suivante :

$$\forall \varepsilon > 0, \exists \alpha > 0 \text{ tq } q(y) \leq \alpha \Longrightarrow \sqrt{q(r(y))} \leq \varepsilon\sqrt{q(y)}.$$

Par suite,

$$2b(y,r(y)) \leq 2\varepsilon q(y).$$

En exhibant une constante $C > 0$ telle que $Cq(y) \leq ||y||^2$, on a finalement

$$q(y)' = -||y||^2 + 2b(y,r(y)) \leq -(C-2\varepsilon)q(y) =: -\beta q(y)$$

pour $q(y) \leq \alpha$, et on est libre de choisir ε suffisamment petit pour que β soit strictement positif. On a enfin que $q(y(t))' \leq -\beta q(y(t))$ tant que $q(y(t))$ reste

5. On justifie à la fin du développement que, sous une bonne condition initiale, la solution est en fait globale.

6. Comme nous sommes en dimension finie, elle est équivalente à la norme $||\cdot||$.

inférieur ou égal à α. Cette condition est satisfaite pour $t \geq 0$ si la donnée initiale x vérifie $q(x) < \alpha$; sinon il existerait un premier instant $t_0 > 0$ tel que $q(y(t_0)) = \alpha$, d'où $q(y)'(t_0) \leq -\beta q(y(t_0)) < 0$ et $q(y(t))$ devrait être strictement plus grand que α pour t légèrement inférieur à t_0, ce qui contredirait par continuité la définition de t_0. L'inéquation différentielle vérifiée par $q(y)$ se résout de manière habituelle, par facteur intégrant :

$$(e^{\beta t} q(y))' = e^{\beta t}(q(y)' + \beta q(y)) \leq 0,$$

ce qui entraîne en particulier comme $y(0) = x$ que

$$q(y(t)) \leq e^{-\beta t} q(x) \text{ pour tout } t \geq 0.$$

Par le lemme des sorties des compacts, on en déduit que notre solution maximale est globale, et qu'elle a le comportement attendu. □

2.4.2 Références

[Rou09], pp. 138-143.

2.4.3 Questions classiques

1. *Détaillez l'inégalité sur* $|||e^{tD}|||$: On commence par remarquer que $\mathrm{Sp}_{\mathbb{C}}(D) = \mathrm{Sp}_{\mathbb{C}}(A)$. En effet, D et N sont trigonalisables et commutent donc sont simultanément trigonalisables : comme les valeurs propres de N sont toutes nulles, on a le résultat. Par suite,

$$|||e^{tD}||| = |||Pe^{tD'}P^{-1}|||$$

où D' est diagonale, en utilisant ici le résultat que $e^{tPD'P^{-1}} = Pe^{tD'}P^{-1}$, et alors

$$|||e^{tD}||| \leq |||P||| \times |||P^{-1}||| \times |||e^{tD'}||| \leq Ke^{t \sup \mathrm{Re}(\lambda)}$$

en invoquant finalement l'équivalence entre la norme $|||.|||$ et la norme $|||.|||_1$ qui donne $|||A|||_1 = \sup_j \sum_i |a_{ij}|$, le max des somme des modules des termes des colonnes.

2.4.4 Remarques

— En dimension 2, la courbe de niveau de q passant par x est une ellipse de centre 0, le vecteur $\nabla q(x)$ est normal en x à cette ellipse, et le vecteur $Ax = z'(0)$ est dirigé vers l'intérieur puisque leur produit scalaire, égal à $-||x||^2$, est négatif.

— Alexandre Liapounov : mathématicien russe, 1857-1918

2.5 Théorème de Cauchy-Lipschitz global

2.5.1 Développement

Théorème 21 (Théorème de Cauchy-Lipschitz global)**.** *Soit I un intervalle de $\mathbb{R}$ et $f : I \times \mathbb{R}^m \to \mathbb{R}^m$ une application continue supposée globalement lipschitzienne en sa seconde variable, i.e. pour tout intervalle compact $K \subset I$ il existe $k > 0$ tel que, pour tous $t \in K, y, z \in \mathbb{R}^m, ||f(t,z) - f(t,y)|| \leq k||z - y||$. Alors le problème de Cauchy $(\mathcal{C}) : y' = f(t,y), y(t_0) = x$ avec $(t_0, x) \in I \times \mathbb{R}^m$ donné admet une unique solution globale, i.e. définie sur I entier.*

Démonstration. L'objectif est de se ramener à un problème de point fixe. On note $E := C^0(I, \mathbb{R}^m)$ et on pose

$$F : \begin{array}{ccc} E & \longrightarrow & E \\ y & \longmapsto & \left(t \mapsto \int_{t_0}^t f(s, y(s))ds\right) \end{array}.$$

Pour commencer, on montre le lemme suivant :

Lemme 27. *On a équivalence entre être solution sur I de $(\mathcal{C})$ et être solution du problème $(\mathcal{E})$: $y \in E$ et $F(y) = y$.*

Démonstration. Supposons que y soit solution de $(\mathcal{C})$ sur I. En particulier y et dérivable et donc continue, et comme $y' = f(t,y)$ est alors continue il vient en intégrant que $y(t) = x + \int_{t_0}^t f(s, y(s))ds$. Réciproquement, si y est continue sur I et vérifie l'égalité précédente, y est dérivable sur I et est solution du problème de Cauchy. □

Supposons alors que $I = [\alpha, \beta]$ est compact, notons $l := \beta - \alpha$ sa longeur et récupérons la constante de Lipschitz k donnée par l'énoncé. On introduit sur E la norme $||y||_k := \max_{t \in I}(e^{-k|t-t_0|}||y(t)||)$. La remarque

$$e^{-kl}||y||_\infty \leq ||y||_k \leq ||y||_\infty$$

permet d'affirmer que E est complet pour $||.||_k$ car complet pour $||.||_\infty$. Comme f est continue, on a de plus que F envoie E dans lui-même. De plus, on a pour tout $y, z \in E, t \in I$ et $t \geq t_0$ que

$$F(y)(t) - F(z)(t) = \int_{t_0}^t \big(f(s, y(s)) - f(s, z(s))\big)ds$$

d'où

$$\begin{aligned} e^{-k(t-t_0)}||F(y)(t) - F(z)(t)|| &\leq e^{-k(t-t_0)} \int_{t_0}^{t} ||f(s,y(s)) - f(s,z(s))||ds \\ &\leq e^{-k(t-t_0)} \int_{t_0}^{t} k||y(s) - z(s)||ds \\ &\leq e^{-k(t-t_0)} \int_{t_0}^{t} ke^{k(s-t_0)}ds||y - z||_k \\ &\leq (1 - e^{-k(t-t_0)})||y - z||_k, \end{aligned}$$

où pour obtenir la troisième inégalité, on a multiplié par $e^{k(s-t_0)}e^{-k(s-t_0)}$ et majoré par $\max_{s\in[t_0,t]}(e^{-k(s-t_0)}||y(s) - z(s)||) \leq ||y - z||_k$.

On obtient de même pour $t \leq t_0$, en remplaçant $\int_{t_0}^{t}$ par $\int_{t}^{t_0}$:

$$e^{k(t-t_0)}||F(y)(t) - F(z)(t)|| \leq (1 - e^{k(t-t_0)})||y - z||_k.$$

En passant au max en t sur chacun des deux intervalles $[\alpha, t_0]$ et $[t_0, \beta]$, on obtient finalement

$$\forall y, z \in E, ||F(y) - F(z)||_k \leq (1 - e^{-kl})||y - z||_k.$$

Comme $0 < 1 - e^{-kl} < 1$, F est contractante et admet un unique point fixe d'après le théorème du point fixe de Picard.

On suppose à présent que I n'est plus compact, et on prend une exhaustion compacte $\bigcup_{j\in\mathbb{N}} I_j$ de I telle que

$$I_0 \subset I_1 \subset ... \subset I_j \subset ...,$$

chaque I_j contenant le point t_0. On note alors y_j l'unique solution sur I_j que l'on a exhibé précédemment. On remarque que si y est solution sur I, alors sa restriction à I_j coïncide nécessairement avec y_j. Réciproquement, l'application y définie par

$$y(t) = y_j(t) \quad \text{pour tout } j \text{ tel que } t \in I_j$$

est bien définie à nouveau par l'unicité des solutions sur chaque intervalle compact, et est bien solution de $(\mathcal{C})$ sur I.

□

2.5.2 Références

[Rou09], pp. 180-183.

2.5.3 Questions classiques

1. *Rappellez la démonstration du théorème du point fixe de Picard* : Soit $f : E \to E$ une application k-contractante, (E, d) étant un espace métrique complet. On définit la suite (x_n) par $x_0 \in E$ quelconque et $x_{n+1} = f(x_n)$. On remarque que $d(x_{n+1}, x_n) = d(f(x_n), f(x_{n-1})) \leq kd(x_n, x_{n-1}) \leq ... \leq k^n d(x_1, x_0)$. La somme $\sum_{k=0}^{+\infty} d(x_{k+1}, x_k)$ étant finie, notre suite est de Cauchy et est donc convergente vers un élément x_* de E. Par continuité de f on obtient $f(x_*) = x_*$. L'unicité est claire.

2.5.4 Remarques

— Augustin Louis Cauchy : mathématicien français, 1789-1857

— Rudolf Lipschitz : mathématicien allemand, 1832-1903

2.6 Méthode du gradient à pas optimal

2.6.1 Développement

On considère une application $J : \mathbb{R}^p \to \mathbb{R}$ supposée elliptique, i.e. de classe C^1 et telle que

$$\exists \alpha > 0 \text{ tq } \forall x, y \in \mathbb{R}^p, \langle \nabla J(x) - \nabla J(y), x - y \rangle \geq \alpha ||x - y||^2.$$

Lemme 28. *On a que J admet un unique minimum en un $u_* \in \mathbb{R}^p$.*

Démonstration. On utilise la formule de Taylor avec reste intégral, qui donne ici :

$$\begin{aligned} J(v) - J(u) &= \int_0^1 \langle \nabla J(u + t(v-u)), v - u \rangle dt \\ &= \langle \nabla J(u), v - u \rangle + \int_0^1 \frac{1}{t} \langle \nabla J(u + t(v-u)) - \nabla J(u), t(v-u) \rangle dt \\ &\geq \langle \nabla J(u), v - u \rangle + \int_0^1 \alpha t ||v - u||^2 dt, \\ J(v) - J(u) &\geq \langle \nabla J(u), v - u \rangle + \frac{\alpha}{2} ||v - u||^2. \end{aligned}$$

Ainsi, dès que $u \neq v$, on a $J(v) > J(u) + \langle \nabla J(u), v - u \rangle$ et, ceci caractérisant les fonctions strictement convexes régulières, J est strictement convexe. De plus, pour $u = 0$ on obtient en utilisant l'inégalité de Cauchy-Schwarz que

$$J(v) \geq J(0) + \langle \nabla J(0), v \rangle + \frac{\alpha}{2} ||v||^2 \geq J(0) - ||\nabla J(0)|| \times ||v|| + \frac{\alpha}{2} ||v||^2 \underset{||v|| \to +\infty}{\longrightarrow} +\infty,$$

nous donnant la coercivité de J. Une fonction strictement convexe et coercive admettant un unique minimum, on a démontré notre résultat. □

On donne sous forme de théorème la méthode du gradient à pas optimal :

Théorème 22 (Méthode du gradient à pas optimal)**.** *Soit $u_0 \in \mathbb{R}^p$ quelconque. Pour $n \in \mathbb{N}^*$, on pose $u_{n+1} = u_n - \rho_n \nabla J(u_n)$, où ρ_n est tel que $\min_{\rho \in \mathbb{R}}(J(u_n - \rho \nabla J(u_n))) = J(u_n - \rho_n \nabla J(u_n))$ (ou bien ρ_n est **la** solution de $\frac{d}{d\rho} J(u_n - \rho \nabla J(u_n)) = 0$). Alors la méthode est bien définie et $\lim_{n \to +\infty} u_n = u_*$.*

Démonstration. Pour voir que la méthode est bien définie, le seul point à vérifier est que ρ_k est déterminé de manière unique (si $\nabla J(u_k) \neq 0$, sinon on arrête la méthode car on a trouvé le minimum). Le lemme précédent nous montrant que J est strictement convexe et coercive, sa restriction à une droite vectorielle est une fonction réelle toujours strictement convexe et coercive, et on vérifie

ce premier point. Détaillons à présent le fait que ρ_k soit solution de $\frac{d}{d\rho}J(u_k - \rho\nabla J(u_k)) = 0$. On a ainsi que

$$-\langle \nabla J(u_k - \rho_k \nabla J(u_k)), \nabla J(u_k)\rangle = 0$$

et donc $\langle \nabla J(u_{k+1}), \nabla J(u_k)\rangle = 0$, ce qui montre d'une part que deux directions de descente successives sont orthogonales, et d'autre part comme $u_{k+1} = u_k - \rho_k \nabla J(u_k)$ que

$$\langle \nabla J(u_{k+1}), u_{k+1} - u_k\rangle = 0.$$

Par application de la première inégalité du lemme, on obtient $J(u_k) - J(u_{k+1}) \geq \frac{\alpha}{2}||u_k - u_{k+1}||^2$. La suite $(J(u_n))$ étant décroissante et minorée par $J(u_*)$, elle converge. En particulier $\lim_{k\to+\infty} J(u_k) - J(u_{k+1}) = 0$, relation qui, jointe à la précédente inégalité, donne $\lim_{k\to+\infty} ||u_k - u_{k+1}|| = 0$. Grâce à l'orthogonalité des directions de descente successives, on peut écrire

$$\begin{aligned} ||\nabla J(u_k)||^2 &= \langle \nabla J(u_k), \nabla J(u_k)\rangle \\ &= \langle \nabla J(u_k), \nabla J(u_k) - \nabla J(u_{k+1})\rangle \\ &\leq ||\nabla J(u_k)|| \times ||\nabla J(u_k) - \nabla J(u_{k+1})|| \end{aligned}$$

et donc

$$||\nabla J(u_k)|| \leq ||\nabla J(u_k) - \nabla J(u_{k+1})||.$$

De plus, comme J est coercive et que $(J(u_n))$ est décroissante, la suite (u_n) est bornée. En appliquant le théorème de Heine à ∇J sur un compact $K \subset \mathbb{R}^p$ contenant tous les termes de la suite (u_n), on a que ∇J est uniformément continue sur K, et donc

$$\lim_{k\to+\infty} ||\nabla J(u_{k+1}) - \nabla J(u_k)|| = 0^{7},$$

et donc

$$\lim_{k\to\infty} \nabla J(u_k) = 0.$$

Démontrons enfin la convergence. On écrit

$$\alpha||u_k - u_*||^2 \leq \langle \nabla J(u_k) - \nabla J(u_*), u_k - u_*\rangle \leq ||\nabla J(u_k)|| \times ||u_k - u_*||,$$

en utilisant l'ellipticité puis la relation $\nabla J(u_*) = 0$, et donc

$$||u_k - u_*|| \leq \frac{1}{\alpha}||\nabla J(u_k)|| \underset{k\to+\infty}{\longrightarrow} 0.$$

□

7. Voir la partie *Remarques*.

2.6.2 Références

[Cia82], pp. 182-183, 189-190.

2.6.3 Questions classiques

1. *Détaillez pourquoi* $\lim_{k\to\infty} ||\nabla J(u_{k+1}) - \nabla J(u_k)|| = 0$: Réécrivons l'uniforme continuité de ∇J. On a que

$$\forall \varepsilon > 0, \exists \eta > 0 \text{ tq } \forall x, y \in \mathbb{R}^p, ||x - y|| \leq \eta \Longrightarrow ||\nabla J(x) - \nabla J(y)|| \leq \varepsilon.$$

   On a de plus que

$$\forall \varepsilon' > 0, \exists N \in \mathbb{N} \text{ tq } \forall k \in \mathbb{N}, n \geq N \Longrightarrow ||u_{k+1} - u_k|| \leq \varepsilon'.$$

   Pour $\varepsilon > 0$, il suffit de choisir un $\eta > 0$ donné par la première assertion puis de choisir $N \in \mathbb{N}$ dans la deuxième assertion avec $\varepsilon' = \eta$.

2.6.4 Remarques

— On pourra donner l'interprétation géométrique de la méthode s'il reste du temps, ou simplement laisser entendre que le gradient donne la direction de la plus grande pente et donc son opposé celui de la plus grande descente.

— La méthode est lente : cela peut se comprendre par le fait que le gradient ne donne que la plus forte pente locale et non globale, et qu'on ne retient pas les déplacements précédents avent d'en effectuer un nouveau. On peut améliorer la méthode avec des informations sur la géométrie de la surface, ou en prenant en compte les déplacements précédents.

2.7 Méthode de Newton

2.7.1 Développement

Soit $f : [c,d] \to \mathbb{R}$ une application de classe C^2 qui vérifie

— $f(c) < 0 < f(d)$,

— $\forall x \in [c,d], f'(x) > 0$.

On remarque que f est continue, strictement croissante et que $0 \in [f(c), f(d)]$. Il existe donc un unique point $a \in]c,d[$ tel que $f(a) = 0$. On cherche à approcher a : pour cela on définit la fonction

$$F : \begin{array}{ccc} [c,d] & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x - \frac{f(x)}{f'(x)} \end{array},$$

on fixe $x_0 \in [c,d]$ et on définit la suite (x_n) par $x_{n+1} = F(x_n)$.

Proposition 12 (Convergence quadratique de la méthode de Newton)**.** *Sous les hypothèses précédentes, on a l'existence d'un $\alpha > 0$ tel que :*

1. *pour $x_0 \in I = [a-\alpha, a+\alpha]$, la méthode est bien définie,*
2. *pour $x_0 \in I$, la méthode converge à l'ordre deux vers a, i.e.* $\lim_{n\to+\infty} x_n = a$ *et*

$$\exists C \geq 0 \text{ tq } \forall n \in \mathbb{N}, |x_{n+1} - a| \leq C|x_n - a|^2.$$

Démonstration. On commence par remarquer que $F(a) = a$ (et $F'(a) = 1 - \frac{f'(a)^2 - f(a)f''(a)}{f'(a)^2} = 1 - 1 = 0$: on est dans le cas d'un point fixe superattractif[8]). On a alors, grâce au fait que $f(a) = 0$:

$$\begin{aligned} F(x) - a &= (x-a) - \frac{f(x) - f(a)}{f'(x)} \\ &= \frac{f(a) - f(x) - (a-x)f'(x)}{f'(x)}. \end{aligned}$$

On applique la formule de Taylor-Lagrange à l'ordre 2, nous donnant l'existence d'un $z_x \in]x,a[$ tel que

$$f(a) - f(x) - (a-x)f'(x) = \frac{1}{2}f''(z_x)(a-x)^2,$$

8. Voir la partie *Remarques*.

d'où

$$F(x) - a = \frac{f''(z_x)}{2f'(x)}(x-a)^2. \qquad (*)$$

On pose $C = \frac{\max_{[c,d]} |f''|}{2\min_{[c,d]} |f'|}$. On a

$$\forall x \in [c,d], |F(x) - a| \leq C|x-a|^2.$$

On choisit alors $\alpha > 0$ tel que $\alpha C < 1$ et tel que $I =]a-\alpha, a+\alpha[\subset [c,d]$. Si $x \in I$, on a que $|F(x) - a| \leq C\alpha^2 < \alpha$ et donc I est stable par F. La méthode est donc bien définie et on a :

$$\forall n \in \mathbb{N}, |x_{n+1} - a| = |F(x_n) - a| \leq C|x_n - a|^2$$

et on a par récurrence que

$$\forall n \in \mathbb{N}, C|x_n - a|^2 \leq (C|x_0 - a|)^{2^n} \leq (C\alpha)^{2^n},$$

et la conclusion car $0 < C\alpha < 1$. □

On suppose une condition supplémentaire sur f : $f'' > 0$ sur $[c,d]$.

Proposition 13. *Sous les hypothèses précédentes, on a que :*

1. $I = [a,d]$ *est stable par* F,
2. *si* $x_0 \in I$, *on a que la suite* (x_n) *est soit constante soit strictement décroissante et on a*

$$\begin{cases} \forall n \in \mathbb{N}, 0 \leq x_{n+1} - a \leq C(x_n - a)^2 \\ x_{n+1} - a \sim \frac{f''(a)}{2f'(a)}(x_n - a)^2 \text{ si } x_0 > a \end{cases}.$$

Démonstration. Comme $f'' > 0$, f est strictement convexe sur $[c,d]$. Si $x \in I$, on a que $f'(x) > 0$ et $f(x) \geq 0$ d'où

$$F(x) = x - \frac{f(x)}{f'(x)} \leq x,$$

avec inégalité stricte si $x > a$. L'inégalité $(*)$ nous permet d'écrire

$$F(x) - a = \frac{f''(z_x)}{f'(x)}(x-a)^2 \geq 0,$$

à nouveau avec inégalité stricte si $x > a$. En combinant ces deux derniers points on obtient que I est stable par F, que si $x \in]a,d]$ alors pour tout $n \in \mathbb{N}$ on a $a < x_n \leq d$ et la suite $(x_n)_{n\in\mathbb{N}}$ est strictement décroissante, et que si $x_0 = a$

cette suite est constante. Dans tout les cas, la suite admet une limite l car est décroissante et minorée et par continuité de F on doit avoir $F(l) = l$ qui donne $f(l) = 0$ et donc $l = a$. Comme précédemment on montre que

$$\forall n \in \mathbb{N}, 0 \leq x_{n+1} - a \leq C(x_n - a)^2$$

qui donne la convergence quadratique. Enfin, si $x_0 \in]a, d]$, tous les x_n sont dans $]a, d]$ et en notant z_n les z_{x_n} obtenus par la formule de Taylor-Lagrange, on a

$$\frac{x_{n+1} - a}{(x_n - a)^2} = \frac{f''(z_n)}{2f'(x_n)} \underset{n\to+\infty}{\longrightarrow} \frac{f''(a)}{2f'(a)}$$

car $a < z_n < x_n \underset{n\to+\infty}{\longrightarrow} a$, d'où le résultat. □

2.7.2 Références

[Rou09], pp. 152-156.

2.7.3 Questions classiques

1. *On fixe $y > 0$ et on prend $f(x) = x^2 - y$. Résolvez la relation de récurrence et donnez une estimation de l'erreur $x_n - a$, avec $a = \sqrt{y}$* : On se place sur un intervalle $[c, d]$ où nos hypothèses sont vérifiées. Dès que $0 < c < d$ et $c^2 < y < d^2$ c'est bon : $f(c) < 0 < f(d)$, $f'(x) = 2x > 0$ et $f''(x) = 2 > 0$. On doit donc itérer la fonction

$$F(x) = x - \frac{x^2 - y}{2x} = \frac{1}{2}(x + \frac{y}{x}).$$

D'après $(*)$ ou par vérification immédiate, on a que

$$F(x) - a = \frac{(x-a)^2}{2x}.$$

Pour approcher l'autre racine $-a = -\sqrt{y}$, on serait amenés à considérer la même fonction F, qui satisfait donc aussi a

$$F(x) + a = \frac{(x+a)^2}{2x}$$

(on aurait encore pu vérifier ça directement). Par suite,

$$\frac{F(x) - a}{F(x) + a} = \left(\frac{x-a}{x+a}\right)^2$$

pour $x > 0$, autrement dit

$$F = \varphi^{-1} \circ G \circ \varphi$$

en notant

$$\varphi(x) = \frac{x-a}{x+a}, G(x) = x^2.$$

Ainsi F est conjuguée par φ à la fonction $x \mapsto x^2$. L'itération $x_n = F^n(x_0)$ s'explicite donc en

$$x_n = (\varphi^{-1} \circ G^n \circ \varphi)(x_0), \text{ i.e. } \frac{x_n - a}{x_n + a} = \Big(\frac{x_0 - a}{x_0 + a}\Big)^{2^n}.$$

Pour $x_0 > a$ on en déduit $x_n > a$ et

$$1 + \frac{2a}{x_n - a} = \Big(1 + \frac{2a}{x_0 - a}\Big)^{2^n} \geq 1 + \Big(\frac{2a}{x_0 - a}\Big)^{2^n},$$

d'où la majoration d'erreur

$$0 < x_n - a \leq 2a\Big(\frac{x_0 - a}{2a}\Big)^{2^n}.$$

2.7.4 Remarques

— On transforme la recherche de 0 en un problème de point fixe : l'idée est de prendre $F(x) = x + \lambda(x)f(x)$ avec λ qui ne s'annule pas. On veut de plus que le point soit superattractif pour avoir une convergence rapide, i.e. que $F'(a) = 0$. Or $F'(a) = 1 + \lambda(a)f'(a)$, ce qui nous incite à prendre $\lambda = -\frac{1}{f'(x)}$ et on retrouve la méthode.

— Géométriquement, on définit l'élément x_{n+1} comme étant l'intersection de la tangente au graphe de f en x_n et l'axe de abscisses. Un dessin permet d'illustrer la vitesse de convergence, en devenant brouillon dès la deuxième itération.

— Isaac Newton : philosophe, mathématicien, physicien, alchimiste, astronome et théologien anglais, 1642-1727

2.8 Une fonction continue, nulle part dérivable

2.8.1 Développement

Proposition 14. *On note Δ la fonction réelle 1 périodique, dont la restriction à $[-\frac{1}{2}, \frac{1}{2}]$ vérifie $\Delta(x) = |x|$. Alors la fonction*

$$f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \sum_{p=0}^{+\infty} \frac{1}{2^p} \Delta(2^p x) \end{array}$$

est continue mais n'est dérivable en aucun point de $\mathbb{R}$.

Démonstration. On commence par remarquer que pour tout $x \in \mathbb{R}$, $|\Delta(x)| \leq \frac{1}{2}$ et donc la série de fonctions $\sum \frac{1}{2^p} \Delta(2^p x)$ converge normalement sur $\mathbb{R}$. Ainsi, f est bien définie sur $\mathbb{R}$, et comme Δ est continue, f est aussi continue. Montrons maintenant que f n'est dérivable en aucun point de $\mathbb{R}$. Comme f est $1-$périodique, il suffit de montrer que f n'est dérivable en aucun point de $[0, 1[$. Soit $x_0 \in [0, 1[$. On considère l'écriture dyadique de $x_0 = \sum_{k=1}^{+\infty} \frac{\varepsilon_k}{2^k}$, où $\varepsilon_k \in \{0, 1\}$ pour tout k. Pour tout $n \in \mathbb{N}^*$, on pose

$$x'_n = \sum_{k=1}^{n} \frac{\varepsilon_k}{2^k} \quad \text{et} \quad x''_n = x'_n + \frac{1}{2^n}.$$

Les deux suites $(x'_n)_{n\in\mathbb{N}^*}$ et $(x''_n)_{n\in\mathbb{N}^*}$ tendent vers x_0. Lorsque $p \geq n$, les nombres $2^p x'_n$ et $2^p x''_n$ sont des entiers, donc $\Delta(2^p x'_n) = \Delta(2^p x''_n) = 0$. À présent, si $p < n$, on a

$$2^p x'_n = N + \sum_{k=p+1}^{n} \frac{\varepsilon_k}{2^{k-p}} \quad \text{où} \quad N = \sum_{k=1}^{p} 2^{p-k} \varepsilon_k \quad \text{est un entier,}$$

donc

$$\Delta(2^p x'_n) = \Delta\Big(\sum_{k=p+1}^{n} \frac{\varepsilon_k}{2^{k-p}}\Big) \quad \text{et de même} \quad \Delta(2^p x''_n) = \Delta\Big(\sum_{k=p+1}^{n} \frac{\varepsilon_k}{2^{k-p}} + \frac{1}{2^{n-p}}\Big). \qquad (*)$$

Si $\varepsilon_{p+1} = 0$, l'encadrement

$$0 \leq \sum_{k=p+1}^{n} \frac{\varepsilon_k}{2^{k-p}} + \frac{1}{2^{n-p}} \leq \sum_{k=p+2}^{n} \frac{1}{2^{k-p}} + \frac{1}{2^{n-p}} = \frac{1}{2}$$

montre que nous travaillons alors dans l'intervalle $[0, \frac{1}{2}]$, sur lequel Δ est l'identité, ce qui nous permet d'écrire

$$\text{si} \quad \varepsilon_{p+1} = 0, \Delta(2^p x''_n) - \Delta(2^p x'_n) = \frac{1}{2^{n-p}}.$$

On montrerait de même que

$$\text{si} \quad \varepsilon_{p+1} = 1, \Delta(2^p x''_n) - \Delta(2^p x'_n) = -\frac{1}{2^{n-p}}.$$

En résumé, on a $\Delta(2^p x''_n) - \Delta(2^p x'_n) = \frac{(-1)^{\varepsilon_{p+1}}}{2^{n-p}}$ pour $0 \leq p < n$, donc finalement

$$f(x''_n) - f(x'_n) = \sum_{k=0}^{n-1} \frac{(-1)^{\varepsilon_{p+1}}}{2^n} \qquad \text{ou encore} \qquad \frac{f(x''_n) - f(x'_n)}{x''_n - x'_n} = \sum_{p=0}^{n-1} (-1)^{\varepsilon_{p+1}},$$

ce qui montre que la suite $(y_n)_{n\in\mathbb{N}^*}$ définie par $y_n = \frac{f(x''_n)-f(x'_n)}{x''_n-x'_n}$ ne converge pas. Si maintenant f est dérivable en x_0, on a

$$f(x'_n) - f(x_0) = (x'_n - x_0)[f'(x_0) + \varepsilon'_n] \qquad \text{et} \qquad f(x''_n) - f(x_0)[f'(x_0) + \varepsilon''_n]$$

où les suites $(\varepsilon'_n)_{n\in\mathbb{N}^*}$ et $(\varepsilon''_n)_{n\in\mathbb{N}^*}$ tendent vers 0. Par différence, on a

$$f(x''_n) - f(x'_n) = (x''_n - x'_n)f'(x_0) + (x_0 - x'_n)\varepsilon_n + (x''_n - x_0)\varepsilon''_n,$$

et comme $x'_n \leq x_0 \leq x''_n$, ceci entraîne

$$|f(x''_n) - f(x'_n) - (x''_n - x'_n)f'(x_0)| \leq (x''_n - x'_n)(\varepsilon'_n + \varepsilon''_n)$$

donc $|y_n - f'(x_0)| \leq \varepsilon'_n + \varepsilon''_n$, donc y_n converge vers $f'(x_0)$, ce qui est contradictoire. Donc f n'est pas dérivable en 0, d'où le résultat.

□

2.8.2 Références

[Gou08], pp. 84-85.

2.8.3 Questions classiques

1. *Expliquez pourquoi la suite $(y_n)_{n\in\mathbb{N}^*}$ ne converge pas* : On a vu que $y_n = \sum_{p=0}^{n-1}(-1)^{\varepsilon_{p+1}}$. Le terme général de cette série étant à valeurs dans $\{-1, 1\}$, il ne peut pas tendre vers 0. Or une série dont le terme général ne tend pas vers 0 ne peut pas converger (on écrit $u_n = \sum_{k=0}^{n} u_k - \sum_{k=0}^{n-1} u_k$), et ainsi $(y_n)_{n\in\mathbb{N}^*}$ n'est pas convergente.

2.8.4 Remarques

— La preuve consiste à construire une série qui introduit une singularité à chaque point admettant un développement dyadique fini d'ordre n, et à étudier le passage à la limite.

2.9 Développement asymptotique de la série harmonique

2.9.1 Développement

Proposition 15. *On donne un développement asymptotique de quatre termes de la série harmonique $H_n = \sum_{k=1}^{n} \frac{1}{k}$, à savoir*

$$H_n = \ln n + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + o\Big(\frac{1}{n^2}\Big).$$

Démonstration. On commence par poser $u_n = H_n - \ln n$ et $v_n = u_n - \frac{1}{n}$. On va montrer que ces suites sont adjacentes : leur différence $u_n - v_n = \frac{1}{n}$ est positive et converge vers 0. La suite $(u_n)_{n\in\mathbb{N}^*}$ est décroissante puisque

$$u_n - u_{n+1} = -\frac{1}{n+1} - \ln n + \ln(n+1) = -\frac{1}{n+1} - \ln\Big(1 - \frac{1}{n+1}\Big) \geq 0$$

en vertu de l'inégalité $\ln(1+x) \leq x$ pour $x > -1$. Cette même inégalité assure la croissance de la suite $(v_n)_{n\in\mathbb{N}^*}$ puisque

$$v_{n+1} - v_n = \frac{1}{n} - \ln(n+1) + \ln n = \frac{1}{n} - \ln\Big(1 + \frac{1}{n}\Big) \geq 0.$$

Les deux suites sont donc adjacentes et convergent vers un réel γ. Comme $v_2 = 1 - \ln(2) > 0$ (toujours de par l'inégalité précédente), on a $\gamma > 0$. On a alors

$$H_n = \ln n + u_n = \ln n + \gamma + o(1).$$

Pour établir les termes suivants, posons $t_n = u_n - \gamma$. On emploie une méthode classique qui consiste, pour obtenir un équivalent à t_n, à chercher un équivalent de $t_n - t_{n-1}$ puis à "sommer" l'équivalent obtenu. On a que

$$t_n - t_{n-1} = \ln\Big(1 - \frac{1}{n}\Big) + \frac{1}{n} \sim -\frac{1}{2n^2}$$

en utilisant le développement limité $\ln(1-x) = -x - \frac{x^2}{2} + o(x^2)$. Ces deux suites étant de signe négatif, leurs séries sont de même nature et donc la série $\sum(t_k - t_{k-1})$ converge grâce au critère de Riemann. Le théorème de sommation des équivalents donne

$$-t_n = \sum_{k=n+1}^{+\infty} (t_k - t_{k-1}) \sim -\frac{1}{2} \sum_{k=n+1}^{+\infty} \frac{1}{k^2} \sim -\frac{1}{2n},$$

le dernier équivalent s'obtenant à l'aide d'une comparaison série intégrale. En effet, comme $t \mapsto \frac{1}{t^2}$ est continue, décroissante sur $[1, +\infty[$, on a pour $k \geq 2$ que

$$\frac{1}{(k+1)^2} \leq \int_k^{k+1} \frac{1}{t^2} dt \leq \frac{1}{k^2} \leq \int_{k-1}^{k} \frac{1}{t^2} dt.$$

En sommant cela de $n+1$ à N, puis en faisant tendre N vers l'infini, on obtient donc

$$\int_{n+1}^{+\infty} \frac{1}{t^2} dt \leq \sum_{k=n+1}^{+\infty} \frac{1}{k^2} \leq \int_n^{+\infty} \frac{1}{t^2} dt.$$

Les termes de gauche et droites étant équivalents tout deux à $\frac{1}{n}$, on en déduit par encadrement que $\sum_{k=n+1}^{+\infty} \frac{1}{k^2} \sim \frac{1}{n}$, d'où le résultat. Bref,

$$H_n = \ln n + \gamma + t_n = \ln n + \gamma + \frac{1}{2n} + o\Big(\frac{1}{n}\Big).$$

On termine avec la même technique : on écrit $w_n = u_n - \gamma - \frac{1}{2n}$, suite qui converge vers 0. La somme $\sum_{k=n+1}^{+\infty} (w_k - w_{k-1})$ vaut $-w_n$ et son terme général s'écrit

$$w_n - wn - 1 = \ln(1 - \frac{1}{n}) + \frac{1}{n} - \frac{1}{2n} + \frac{1}{2n-2}.$$

On a donc, a l'aide du développement limité $\ln(1-x) = -x - \frac{x^2}{2} - \frac{x^3}{3} + o(x^3)$,

$$\begin{aligned} w_n - w_{n-1} &= -\frac{1}{n} - \frac{1}{2n^2} - \frac{1}{3n^3} + \frac{1}{n} - \frac{1}{2n} + \frac{1}{2n} \cdot \frac{1}{1 - \frac{1}{n}} + o\Big(\frac{1}{n^3}\Big) \\ &= -\frac{1}{2n^2} - \frac{1}{3n^3} - \frac{1}{2n} + \frac{1}{2n}\Big(1 + \frac{1}{n} + \frac{1}{n^2} + o\Big(\frac{1}{n^2}\Big)\Big) + o\Big(\frac{1}{n^3}\Big) \\ &= -\frac{1}{3n^3} + \frac{1}{2n^3} + o\Big(\frac{1}{n^3}\Big) \sim \frac{1}{6n^3}. \end{aligned}$$

On a alors comme précédemment que

$$-w_n \sim \sum_{k=n+1}^{+\infty} \frac{1}{6k^3} \sim \frac{1}{12n^2}.$$

Finalement, on obtient

$$H_n = \ln n + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + o\Big(\frac{1}{n^2}\Big).$$

□

2.9.2 Références

[FGN14c], pp. 156-159.

2.9.3 Questions classiques

1. *Détaillez l'inégalité* $\ln(1+x) \leq x$ *pour* $x > -1$: On a que

$$(-\ln(1+x))'' = \frac{1}{(1+x)^2} > 0$$

   donc la fonction logarithme est concave et est par conséquent en dessous de ses tangentes. Or sa tangente en 0 est justement

$$\ln(1+x)'|_{x=0}(x-0) + \ln(1+0) = x.$$

2. *Détaillez pourquoi* $t_n = \frac{1}{2n} + o(\frac{1}{n})$: Par définition, $f \sim g$ si et seulement si $f - g = o(g)$. Ici, $t_n = \frac{1}{2n} + o(\frac{1}{2n})$ et les $o(\frac{1}{2n})$ sont exactement les $o(\frac{1}{n})$.

2.9.4 Remarques

— On appelle $\gamma = 0,577215664...$ la constante d'Euler.

2.10 Densité des polynômes orthogonaux

2.10.1 Développement

Soit $I \subset \mathbb{R}$ un intervalle. On appelle poids une fonction $\rho : I \to \mathbb{R}^{+*}$ mesurable telle que $\forall n \in \mathbb{N}, \int_I |x|^n \rho(x)dx < +\infty$. On note $\mathrm{L}^2(I,\rho)$ l'espace des fonctions de carré intégrable pour la mesure de densité ρ par rapport à la mesure de Lebesgue, qui est un espace de Hilbert pour le produit scalaire $\langle f,g\rangle_\rho = \int_I f(x)\overline{g(x)}\rho(x)dx$. On appelle polynômes orthogonaux associée au poids ρ la famille de polynômes $(P_n)_{n\in\mathbb{N}}$ unitaires, orthogonaux deux à deux et tels que $\deg P_n = n$ obtenus en appliquant le procédé d'orthogonalisation de Gram-Schmidt à la famille $(x^n)_{n\in\mathbb{N}}$ (on confond polynôme et fonction polynomiale). Le résultat est le suivant :

Théorème 23. *On suppose qu'il existe $\alpha > 0$ tel que $\int_I e^{\alpha|x|}\rho(x)dx < +\infty$. Alors les polynômes orthogonaux associés au poids ρ forment une base hilbertienne de $\mathrm{L}^2(I,\rho)$.*

Démonstration. On commence par vérifier rapidement que les polynômes sont bien dans $\mathrm{L}^2(I,p)$, en montrant qu'en fait on a $x \mapsto x^n \in L^p(I,\rho)$ pour tout $n \in \mathbb{N}$ et $p \in [1,+\infty[$: on a en effet l'inégalité $|x|^{np} \leq 1 + |x|^{\lfloor np\rfloor+1}$ pour tout $x \in \mathbb{R}$ et donc

$$\int_I |x|^{np}p(x)dx \leq \int_I (1+|x|^{\lfloor np\rfloor+1})\rho(x)dx < +\infty$$

par le fait que ρ est un poids.

À présent, on considère $f \in \mathrm{L}^2(I,\rho)$ quelconque : le but est de montrer que si l'on a $\langle f,x^n\rangle_\rho = 0$ pour tout $n \in \mathbb{N}$, alors $f = 0$ pour presque tout $x \in I$, ce qui assurera que la famille de polynômes orthogonaux est une base hilbertienne (comme nous travaillons dans un espace de Hilbert séparable...). On définit pour cela $\varphi : \mathbb{R} \to \mathbb{R}$ par $\varphi(x) = f(x)\rho(x)\mathbf{1}_I(x)$. Montrons que $\varphi \in \mathrm{L}^1(\mathbb{R})$: on remarque que pour $t \leq 0$, on a l'inégalité $t \leq \frac{(1+t^2)}{2}$ (en vertu de $t^2 - 2t + 1 = (t-1)^2 \geq 0$), et on a donc que

$$\forall x \in I, |f(x)|\rho(x) \leq \frac{1}{2}(1+|f(x)|^2)\rho(x).$$

Comme ρ et $f^2\rho$ sont intégrables sur I (respectivement car ρ est un poids et car $f \in \mathrm{L}^2(I,\rho)$), on a finalement que $\varphi \in \mathrm{L}^1(\mathbb{R})$. On peut alors considérer sa transformée de Fourier, définie par $\hat{\varphi}(\omega) = \int_I e^{-i\omega x}f(x)\rho(x)dx$ pour $\omega \in \mathbb{R}$. Celle-ci se prolonge en une fonction F holomorphe sur $B_\alpha = \{z \in \mathbb{C}\ ;\ |\mathrm{Im}(z)| < \frac{\alpha}{2}\}$: montrons le. Si l'on note $g(z,x) = e^{-izx}f(x)\rho(x)$, alors pour $z \in B_\alpha$ on peut écrire

$$\int_I |g(z,x)|dx \leq \int_I e^{\frac{\alpha|x|}{2}}|f(x)|\rho(x)dx.$$

En utilisant l'inégalité de Hölder, on obtient de plus

$$\int_I e^{\frac{\alpha|x|}{2}}|f(x)|\rho(x)dx \leq \Big(\int_I e^{\alpha|x|}\rho(x)dx\Big)^{\frac{1}{2}}\Big(\int_I |f(x)|^2\rho(x)dx\Big)^{\frac{1}{2}} < +\infty$$

par hypothèse sur notre poids. On peut donc définir $F : B_\alpha \to \mathbb{C}$ par

$$\forall z \in B_\alpha, F(z) = \int_I e^{-izx}f(x)\rho(x)dx = \int_I g(z,x)dx.$$

On vérifie ensuite les hypothèses du théorème d'holomorphie sous le signe somme :

— Pour tout $z \in B_\alpha, x \mapsto g(z,x)$ est mesurable comme on vient de le voir,

— Pour tout $x \in I$, l'application $z \mapsto g(z,x)$ est holomorphe en tant que composée de fonctions holomorphes,

— Pour tout $z \in B_\alpha$, on a la majoration $|g(z,x)| \leq h(x) = e^{\frac{\alpha|x|}{2}}|f(x)|\rho(x)$, et on a vu que la fonction h était intégrable.

On a donc que F est holomorphe sur B_α et coïncide avec $\hat{\varphi}$ sur $\mathbb{R}$. Calculons les dérivées de F :

$$\forall z \in B_\alpha, F^{(n)}(z) = (-i)^n \int_I x^n e^{-izx}f(x)\rho(x)dx.$$

Ainsi on obtient

$$F^{(n)}(0) = (-i)^n \int_I x^n f(x)\rho(x)dx = (-i)^n\langle f, x^n\rangle_\rho = 0$$

en utilisant notre hypothèse sur f. L'analycité de F implique alors que $F = 0$ sur un voisinage de 0, et le théorème de prolongement analytique implique quant à lui que $F = 0$ sur le connexe B_α tout entier, en particulier sur $\mathbb{R}$. On a donc $\hat{\varphi} = 0$, et ainsi $\varphi = 0$ par injectivité de la transformée de Fourier. On en déduit comme $\rho(x) > 0$ pour tout $x \in I$ que $f(x) = 0$ pour presque tout $x \in I$. On a prouvé notre théorème. □

2.10.2 Références

[BMP05], pp. 112, 140-142.

2.10.3 Questions classiques

1. *Montrez que sur* $I =]0, +\infty[$ *muni du poids* $w(x) = x^{-\ln(x)}$, *les polynômes orthogonaux pour le poids* w *ne forment pas une base hilbertienne de* $\mathrm{L}^2(I, w)$: On considère la fonction $f : I \to \mathbb{R}$ définie par $f(x) = \sin(2\pi \ln(x))$. Montrons qu'elle est orthogonale à tous les monômes : on calcule donc

$$\langle f, x^n \rangle_w = \int_I x^n \sin(2\pi \ln(x)) x^{-\ln(x)} dx.$$

Le changement de variables $y = \ln(x)$ permet d'écrire

$$\langle f, x^n \rangle_w = \int_{\mathbb{R}} e^{(n+1)y} \sin(2\pi y) e^{-y^2} dy = e^{\frac{(n+1)^2}{4}} \int_{\mathbb{R}} e^{-(y-\frac{n+1}{2})^2} \sin(2\pi y) dy.$$

Le deuxième changement de variables $t = y - \frac{n+1}{2}$ donne

$$\langle f, x^n \rangle_w = (-1)^{n+1} e^{\frac{(n+1)^2}{4}} \int_{\mathbb{R}} \sin(2\pi t) e^{-t^2} = 0$$

puisque la fonction est impaire : ainsi la famille des monômes n'est pas totale dans $L^2(I, w)$ et donc la famille des polynômes orthogonaux pour le poids w ne saurait l'être.

2. *Donnez des exemples de polynômes orthogonaux* : On a les polynômes d'Hermite, donnés par $I = \mathbb{R}$ et $\rho(x) = e^{-x^2}$:

$$P_0 = 1, P_1 = X, P_2 = X^2 - \frac{1}{2}, \ldots, P_n = \frac{(-1)^n}{2^n} e^{x^2} \frac{d^n}{dx^n}(e^{-x^2}).$$

On a aussi les polynômes de Legendre, donnés par $I = [-1, 1]$ et $\rho(x) = 1$:

$$P_0 = 1, P_1 = X, P_2 = X^2 - \frac{1}{3}, \ldots, P_n = \frac{n!}{(2n)!} \frac{d^n}{dx^n}((x^2 - 1)^n).$$

3. *À l'aide du théorème, exhibez une base hilbertienne de* $\mathrm{L}^2(\mathbb{R})$: À l'aide des polynômes d'Hermite, i.e. $\rho(x) = e^{-x^2}$, on exhibe une base hilbertienne de L^2 via l'isométrie

$$i : \begin{array}{ccc} \mathrm{L}^2(\mathbb{R}, \rho) & \longrightarrow & \mathrm{L}^2(\mathbb{R}) \\ f & \longmapsto & f\sqrt{\rho} \end{array},$$

à savoir les $(P_n(x)e^{-\frac{x^2}{2}})$.

2.10.4 Remarques

— La méthode utilisée dans la preuve consiste à se placer sur un ouvert complexe connexe contenant la droite réelle pour passer d'un résultat local à un résultat global grâce aux propriétés des fonctions holomorphes.

— Lorsque l'intervalle I est borné, on peut utiliser d'autres arguments pour prouver ce résultat (le théorème d'approximation de Weierstrass et la continuité de l'inclusion $C(I) \subset \mathrm{L}^2(I, \rho)$).

— Il est bon d'avoir une interprétation géométrique du procédé d'orthogonalisation de Gram-Schidt.

2.11 Théorème d'approximation de Weierstrass par les polynômes de Bernstein

2.11.1 Développement

Théorème 24. *Soit $f : [0,1] \to \mathbb{C}$ une fonction continue, ω son module de continuité uniforme, i.e. $\omega(h) = \sup\{|f(u) - f(v)| \ ; \ |u - v| \leq h\}$. Pour $n \geq 1$, on considère le polynôme $B_n(f,x) = B_n(x) = \sum_{k=0}^{n} \binom{n}{k} x^k (1-x)^{n-k} f\left(\frac{k}{n}\right)$ le $n-$ième polynôme de Bernstein. Alors :*

1. *La suite des B_n converge uniformément vers f sur $[0,1]$,*
2. *Plus précisément, on a $||f - B_n||_\infty \leq C\omega(\frac{1}{\sqrt{n}})$, où C est une constante numérique.*

Démonstration. 1. Soit $x \in [0,1]$, $X \sim \mathcal{B}(x)$, $X_1, \ldots, X_n$ un échantillon de X et $S_n = X_1 + \cdots + X_n$. On a alors par le théorème du transport que

$$\mathbb{E}(f\Big(\frac{S_n}{n}\Big)) = \sum_{k=0}^{n} \binom{n}{k} x^k (1-x)^{n-k} f\Big(\frac{k}{n}\Big) = B_n(x).$$

Fixons $\delta \in]0,1[$: on a $f(x) - B_n(x) = \mathbb{E}(f(x) - f(\frac{S_n}{n}))$, d'où $|f(x) - B_n(x)| \leq \mathbb{E}(|f(x) - f(\frac{S_n}{n})|)$. Or on a que $|f(x) - f(\frac{S_n}{n})| \leq \omega(\delta)$ lorsque $|x - \frac{S_n}{n}| \leq \delta$, et $|f(x) - f(\frac{S_n}{n})| \leq 2||f||_\infty$ lorsque $|x - \frac{S_n}{n}| > \delta$, ce qui nous donne :

$$\begin{aligned}
\mathbb{E}(|f(x) - f\Big(\frac{S_n}{n}\Big)|) &\leq \omega(\delta) + 2||f||_\infty \cdot \mathbb{E}(\mathbf{1}_{\{|x - \frac{S_n}{n}| > \delta\}}) \\
&= \omega(\delta) + 2||f||_\infty \cdot \mathbb{P}\Big(\Big|\frac{S_n}{n} - x\Big| > \delta\Big) \\
&\leq \omega(\delta) + \frac{||f||_\infty}{2n\delta^2},
\end{aligned}$$

où l'on a utilisé à la fin l'inégalité de Bienaymé-Tchebychev. Il en résulte que $||f - B_n||_\infty \leq \omega(\delta) + \frac{||f||_\infty}{2n\delta^2}$, puis que $\limsup_{n \to +\infty} ||f - B_n||_\infty \leq \omega(\delta)$. Or, $\omega(\delta) \underset{\delta \to 0}{\longrightarrow} 0$, ce qui implique finalement $\lim_{n \to +\infty} ||f - B_n||_\infty = 0$.

2. On utilise pour cette partie l'inégalité $\omega(\lambda h) \leq (\lambda + 1)\omega(h)$ si $h, \lambda h \in [0,1]$. Cela nous donne en particulier que $\omega(|x - \frac{S_n}{n}|) \leq (\sqrt{n}|x - \frac{S_n}{n}| + 1)\omega(\frac{1}{\sqrt{n}})$. Or nous savons que $|f(x) - B_n(x)| \leq \mathbb{E}(|f(x) - f(\frac{S_n}{n})|) \leq$

$\mathbb{E}(\omega(|x-\frac{S_n}{n}|))$. Il en résulte que

$$\begin{aligned}
|f(x)-B_n(x)| &\leq \omega\Big(\frac{1}{\sqrt{n}}\Big)\mathbb{E}\Big(\sqrt{n}|x-\frac{S_n}{n}|+1\Big)\\
&= \omega\Big(\frac{1}{\sqrt{n}}\Big)\Big(1+\sqrt{n}||x-\frac{S_n}{n}||_1\Big)\\
&\leq \omega\Big(\frac{1}{\sqrt{n}}\Big)\Big(1+\sqrt{n}||x-\frac{S_n}{n}||^2\Big)\\
&= \omega\Big(\frac{1}{\sqrt{n}}\Big)\Big[1+\sqrt{n}\sqrt{\frac{x(1-x)}{n}}\Big] \leq \frac{3}{2}\omega\Big(\frac{1}{\sqrt{n}}\Big),
\end{aligned}$$

ce qui démontre le résultat annoncé avec $C=\frac{3}{2}$.

□

2.11.2 Références

[QZ13], pp. 518-519.

2.11.3 Questions classiques

1. *Que pouvez-vous dire à propos de la vitesse de convergence de cette méthode* : On sait modulo un exercice que l'estimation précédente est optimale et que la vitesse est donc en $\frac{1}{\sqrt{n}}$: c'est donc un résultat qui est d'ordre théorique et non pratique, la convergence n'étant pas polynomiale elle n'est pas réellement exploitable.

2.11.4 Remarques

— L'intuition qui guide la première partie de la preuve est que $B_n(x)$ devrait être proche de de $\mathbb{E}(f(x))=f(x)$ étant donné que l'on a convergence en probabilité de $\frac{S_n}{n}$ vers x.

— Karl Weierstrass : mathématicien allemand, 1815-1897

— Sergeï Bernstein : mathématicien russe, 1880-1968

2.12 Théorème central limite

2.12.1 Développement

Théorème 25 (Théorème central limite)**.** *Soit $(X_n)_{n\in\mathbb{N}}$ une suite de variables aléatoires i.i.d. de $\mathrm{L}^2(\Omega,\mathcal{A},\mathbb{P})$. On note $S_n=\sum_{i=1}^n X_i$, $\mu=\mathbb{E}(X_1)$ et $\sigma^2=\mathrm{Var}(X_1)>0$. Alors on a que*

$$\frac{S_n-n\mu}{\sqrt{n\sigma^2}} \xrightarrow{\mathcal{L}} \mathcal{N}(0,1),$$

la notation signifiant que la variable aléatoire limite suit une loi normale centrée réduite.

La démonstration s'appuie sur le théorème de Lévy, dont la preuve générale est difficile, qui affirme que (X_n) converge en loi vers X si et seulement si φ_{X_n} converge simplement vers φ_X. Donnons la preuve dans le cas réel [9] :

Démonstration. Si (X_n) converge en loi vers X, alors comme $x\mapsto e^{itx}$ est continue pour tout $t\in\mathbb{R}$, on a que $\varphi_{X_n}(t)$ converge vers $\varphi_X(t)$ pour tout t par définition de la convergence en loi. Pour la réciproque, considérons d'abord le cas où f est dans l'image de la transformée de Fourier des fonctions L^1, i.e. $f(x)=\int_{\mathbb{R}} e^{itx}\varphi(t)\,dt$ avec $\varphi\in\mathrm{L}^1$. Le théorème de Fubini et le théorème de convergence dominée assurent que

$$\mathbb{E}(f(X_n))=\mathbb{E}\Big(\int_{\mathbb{R}} e^{itX_n}\varphi(t)\,dt\Big)=\int_{\mathbb{R}}\varphi(t)\mathbb{E}(e^{itX_n})\,dt\longrightarrow\int_{\mathbb{R}}\varphi(t)\mathbb{E}(e^{itX})\,dt=\mathbb{E}(f(X)).$$

Comme l'image de la transformée de Fourier sur L^1 contient l'espace de Schwartz, elle est uniformément dense dans $C_0(\mathbb{R})$. On a encore $\mathbb{E}(f(X_n))\to\mathbb{E}(f(X))$ pour tout $f\in C_0(\mathbb{R})$, ce qui achève la preuve. □

On a ensuite la proposition suivante :

Proposition 16. *Soit X une variable aléatoire de loi $\mathcal{N}(0,1)$. Alors sa fonction caractéristique est donnée par*

$$\forall t\in\mathbb{R},\ \varphi_X(t)=e^{-\frac{t^2}{2}}.$$

Démonstration. On a par définition que, pour tout $t\in\mathbb{R}$,

$$\varphi_X(t)=\int_\Omega e^{itX}\,d\mathbb{P}\overset{\text{T.T.}}{=}\int_{\mathbb{R}} e^{itx}\,d\mathbb{P}_X(x)=\frac{1}{\sqrt{2\pi}}\int_{\mathbb{R}} e^{itx-\frac{x^2}{2}}\,dx.$$

Montrons qu'elle est de classe C^1, ce grâce au théorème de dérivation sous le signe somme appliqué à la fonction $g(x,t)=e^{itx-\frac{x^2}{2}}$:

9. À effectuer en fin de développement s'il reste du temps.

— Pour tout $t \in \mathbb{R}, x \mapsto g(x,t)$ est mesurable et intégrable ($|e^{itx-\frac{x^2}{2}}| = e^{-\frac{x^2}{2}} = \underset{+\infty}{o}(\frac{1}{x^2})$),

— Pour tout $x \in \mathbb{R}, t \mapsto g(x,t)$ est de classe C^1, de dérivée $\frac{\partial g}{\partial t}(x,t) = ixe^{itx-\frac{x^2}{2}}$,

— Pour tout $(x,t) \in \mathbb{R}^2$, $|\frac{\partial g}{\partial t}(x,t)| = |x|e^{-\frac{x^2}{2}} =: \psi(x)$, avec $\psi(x)$ intégrable.

Il vient via une intégration par parties que

$$\begin{aligned}\varphi'_X(t) &= \frac{i}{\sqrt{2\pi}}\int_{\mathbb{R}}(xe^{-\frac{x^2}{2}})e^{itx}\,dx \\ &= \frac{i}{\sqrt{2\pi}}\Big[\big[-e^{-\frac{x^2}{2}}e^{itx}\big]_{-\infty}^{+\infty} + it\int_{\mathbb{R}} e^{-\frac{x^2}{2}}e^{itx}\,dx\Big] \\ &= -t\varphi_X(t),\end{aligned}$$

ce qui donne le résultat par facteur intégrant en remarquant que $\varphi_X(0) = 1$. □

Démontrons à présent le théorème :

Démonstration. Quitte à remplacer chacune des X_i par $\frac{X_i-\mu}{\sigma}$, on peut supposer que $\mathbb{E}(X_1) = 0$ et que $\sigma^2 = 1$. Il s'agit donc de montrer que $\varphi_{\frac{S_n}{\sqrt{n}}}$ converge simplement vers la fonction $t \mapsto e^{-\frac{t^2}{2}}$ sur $\mathbb{R}$. L'hypothèse d'indépendance des X_i permet d'écrire

$$\forall t \in \mathbb{R}, \varphi_{\frac{S_n}{\sqrt{n}}}(t) = \varphi_{X_1}\Big(\frac{t}{\sqrt{n}}\Big)^n.$$

Comme X_1 admet des moments jusqu'à l'ordre 2, φ est de classe C^2 et on a $\varphi'_{X_1}(0) = i\mathbb{E}(X_1) = 0$ et $\varphi''_{X_1}(0) = -\mathbb{E}(X_1^2) = -1$; son développement limité à l'ordre 2 au voisinage de 0 s'écrit donc

$$\forall t \in \mathbb{R}, \varphi_{X_1}(t) = 1 - \frac{t^2}{2} + o(t^2).$$

On a alors pour $t \in \mathbb{R}$ fixé :

$$\forall n \in \mathbb{N}^*, \varphi_{X_1}\Big(\frac{t}{\sqrt{n}}\Big) = 1 - \frac{t^2}{2n} + o\Big(\frac{1}{n}\Big),$$

d'où

$$\forall n \in \mathbb{N}^*, \varphi_{\frac{S_n}{\sqrt{n}}}(t) = \Big(1 - \frac{t^2}{2n} + o\Big(\frac{1}{n}\Big)\Big)^n.$$

Or, comme pour n assez grand on a $1 - \frac{t^2}{2n} + o(\frac{1}{n}) \in B(1, \frac{1}{2}) \subset \mathbb{C}$, on peut considérer la détermination principale du logarithme complexe sur $\mathbb{C} \setminus \mathbb{R}^{*-}$ pour finalement écrire :

$$\begin{aligned} \varphi_{\frac{S_n}{\sqrt{n}}}(t) &= e^{n \ln(1 - \frac{t^2}{2n} + o(\frac{1}{n}))} \\ &= e^{-\frac{t^2}{2} + o(1)} \underset{n \to +\infty}{\longrightarrow} e^{-\frac{t^2}{2}}, \end{aligned}$$

d'où le résultat.

□

2.12.2 Références

[QZ13], p. 536, [BL07], pp. 70, 136-137.

2.12.3 Questions classiques

1. *Justifiez comment vous étendez la convergence aux $f \in C_0(\mathbb{R})$* : En considérant $f \in C_0(\mathbb{R})$, on peut l'approcher uniformément par une suite de de fonctions $C^\infty(\mathbb{R})$ à support compact, en prenant la fonction qui vaut 0 dès que f est plus petite que $\frac{1}{n}$ - disons sur $]-M, M[$ - et on utilise la densité de $C_0^\infty([-M + \varepsilon, M - \varepsilon])$ dans $C([-M, M])$ pour la norme uniforme pour finalement obtenir $\psi_n \in C_0^\infty(\mathbb{R})$ telle que $||\psi_n - f||_\infty \leq \frac{1}{n}$ (le ε est là pour assurer que le raccord se fasse bien de manière C^∞). On écrit finalement que :

2.12.4 Remarques

— Dans la preuve du théorème de Lévy, on utilise le fait qu'il y a équivalence entre $\mathbb{E}(f(x_n)) \to \mathbb{E}(f(X))$ pour tout $f \in C_0(\mathbb{R})$ et pour tout $f \in C_b^0(\mathbb{R})$.

— On est obligé de considérer la détermination principale du logarithme complexe, car la fonction caractéristique est *a priori* à valeurs complexes, ce qui est caché dans le $o(\frac{1}{n})$.

— À propos des petits o, il faut faire remarquer que la variable impliquée à t fixé est alors l'entier n.

2.13 Théorème de projection dans un espace de Hilbert

2.13.1 Développement

Théorème 26. *Soit K un convexe fermé d'un espace de Hilbert $(H, \langle .,. \rangle)$ et $x \in H$. Alors :*

1. *Il existe un unique $p_K(x) \in K$ tel que $||x - p_K(x)|| = d(x, K)$,*
2. *Le point $p_K(x)$ est caractérisé par $\forall u \in K, \mathrm{Re}\langle x - p_K(x), u - p_K(x)\rangle \leq 0$,*
3. *L'application $p_K : H \to K, x \mapsto p_K(x)$ est 1-lipschitzienne.*

Démonstration. Démontrons le résultat point par point :

1. Montrons l'existence puis l'unicité.

   — Existence : Soit $x \in H$. Montrons l'existence de $p_K(x)$. On note $d = d(x, K)$. Comme $d = \inf\{||x - k|| \ ; \ k \in K\}$, il existe une suite minimisante (k_n) de points de K, i.e. telle que $\lim_{n\to+\infty} ||x - k_n|| = d$. Montrons que cette suite est de Cauchy : soit $(p, q) \in \mathbb{N}^2$. L'identité du parallélogramme appliquée aux deux points $x - k_p$ et $x - k_q$, donne

   $$||2x - k_p - k_q||^2 + ||k_q - k_p||^2 = 2(||x - k_p||^2 + ||x - k_q||^2)$$

   soit encore

   $$||k_q - k_p||^2 = 2(||x - k_p||^2 + ||x - k_q||^2) - 4||x - \frac{k_p + k_q}{2}||^2.$$

   Comme K est un espace convexe, et que par conséquent $\frac{k_p+k_q}{2} \in K$, on a $||x - \frac{k_p+k_q}{2}|| \leq d$. Il vient alors

   $$||k_q - k_p||^2 \leq 2(||x - k_p||^2 + ||x - k_q||^2) - 4d^2.$$

   Par définition de la suite (k_n), on a $\lim_{p\to+\infty} ||x - k_p|| = \lim_{q\to+\infty} ||x - k_q|| = d$. Ainsi, la suite est de Cauchy et converge dans le complet (car fermé d'un complet) K : on note $p_K(x)$ sa limite. Par continuité de la norme, on a $d = \lim_{n\to+\infty} ||x - k_n|| = ||x - p_K(x)||$.

   — Unicité [10] : Supposons qu'il existe deux points k_1 et k_2 tels que $||x - k_1|| = ||x - k_2|| = d$. Posons $k = \frac{k_1+k_2}{2}$: par convexité de K, $k \in K$ et

10. À admettre car facile.

donc $||x-k|| \geq d$. En appliquant l'identité de la médiane à $x-k_1$ et $x-k_2$, on a

$$4||x-k||^2 + ||k_1-k_2||^2 = 2(||x-k_1||^2 + ||x-k_2||^2) = 4d^2,$$

ce qui donne $||k_1-k_2|| \leq 0$ et $k_1 = k_2$.

2. Montrons que le point $p_K(x)$ vérifie $\forall u \in K, \mathrm{Re}\langle x-p_K(x), u-p_K(x)\rangle \leq 0$. Soit $y \in K$. On a les égalités

$$\begin{aligned} ||x-y||^2 &= ||(x-p_K(x)) - (y-p_K(x))||^2 \\ &= ||x-p_K(x)||^2 - 2\mathrm{Re}\langle x-p_K(x), y-p_K(x)\rangle + ||y-p_K(x)||^2. \end{aligned}$$

Comme $||x-y|| \geq d(x,K) = ||x-p_K(x)||$, on a

$$2\mathrm{Re}\langle x-p_K(x), y-p_K(x)\rangle \leq ||y-p_K(x)||^2.$$

Soit à présent $t \in]0,1]$ et soit $u \in K$. Par convexité de K, $y = (1-t)p_K(x) + tu \in K$. L'égalité obtenue précédemment donne alors

$$2t\mathrm{Re}\langle x-p_K(x), u-p_K(x)\rangle \leq t^2||u-p_K(x)||^2.$$

En simplifiant par t il vient

$$2\mathrm{Re}\langle x-p_K(x), u-p_K(x)\rangle \leq t||u-p_K(x)||^2,$$

et on obtient le résultat voulu en faisant tendre t vers 0. Montrons maintenant que si $y \in K$ est tel que $\forall u \in K, \mathrm{Re}\langle x-y, u-y\rangle \leq 0$, alors $y = p_K(x)$, ce qui achèvera de montrer le deuxième point. Soit alors $z \in K$. Comme $||x-z||^2 = ||x-y||^2 - 2\mathrm{Re}\langle x-y, z-y\rangle + ||z-y||^2$, l'hypothèse faite sur y permet d'affirmer que $||x-y|| \leq ||x-z||$ et donc en passant à l'inf dans cette inégalité et en se souvenant que $||x-y|| \geq d$, l'unicité prouvée au premier point permet d'affirmer que $y = p_K(x)$.

3. Soit $(x_1, x_2) \in H^2$. On a

$$x_1 - x_2 = p_K(x_1) - p_K(x_2) + r$$

où l'on a noté $r = (x_1 - p_K(x_1)) + (x_2 - p_K(x_2))$. Ainsi,

$$||x_1-x_2||^2 = ||p_K(x_1)-p_K(x_2)||^2 + ||r||^2 + 2\mathrm{Re}\langle r, p_K(x_1)-p_K(x_2)\rangle.$$

En notant $a = \langle r, p_K(x_1)-p_K(x_2)\rangle$, il vient

$$a = \langle x_1-p_K(x_1), p_K(x_1)-p_K(x_2)\rangle - \langle x_2-p_K(x_2), p_K(x_1)-p_K(x_2)\rangle.$$

Le deuxième point nous permet d'affirmer que $\langle x_1-p_K(x_1), p_K(x_2)-p_K(x_1)\rangle \leq 0$ et que $\langle x_2-p_K(x_2), p_K(x_1)-p_K(x_2)\rangle \leq 0$, d'où finalement $\mathrm{Re}(a) \geq 0$. Finalement, $||p_K(x_1)-p_K(x_2)|| \leq ||x_1-x_2||$, et on a notre résultat.

□

Application 2. Soit F un sous-espace vectoriel fermé de H différent de $\{0\}$. Alors il existe une projection linéaire continue p_F de H sur F telle que $||p_F|| = 1$. De plus, $\ker p_F = F^\perp$ et $H = F \oplus F^\perp$.

Démonstration. Soit $x \in H$. On écrit $x = p_F(x) + (x - p_F(x))$: il nous faut montrer que $x - p_F(x) \in F^\perp$. Soit $y \in F$. Comme $u := p_F(x) + y \in F$, en appliquant l'inégalité du deuxième point à u on obtient $\mathrm{Re}\langle x - p_F(x), y\rangle \leq 0$. En faisant la même chose avec $-y$, on a finalement $\mathrm{Re}\langle x - p_F(x), y\rangle = 0$. Enfin, en considérant $iy \in F$, on obtient aussi $\mathrm{Im}\langle x - p_F(x), y\rangle = 0$. Bref, $x - p_F(x) \in F^\perp$. Comme $F \cap F^\perp = \{0\}$, on a bien

$$H = F \oplus F^\perp.$$

D'après ce qui précède, la projection orthogonale de H sur F coïncide avec p_F. Enfin, comme p_F vérifie $p_F \circ p_F = p_F$ et que p_F est non-nul (comme on suppose que $F \neq \{0\}$), alors $||p_F|| \geq 1$. Comme de plus on a le théorème de Pythagore qui donne

$$||p_F(x)||^2 = ||x||^2 - ||x - p_F(x)||^2 \leq ||x||^2$$

et donc $||p_F|| \leq 1$, on a bien $||p_F|| = 1$. □

2.13.2 Références

[Mad97], pp. 76-79.

2.13.3 Questions classiques

1.

2.13.4 Remarques

— Il faut faire un dessin dans le plan pour expliquer la caractérisation du second point.

— Dans la pratique, on démontre : l'existence dans le point 1, l'implication dans le point 2, et on donne l'idée dans le point 3. On fait ensuite l'application entièrement. On annonce avant les points que l'on va aborder.

2.14 Prolongement méromorphe de la fonction Γ

2.14.1 Développement

Une proposition admise [11] nous rappelle quelques propriétés de la fonction Γ :

Proposition 17. *Pour $x > 0$ on pose $\Gamma(x) = \int_0^{+\infty} t^{x-1}e^{-t}\,dt$. On a que :*

1. *La fonction Γ est bien définie,*
2. *La fonction Γ est C^∞ sur $]0, +\infty[$,*
3. *La fonction Γ se prolonge en une fonction holomorphe dans l'ouvert $\omega = \{z \in \mathbb{C}\ ;\ \mathrm{Re}(z) > 0\}$,*
4. *Pour tout $z \in \omega$, $\Gamma(z+1) = z\Gamma(z)$ et $\Gamma(n+1) = n!$ pour tout $n \in \mathbb{N}$.*

Le résultat principal est le suivant :

Théorème 27. *La fonction Γ se prolonge en une fonction méromorphe sur $\mathbb{C}$ avec des pôles simples sur $-\mathbb{N}$.*

Remarque 1. La proposition précédente donne déjà un prolongement méromorphe sur $\mathbb{C} \setminus (-\mathbb{N})$: il suffit de poser $\Gamma(z) = \frac{\Gamma(z+1)}{z}$ sur $\{z \in \mathbb{C} \setminus \{0\}\ ;\ \mathrm{Re}(z) > -1\}$, puis $\Gamma(z) = \frac{\Gamma(z+2)}{z(z+1)}$ sur $\{z \in \mathbb{C} \setminus \{-1, 0\}\ ;\ \mathrm{Re}(z) > -2\}$, etc. Les pôles $-\mathbb{N}$ sont simples, via la remarque

$$\Gamma(z) = (z+n)^{-1} \underbrace{\frac{\Gamma(z+n+1)}{z \dots (z+n-1))}}_{\neq 0 \text{ en } -n}.$$

On désire cependant en savoir plus sur le prolongement, en particulier montrer que $\Gamma(z) \neq 0$ pour $z \in \mathbb{C} \setminus (-\mathbb{N})$.

Démonstration. On commence par un lemme dû à Euler :

Lemme 29. *Pour $z \in \omega$, on a*

$$\Gamma(z) = \lim_{n \to +\infty} \frac{n^z\, n!}{z(z+1)\dots(z+n)}.$$

11. Lors des leçons portant sur l'analyse complexe.

Démonstration du lemme. On considère la suite de fonctions

$$f_n(t) = \mathbf{1}_{]0,n[}(t)\Big(1-\frac{t}{n}\Big)^n t^{z-1}.$$

Un développement limité montre que la suite (f_n) converge simplement vers la fonction $f(t) = \mathbf{1}_{]0,+\infty[}e^{-t}t^{z-1}$. D'autre part, l'inégalité $1-u \leq e^{-u}$ pour $0 \leq u \leq 1$ montre que $|f_n(t)| \leq \mathbf{1}_{]0,n[}(t)(e^{-\frac{t}{n}})^n t^{x-1} \leq \mathbf{1}_{]0,+\infty[}(t)t^{x-1}e^{-t}$, où $x = \mathrm{Re}(z) > 0$. Le théorème de convergence dominée assure que

$$\Gamma(z) = \int_0^{+\infty} t^{z-1}e^{-t}\,dt = \lim_{n\to+\infty}\int_0^n t^{z-1}\Big(1-\frac{t}{n}\Big)^n\,dt.$$

Le changement de variables $t = ns$ donne

$$\Gamma(z) = \lim_{n\to+\infty} n^z\int_0^1 s^{z-1}(1-s)^n\,ds =: \lim_{n\to+\infty} n^z I_n(z).$$

Montrons par récurrence [12] sur $n \in \mathbb{N}$ que

$$I_n(z) = \frac{n!}{z(z+1)\dots(z+n)}, \forall z \in \omega.$$

L'initialisation est immédiate. Pour la récurrence, on fait l'intégration par parties suivante :

$$\begin{aligned}
I_{n+1}(z) &= \int_0^1 s^{z-1}(1-s)^{n+1}\,ds \\
&= \underbrace{[\frac{s^z}{z}(1-s)^{n+1}]_0^1}_{=0} + \int_0^1 \frac{s^z}{z}(n+1)(1-s)^n\,ds \\
&= \frac{n+1}{z}I_n(z+1) \\
&= \frac{(n+1)n!}{z(z+1)\dots(z+n+1)} \\
&= \frac{(n+1)!}{z\dots(z+n+1)}.
\end{aligned}$$

Ceci prouve le lemme. □

L'idée est d'étudier l'inverse de la fraction-limite du lemme, et de montrer qu'elle est holomorphe et qu'elle ne s'annule que sur $-\mathbb{N}$: on réalisera

12. Admise lors de l'oral, sinon le développement est trop long.

ainsi Γ comme l'inverse de cette fonction holomorphe, qui sera bien non-nulle. On considère pour cela $z \in \mathbb{C}$ la fonction $G(z) = \lim_{n\to+\infty} \frac{z(z+1)\dots(z+n)}{n^z\, n!} = \lim_{n\to+\infty} \frac{z(z+1)\dots(z+n)}{(n+1)^z\, n!} = \lim_{n\to+\infty} G_n(z)$ (l'avant dernière égalité est là pour nous permettre d'exprimer facilement $G_n(z)$, comme nous allons le voir immédiatement). Montrons que G est bien définie et que c'est une fonction entière, en la réalisant comme un produit infini de fonctions holomorphes : on écrit que $\frac{1}{(n+1)^z} = e^{-z\ln(n+1)} = \prod_{k=1}^{n} e^{z\ln(\frac{k}{k+1})}$ (à la manière d'un téléscopage dans les séries) et $n! = 1 \cdot 2 \dots \cdot n$, et il vient

$$G_n(z) = z\prod_{k=1}^{n}\Big(\frac{z+k}{k}\Big)e^{z\ln\frac{k}{k+1}} = z\prod_{k=1}^{n}\Big(1+\frac{z}{k}\Big)e^{z\ln\frac{k}{k+1}} =: z\prod_{k=1}^{n} f_k(z),$$

où chaque f_k est holomorphe dans $\mathbb{C}$. Montrons que l'on a convergence uniforme sur tout compact : Soit $R > 0$ et $|z| < R$. Pour $n > R$ on écrit

$$G_n(z) = z\prod_{1\le k\le R} f_k(z)\prod_{R<k\le n} f_k(z).$$

Pour $k > R$, on a $\frac{|z|}{k} < 1$ et donc on peut écrire $f_k(z) = e^{\ln(1+\frac{z}{k})-z\ln(1+\frac{1}{k})}$, d'où

$$G_n(z) = z\prod_{1\le k\le R} f_k(z) \times \exp\Big[\sum_{k=\lfloor R\rfloor+1}^{n}\Big(\ln\Big(1+\frac{z}{k}\Big) - z\ln\Big(1+\frac{1}{k}\Big)\Big)\Big].$$

Or $\Big|\ln(1+\frac{z}{k}) - z\ln(1+\frac{1}{k})\Big| \le \frac{C(R)}{k^2}$ pour $k \ge \lfloor R\rfloor + 1$ (à travers un nouveau développement limité, que l'on peut effectuer car $\frac{|z|}{k} < 1$) ; on en déduit que la série de terme général $\ln(1+\frac{z}{k}) - z\ln(1+\frac{1}{k})$ converge uniformément dans $\{|z| < R\}$ vers une fonction holomorphe. Comme la fonction exp est uniformément continue sur $\{|z| < R\}$, on en déduit que la suite (G_n) converge elle aussi uniformément sur $\{|z| < R\}$ vers une fonction holomorphe. Comme R est arbitraire, on a bien prouvé ce que l'on avait annoncé. Le lemme d'Hurwitz affirme que les zéros de G sont 0 et les zéros des f_k, i.e. $-\mathbb{N}$. On en déduit que la fonction $F(z) = \frac{1}{G(z)}$ est holomorphe sans zéros dans $\mathbb{C}\setminus(-\mathbb{N})$, et comme le lemme d'Euler donne que F et Γ coïncident sur ω, F est le prolongement cherché.

□

2.14.2 Références

[QZ13], pp. 312-315.

2.14.3 Questions classiques

1.

2.14.4 Remarques

— Attention, le deuxième "changement de variable" du livre est en fait une intégration par parties (remarquer le dv qui n'est pas un du !).

2.15 Théorèmes d'Abel angulaire et Taubérien faible

2.15.1 Développement

Théorème 28 (Théorème d'Abel angulaire)**.** *Soit $\sum a_n z^n$ une série entière de rayon de convergence ≥ 1 telle que $\sum a_n$ converge* [13]*. On note f la somme de cette série entière sur le disque unité. On fixe $\theta_0 \in [0, \frac{\pi}{2}[$ et on pose*

$$\Delta_{\theta_0} = \{z \in \mathbb{C} \ ; \ |z| < 1 \text{ et } \exists \rho > 0 \text{ tq } \exists \theta \in [-\theta_0, \theta_0] \text{ tq } z = 1 - \rho e^{i\theta}\}.$$

Alors $\lim\limits_{\substack{z \to 1 \\ z \in \Delta_0}} f(z) = \sum_{n=0}^{+\infty} a_n$.

Démonstration. Notons $S_n = \sum_{k=0}^{n} a_k$, $S = \lim_{n\to+\infty} S_n$ et $R_n = S - S_n$. On va majorer $|f(z) - S|$ à l'aide d'une transformation d'Abel en écrivant $a_n = R_{n-1} - R_n$ pour tout n. Soit $z \in \mathbb{C}^*, |z| < 1$. Pour tout $N \in \mathbb{N}^*$, on a

$$\begin{aligned}\Big(\sum_{n=0}^{N} a_n z^n\Big) - S_N &= \sum_{n=1}^{N} (R_{n-1} - R_n)(z^n - 1) = \sum_{n=0}^{N-1} R_n(z^{n+1} - 1) - \sum_{n=1}^{N} R_n(z^n - 1) \\ &= \sum_{n=0}^{N-1} R_n(z^{n+1} - z^n) - R_N(z^N - 1) = (z-1)\sum_{n=0}^{N-1} R_n z^n - R_N(z^N - 1),\end{aligned}$$

et en faisant tendre $N \to +\infty$ on en déduit

$$f(z) - S = (z-1)\sum_{n=0}^{+\infty} R_n z^n.$$

On fixe à présent $\varepsilon > 0$ et $N \in \mathbb{N}$ tel que $|R_n| < \varepsilon$ pour tout $n \geq N$ (possible car $R_n \underset{n\to+\infty}{\longrightarrow} 0$ en tant que reste d'une série convergente). L'égalité précédente donne, pour tout $|z| < 1$,

$$|f(z) - S| \leq |z-1|\Big|\sum_{n=0}^{N} R_n z^n\Big| + \varepsilon|z-1|\Big(\sum_{n=N+1}^{+\infty} |z|^n\Big) \leq |z-1|\Big(\sum_{n=0}^{N} |R_n|\Big) + \varepsilon\frac{|z-1|}{1-|z|}.$$

Soit $z \in \Delta_{\theta_0}$, de sorte que $z = 1 - \rho e^{i\varphi}$ avec $\rho > 0$ et $|\varphi| \leq \theta_0$. On a $|z|^2 = 1 - 2\rho\cos\varphi + \rho^2$, et lorsque $\rho \leq \cos\theta_0$ (on peut minorer ρ comme on le souhaite, car on veut faire tendre z vers 1), on a la majoration

$$\frac{|z-1|}{1-|z|} = \frac{|z-1|}{1-|z|^2}(1+|z|) = \frac{\rho}{2\rho\cos\varphi - \rho^2}(1+|z|) \leq \frac{2}{2\cos\varphi - \rho} \leq \frac{2}{2\cos\theta_0 - \cos\theta_0} = \frac{2}{\cos\theta_0}$$

13. Ce point à lui seul assure que le RCV de $\sum a_n$ est ≥ 1.

où l'on a utilisé que $\cos\theta_0 \leq \cos\varphi$ (faire un dessin). Si on choisit maintenant $\alpha > 0$ tel que $\alpha \sum_{n=0}^{N} |R_n| < \varepsilon$, on a donc pour $z \in \Delta_{\theta_0}$ et $|z-1| \leq \inf(\alpha, \cos\theta_0)$ que

$$|f(z) - S| \leq \varepsilon + \varepsilon \frac{2}{\cos\theta_0}.$$

□

La réciproque à ce théorème n'est pas vraie : on a

$$\lim_{\substack{z\to 1\\ |z|<1}} \sum_{n=0}^{+\infty} (-1)^n z^n = \lim_{\substack{z\to 1\\ |z|<1}} \frac{1}{1+z} = \frac{1}{2},$$

mais $\sum (-1)^n$ diverge. Donnons une réciproque affaiblie :

Théorème 29 (Théorème Taubérien faible)**.** *Soit $\sum a_n z^n$ une série entière de rayon de convergence 1 et f la somme de cette série entière sur le disque unité. On suppose que*

$$\exists S \in \mathbb{C} \text{ tq } \lim_{\substack{x\to 1\\ |x|<1}} f(x) = S \,[14].$$

Si $a_n = o(\frac{1}{n})$, alors $\sum a_n$ converge et $\sum_{n=0}^{+\infty} a_n = S$.

Démonstration. On a

$$\forall n \in \mathbb{N}^*, \forall x \in]0,1[, S_n - f(x) = \sum_{k=1}^{n} a_k(1-x^k) - \sum_{k=n+1}^{+\infty} a_k x^k,$$

et comme $(1-x^k) = (1-x)(1+x+\cdots+x^{k-1}) \leq k(1-x)$ pour $0 < x < 1$, on en déduit

$$|S_n - f(x)| \leq (1-x)\sum_{k=1}^{n} k|a_k| + \sum_{k=n+1}^{+\infty} \frac{k|a_k|}{n} x^k \leq (1-x)Mn + \frac{\sup_{k>n} k|a_k|}{n(1-x)},$$

où M désigne un majorant de la suite $(k|a_k|)$ (qui tend vers 0 par hypothèse). Fixons à présent $\varepsilon \in]0,1[$. L'inégalité précédente entraîne

$$\forall n \in \mathbb{N}^*, \left|S_n - f(1-\frac{\varepsilon}{n})\right| \leq M\varepsilon + \frac{\sup_{k>n} k|a_k|}{\varepsilon},$$

donc en choisissant N_0 tel que $\sup_{k>N_0} k|a_k| < \varepsilon^2$, on en déduit

$$\forall n \geq N_0, \left|S_n - f(1-\frac{\varepsilon}{n})\right| \leq M\varepsilon + \varepsilon = (M+1)\varepsilon.$$

14. Contrairement au théorème d'Abel angulaire, la limite se prend ici le long de l'axe réel.

D'après les hypothèses, $f(x)$ tend vers S lorsque $x \to 1^-$, donc il existe $N_1 \geq N_0$ tel que $|f(1-\frac{\varepsilon}{n}) - S| < \varepsilon$ pour tout $n \geq N_1$. Ainsi,

$$\forall n \geq N_1, |S_n - S| \leq |S_n - f(1-\frac{\varepsilon}{n})| + |f(1-\frac{\varepsilon}{n}) - S| \leq (M+1)\varepsilon + \varepsilon = (M+2)\varepsilon.$$

□

2.15.2 Références

[Gou08], pp. 252-254.

2.15.3 Questions classiques

1. *Dans le théorème d'Abel angulaire, que pouvez vous dire lorsque la série $\sum a_n$ converge absolument* : Le résultat est alors immédiat, via le fait que $\sum a_n z^n$ converge normalement sur $|z| \leq 1$ et est donc continue sur $|z| \leq 1$, en particulier elle l'est en 1.
2. *Que donne le premier théorème appliqué à la série $\sum \frac{(-1)^n}{(2n+1)}$* : Cette série converge d'après le théorème des séries alternées. On a alors

$$\sum_{n=0}^{+\infty} \frac{(-1)^n}{(2n+1)} = \lim_{\substack{x\to 1 \\ x<1}} \sum_{n=0}^{+\infty} \frac{(-1)^n}{(2n+1)} x^n = \lim_{\substack{x\to 1 \\ x<1}} \arctan x = \arctan 1 = \frac{\pi}{4}.$$

2.15.4 Remarques

— Le second résultat reste vrai en supposant seulement $a_n = O(\frac{1}{n})$: c'est le théorème Taubérien fort, aussi appelé théorème d'Hardy-Littlewood.

— Il y a quelques coquilles dans le Gourdon (un n qui se substitue à un N, etc.).

2.16 Théorème de Riesz-Fischer

2.16.1 Développement

Théorème 30 (Théorème de Riesz-Fischer)**.** *Soit $(\Omega, \mathcal{A}, \mu)$ un espace mesuré. Alors pour $1 \leq p \leq \infty$, $\mathrm{L}^p(\Omega, \mathcal{A}, \mu) = \mathrm{L}^p$ est un espace de Banach.*

Démonstration. 1. **Étape 1 : le cas** $p = \infty$. Soit (f_n) une suite de Cauchy dans L^∞. On a donc

$$\forall k \in \mathbb{N}^*, \exists N_k \in \mathbb{N} \text{ tq } \forall m, n \geq N_k, ||f_n - f_m||_{\mathrm{L}^\infty} \leq \frac{1}{k}.$$

Il existe alors une famille d'ensembles négligeables E_k (dépendants aussi de m et de n : en réalité on pose $E_k = \cup_{m,n \geq N_k} E_{k,m,n}$, qui reste négligeable en tant qu'union dénombrable d'ensembles négligeables) tels que

$$\forall k \in \mathbb{N}^*, \exists N_k \in \mathbb{N} \text{ tq } \forall m, n \geq N_k, \forall x \in \Omega \setminus E_k, |f_n(x) - f_m(x)| \leq \frac{1}{k}.$$

Si l'on pose $E = \cup_{k \in \mathbb{N}^*} E_k$, qui est (lui aussi) négligeable en tant qu'union dénombrable d'ensembles négligeables, on a finalement que pour tout $x \in \Omega \setminus E$, la suite $(f_n(x))$ est de Cauchy dans $\mathbb{C}$. Or, $\mathbb{C}$ étant complet, ces suites convergent : on note $f(x)$ leurs limites. Il nous reste à montrer que f ainsi définie est bien dans L^∞ et qu'elle est limite de la suite (f_n) pour la norme infinie. Passant à la limite en m dans l'assertion précédente, on obtient

$$\forall k \in \mathbb{N}^*, \exists N_k \in \mathbb{N} \text{ tq } \forall n \geq N_k, \forall x \in \Omega \setminus E, |f_n(x) - f(x)| \leq \frac{1}{k}.$$

En particulier on a que $f_{N_1} - f \in \mathrm{L}^\infty$ et donc $f = f_{N_1} - (f_{N_1} - f) \in \mathrm{L}^\infty$, et

$$\forall k \in \mathbb{N}^*, \exists N_k \in \mathbb{N} \text{ tq } \forall n \geq N_k, ||f_n - f||_{\mathrm{L}^\infty} \leq \frac{1}{k},$$

i.e. $||f_n - f||_{\mathrm{L}^\infty} \underset{n \to +\infty}{\longrightarrow} 0$, ce qui prouve le premier point.

2. **Étape 2 : le cas** $1 \leq p < \infty$. Soit (f_n) une suite de Cauchy dans L^p. Pour conclure il suffit de montrer qu'une sous-suite extraite converge dans L^p : une suite de Cauchy admettant une sous-suite convergente étant convergente, on aura notre résultat. Commençons par extraire une sous-suite f_{n_k} telle que

$$\forall k \in \mathbb{N}, ||f_{n_{k+1}} - f_{n_k}||_{\mathrm{L}^p} \leq \frac{1}{2^k},$$

de la manière suivante : on choisit n_0 tel que $\forall m, n \geq n_0, ||f_m - f_n||_{\mathrm{L}^p} \leq 1$, puis $n_1 \geq n_0$ tel que $\forall m, n \geq n_1, ||f_m - f_n||_{\mathrm{L}^p} \leq \frac{1}{2}$, etc. Montrons que (f_{n_k}), que l'on note encore (f_n) pour alléger les notations, est convergente dans L^p. Posons

$$g_n = \sum_{k=0}^{n} |f_{k+1} - f_k|.$$

Les g_n ainsi définies sont dans L^p en tant que somme de fonctions L^p ($f \in \mathrm{L}^p \iff |f| \in \mathrm{L}^p$), et on a de plus par l'inégalité de Minkowski que

$$||g_n||_{\mathrm{L}^p} \leq \sum_{k=0}^{n} ||f_{k+1} - f_k||_{\mathrm{L}^p} \leq \sum_{k=0}^{+\infty} \frac{1}{2^k} = 2.$$

En remarquant ensuite que g_n converge simplement sur Ω vers une certaine fonction g (en tant que limite de série de terme général positif, éventuellement infinie) et que pour tout $m \leq n, 0 \leq g_m \leq g_n$ et donc $|g_m|^p \leq |g_n|^p$, le théorème de convergence monotone assure que

$$\int_\Omega |g|^p \, d\mu = \lim_{n \to +\infty} \int_\Omega |g_n|^p \, d\mu = \lim_{n \to +\infty} ||g_n||_{\mathrm{L}^p}^p \leq 2^p.$$

Comme on sait qu'alors g est finie p.p. [15], on note E l'ensemble négligeable sur lequel elle atteint la valeur $+\infty$. On a pour $1 \leq m \leq n$ que

$$\begin{aligned} \forall x \in \Omega \setminus E, |f_n(x) - f_m(x)| &\leq |f_n(x) - f_{n-1}(x)| + \cdots + |f_{m+1}(x) - f_m(x)| \\ &\leq \underbrace{g(x) - g_{m-1}(x)}_{:= R_{m-1}(x)}, \end{aligned}$$

et il en résulte que sur $\Omega \setminus E$, $(f_n(x))$ est de Cauchy et converge vers une limite $f(x)$. Comme on a pour tout $x \in \Omega \setminus E$ que $|f(x) - f_m(x)| \leq g(x)$ par positivité de $g_{m-1}(x)$ et en passant à la limite en n, et qu'alors $|f(x) - f_m(x)|^p \leq g^p(x)$, on a d'une part que $f - f_m \in \mathrm{L}^p$ pour $m \geq 1$ et donc $f = f_1 - (f - f_1) \in \mathrm{L}^p$, et d'autre part le théorème de convergence dominée qui assure que $||f_n - f||_{\mathrm{L}^p} \underset{n \to +\infty}{\longrightarrow} 0$.

□

2.16.2 Références

[Bre05], pp. 57-58.

15. Rappelons la convention : pour $0 < p < +\infty, (+\infty)^p = +\infty$.

2.16.3 Questions classiques

1. *Comment montrez-vous l'inégalité de Minkowski* : Il s'agit de faire un travail préliminaire pour se restreindre au cas où f et g sont positives, puis que leurs intégrales sont finies. Ensuite, on écrit $(f+g)^p = f(f+g)^{p-1} + g(f+g)^{p-1}$, puis on applique l'inégalité de Hölder à chacun de termes (en considérant q le conjugué de p), puis on conclut.

2.16.4 Remarques

— On utilise dans ce développement le fait que les L^p sont des espaces vectoriels, il ne faut pas oublier de le préciser à l'oral (en citant l'inégalité de Minkowski et la convexité de $t \mapsto t^p$ pour $p \geq 1$).

— Les deux étapes consistent à considérer une suite de fonctions (f_n) dans L^p (en fait une suite de classes d'équivalences de fonctions !), et à s'intéresser à une suite de représentants de chacune de ces classes (en l'occurence les f_n, par abus de notation), à obtenir de l'information sur ces f_n, et à voir enfin comment on peut retransmettre cette information en repassant au quotient. En fait, on fait considère la suite de représentants immédiatement après avoir introduit chacune de nos deux suites de Cauchy.

— Attention, la preuve du livre demande quelques clarifications ! Notamment de détailler l'utilisation du théorème de convergence monotone dans l'étape 2, et de définir l'ensemble E dans l'étape 2 : comme on utilise une fonction $g : \Omega \to [0, +\infty]$, on ne peut a priori pas parler de $g - g_n$ sans arriver à des expressions de la forme $+\infty - 1$ qui ne sont pas définies (et si jamais ça l'était, on aurait $g(x) - g_n(x) = +\infty - g_n(x) = +\infty \longrightarrow_{n\to+\infty} +\infty$, et la suite $(f_n(x))$ ne serait pas a priori de Cauchy). De même, si jamais on s'arrête un cran avant la dernière inégalité pour écrire que $|f_n(x) - f_m(x)| \leq |g_{n-1}(x) - g_{m-1}(x)|$ et que $(f_n(x))$ est de Cauchy car $(g_n(x))$ l'est, c'est oublier de dire que dans $[0, +\infty]$ on considère la distance $d(x, y) = |\arctan(y) - \arctan(x)|$. La seule manière de procéder est de réaliser g comme une la somme d'une série dans $\mathbb{C}$ pour pouvoir utiliser la bonne distance (convergent dans $([0, +\infty[, |\arctan(\cdot) - \arctan(\cdot)|)$ équivaut à convergent dans $([0, +\infty[, |\cdot - \cdot|)$), quitte à devoir se priver d'un ensemble négligeable. Enfin, pour finir d'insister sur ce point, en ne faisant pas attention aux remarques précédentes, on serait parvenus à extraire de (f_n) une sous-suite convergent non pas presque partout, mais partout, et ce résultat est faux.

— On réserve le symbole $||f||_{\mathrm{L}^p}$ aux $f \in \mathrm{L}^p$, sinon on note $\left(\int_\Omega |f|^p \, d\mu\right)^{\frac{1}{p}}$.

— Frigyes Riesz : mathématicien hongrois, 1880-1956
— Ernst Fischer : mathématicien autrichien, 1875-1954

2.17 Théorème des extrema liés

2.17.1 Développement

Théorème 31. *Soient U un ouvert de $\mathbb{R}^n$, $f, g_1, \dots, g_k \in C^1(U, \mathbb{R})$,*

$$M = \{x \in U \ ; \ g_1(x) = \cdots = g_k(x) = 0\},$$

et $m \in M$. Si $f|_M$ présente un extremum local en m et si les formes linéaires $dg_1(m), \dots, dg_k(m)$ sont linéairement indépendantes, alors il existe un unique $k-$uplet $(\lambda_1, \dots, \lambda_k) \in \mathbb{R}^k$ tel que

$$df(m) = \sum_{i=1}^{k} \lambda_i dg_i(m).$$

Démonstration. Avec les notations et hypothèses du théorème, M est une sous-variété de $\mathbb{R}^n$ en m. On sait alors que l'espace tangent T_mM est égal à l'intersection $\cap_{i=1}^k \ker dg_i(m)$. Soit $v \in T_mM$. Il existe un intervalle I ouvert contenant 0 et $\gamma : I \to \mathbb{R}^n$ dérivable telle que $\gamma(I) \subset M, \gamma(0) = m$ et $\gamma'(0) = v$. Par hypothèse, $f \circ \gamma$ admet un extremum en 0, i.e. [16]

$$0 = (f \circ \gamma)'(0) = df(\gamma(0))(\gamma'(0)) = df(m)(v).$$

On a donc

$$\bigcap_{i=1}^{k} \ker dg_i(m) \subset \ker df(m).$$

Par ailleurs, on note $b_1, \dots, b_k$ les formes linéaires $dg_1(m), \dots, dg_k(m)$. On peut compléter la famille $(b_1, \dots, b_k)$ en une base $(b_1, \dots, b_n)$ du dual $(\mathbb{R}^n)^*$. Soit $(e_1, \dots, e_n)$ sa base antéduale. Il existe un unique $n-$uplet $(\lambda_1, \dots, \lambda_n) \in \mathbb{R}^n$ tel que $df(m) = \sum_{i=1}^n \lambda_i b_i$. On a pour tout $i \in \{1, \dots, k\}$ et $j \in \{k+1, \dots, n\}$ que $dg_i(m)(e_j) = b_i(e_j) = 0$, et d'après l'inclusion entre noyaux précédemment établie on a que

$$\forall j \in \{k+1, \dots, n\}, 0 = df(m)(e_j) = \sum_{i=1}^{n} \lambda_i b_i(e_j) = \lambda_j,$$

d'où

$$df(m) = \sum_{i=1}^{k} \lambda_i dg_i(m).$$

□

16. On rappelle l'identification classique entre $\gamma'(0) = d\gamma(0)(1)$ et $d\gamma(0)$.

Application 3 (Théorème spectral)**.** Soit E un espace euclidien et soit $u \in \mathcal{L}(E)$ un endomorphisme symétrique. Alors u est diagonalisable en base orthonormée.

Démonstration. On démontre le résultat par récurrence sur la dimension n de E.

1. Initialisation : Si $n = 1$, il n'y a rien à démontrer.
2. Hérédité : On suppose que la propriété est vérifiée pour tout espace de dimension n. Soit E un espace euclidien de dimension $n+1$ est soit $u \in \mathcal{L}(E)$ un endomorphisme symétrique. Les applications

$$f : \begin{array}{ccc} E & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \langle u(x), x\rangle \end{array} \quad \text{et} \quad g : \begin{array}{ccc} E & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \langle x, x\rangle - 1 \end{array}$$

sont de classe C^1 sur E. De plus, la sphère unité de E $S = g^{-1}(\{0\})$ est compacte car E est de dimension finie : f est donc bornée et atteint son maximum sur S, en un point noté e_1. Pour tout $x \in E$, $df(x)$ et $dg(x)$ sont les applications

$$df(x) : h \mapsto 2\langle u(x), h\rangle \quad \text{et} \quad dg(x) : h \mapsto 2\langle x, h\rangle,$$

où l'on a utilisé la symétrie de u pour simplifier $df(x)$. D'après le théorème des extrema liés[17], il existe $\lambda_1 \in \mathbb{R}$ tel que $df(e_1) = \lambda_1 dg(e_1)$. On a donc : $\forall h \in E, 2\langle u(e_1), h\rangle = 2\lambda_1\langle e_1, h\rangle$. Donc $u(e_1) = \lambda_1 e_1$. En particulier, la droite vectorielle engendrée par u est stable par u donc, puisque u est symétrique, $\text{vect}(e_1)^\perp$ est aussi stable par u. Ainsi, $u|_{\text{vect}(e_1)^\perp}$ est un endomorphisme symétrique sur un espace euclidien de dimension n. En concaténant e_1 et la base $(e_2, \ldots, e_n)$ fournie par l'hypothèse de récurrence, on a montré le théorème.

□

2.17.2 Références

[Ave91], pp. 102-104.

2.17.3 Questions classiques

1. *Comment calculez vous la base antéduale* : Étant données des bases $\mathcal{C}, \mathcal{C}^*$ et $\mathcal{B}^*$, on sait que ${}^t[{}^t\text{id}]_{\mathcal{C}^*\mathcal{B}^*} = [\text{id}]_{\mathcal{B}\mathcal{C}}$. En s'aidant alors de la base canonique et de la base canonique duale, il suffit de calculer la matrice $[{}^t\text{id}]_{\mathcal{C}^*\mathcal{B}^*}$, de la transposer, puis enfin de l'inverser ; les vecteurs colones de la matrice obtenue sont ceux de la matrice $[\text{id}]_{\mathcal{C}\mathcal{B}}$, i.e. les vecteurs de $\mathcal{B}$.

17. Que l'on peut appliquer car $dg(x)$ est nul si et seulement si $x = 0$, et ici $||e_1|| = 1$.

2.17.4 Remarques

—

2.18 Inégalité de Hoeffding

2.18.1 Développement

Théorème 32. *Soit $(X_n)_{n\in\mathbb{N}^*}$ une suite de variables aléatoires réelles indépendantes. Supposons qu'il existe deux suites de réels $(a_n))_{n\in\mathbb{N}^*}$ et $(b_n))_{n\in\mathbb{N}^*}$ telles que, pour tout $n \geq 1$, $a_n < b_n$ et*

$$\mathbb{P}(a_n \leq X_n \leq b_n) = 1.$$

Posons $S_n = X_1 + \cdots + X_n$. On a alors pour tout $x > 0$ et tout $n \geq 1$:

$$\mathbb{P}(|S_n - \mathbb{E}(S_n)| > x) \leq 2\exp\Big(-\frac{2x^2}{\sum_{i=1}^n (b_i - a_i)^2}\Big).$$

On commence par démontrer le lemme suivant :

Lemme 30. *Soit Y une variable aléatoire réelle bornée, centrée et telle qu'il existe deux réels a et b tels que $a < b$ et $\mathbb{P}(a \leq Y \leq b) = 1$. Alors pour tout réel $t > 0$, on a*

$$\mathbb{E}(e^{tY}) \leq \exp\Big((b-a)^2\frac{t^2}{8}\Big).$$

Démonstration du lemme. Comme la fonction $x \mapsto e^{tx}$ est convexe, on voit que lorsqu'on a $a \leq Y \leq b$, alors

$$e^{tY} \leq \frac{b-Y}{b-a}e^{ta} + \frac{Y-a}{b-a}e^{tb}$$ [18].

Comme on sait que $\mathbb{P}(a \leq Y \leq b) = 1$ [19] et que $\mathbb{E}(Y) = 0$, l'inégalité précédente nous donne, en prenant l'espérance :

$$\mathbb{E}(e^{tY}) \leq \frac{b}{b-a}e^{ta} - \frac{a}{b-a}e^{tb}.$$

On pose alors $u = t(b-a)$ et on applique la formule de Taylor-Lagrange à la fonction

$$\psi(u) = \ln\Big(\frac{b}{b-a}e^{ta} + \frac{-a}{b-a}e^{tb}\Big) = \frac{a}{b-a}u + \ln\Big(\frac{a}{b-a}(1-e^u)\Big),$$

en remarquant que $\psi(0) = \psi'(0) = 0$ et

$$\psi''(u) = -\frac{a}{b-a}e^u\frac{1+\frac{a}{b-a}}{(1+\frac{a}{b-a}(1-e^u))^2}.$$

18. C'est la corde qui joint (a, e^{ta}) à (b, e^{tb}).
19. Et que donc intégrer sur Ω, c'est intégrer sur $\{a \leq Y \leq b\}$.

Comme $\psi''(u)$ est de la forme $\frac{\alpha\beta}{(\alpha+\beta)^2}$, le seconde identité remarquable assure que $|\psi''(u)| \leq \frac{1}{4}$. Ainsi, par la formule de Taylor-Lagrange, il existe un réel $0 \leq s \leq u$ tel que

$$\psi(u) = \psi(0) + \psi'(0)u + \psi''(s)\frac{u^2}{2} \leq \frac{(b-a)^2}{8}t^2.$$

□

Prouvons maintenant l'inégalité de Hoeffding :

Démonstration du théorème. Posons, pour tout $i \in \{1, \ldots, n\}$, $Y_i = X_i - \mathbb{E}(X_i)$, $\alpha_i = a_i - \mathbb{E}(X_i)$ et $\beta_i = b_i - \mathbb{E}(X_i)$. On remarque que $\mathbb{P}(\alpha_i \leq Y_i \leq \beta_i) = 1$ et $S_n - \mathbb{E}(S_n) = Y_1 + \cdots + Y_n$. De plus, comme les variables X_i sont indépendantes, il en des de même pour les Y_i. Par l'inégalité de Markov, on a donc pour tout $x \geq 0$ et pour tout $u > 0$

$$\mathbb{P}(S_n - \mathbb{E}(S_n) \geq x) \leq \mathbb{E}(e^{u(S_n - \mathbb{E}(S_n))})e^{-ux} = \mathbb{E}(e^{u(Y_1+\cdots+Y_n)})e^{-ux} = e^{-ux}\prod_{i=1}^{n}\mathbb{E}(e^{uY_i}).$$

On obtient alors grâce au lemme précédent appliqué à Y_i, en remarquant que $\beta_i - \alpha_i = b_i - a_i$, que

$$\mathbb{P}(S_n - \mathbb{E}(S_n) \geq x) \leq \exp\Big(-ux + \frac{u^2}{8}\sum_{i=1}^{n}(b_i - a_i)^2\Big).$$

Cette inégalité étant vraie pour tout u [20], choisissons celui qui minimise la borne de droite en cherchant celui qui annule la dérivée de ce polynôme de degré 2 : on trouve

$$u = \frac{4x}{\sum_{i=1}^{n}(b_i - a_i)^2},$$

ce qui montre que

$$\mathbb{P}(S_n - \mathbb{E}(S_n) \geq x) \leq \exp\Big(-\frac{2x^2}{\sum_{i=1}^{n}(b_i - a_i)^2}\Big).$$

En remplaçant X_i par $-X_i$ dans ce qui précède, on obtient l'inégalité similaire

$$\mathbb{P}(S_n - \mathbb{E}(S_n) \leq -x) \leq \exp\Big(-\frac{2x^2}{\sum_{i=1}^{n}(b_i - a_i)^2}\Big).$$

L'inégalité cherchée est donc une conséquence directe de ces deux derniers résultats. □

20. Si $u \leq 0$, on est en train de considérer l'exponentielle d'une quantité positive, et donc plus grande que 1.

Exemple 1. Supposons que $(X_1, \dots, X_n)$ soit un vecteur aléatoire composé de variables indépendantes de même loi de Bernoulli $\mathcal{B}(p)$, avec $0 < p < 1$. La variable S_n suit alors une loi binomiale $\mathcal{B}(n, p)$. L'inégalité de Bienaymé-Tchebychev donne

$$\mathbb{P}(|S_n - \mathbb{E}(S_n)| \geq x) \leq \frac{np(1-p)}{x^2},$$

alors que l'inégalité de Hoeffding donne

$$\mathbb{P}(|S_n - \mathbb{E}(S_n)| \geq x) \leq 2\exp\Big(-\frac{2}{n}x^2\Big).$$

La précision est nettement plus importante pour x grand dans le second cas.

2.18.2 Références

[GK11], pp. 346-348.

2.18.3 Questions classiques

1.

2.18.4 Remarques

— Wassily Hoeffding : mathématicien américain, 1914-1991

2.19 Théorème de Sarkovski

2.19.1 Développement

Théorème 33. *Soit I un segment de $\mathbb{R}$ et $f : I \to I$ une application continue. Si $x \in I$ vérifie $f^n(x) = x$ et $f^k(x) \neq x$ pour $k \in \{1, \dots, n-1\}$, on dit que x est un point $n-$périodique. Montrer que s'il existe un point $3-$périodique, alors il existe un point $n-$périodique pour tout $n \in \mathbb{N}^*$.*

On commence par démontrer le lemme suivant :

Lemme 31. *Si K est un segment inclus dans $f(I)$, il existe un segment L inclus dans I tel que $K = f(L)$.*

Démonstration du lemme. [21] Posons $K = [\alpha, \beta]$. Comme $K \subset f(I)$, il existe $(a, b) \in I^2$ tel que $\alpha = f(a)$ et $\beta = f(b)$. Si $\alpha = \beta$, alors $K = \{\alpha\}$ et le singleton $L = \{a\}$ convient. On suppose désormais $\alpha \neq \beta$ et donc $a \neq b$.

1. Supposons $a < b$. L'idée est de prendre dans $[a, b]$ un antécédent u de α et un antécédent v de β, tels qu'entre u et v il n'y ait plus d'autre antécédent de α ni de β. Considérons $A = \{x \in [a, b] \ ; \ f(x) = \beta\}$. C'est un fermé non-vide et minoré par a. Prenons v le plus petit élément de A. On a $f(v) = \beta$ et $f(t) < \beta$ pour tout $t \in [a, v[$ en vertu du théorème des valeurs intermédiaires (car $f(a) = \alpha < \beta$). On fait le même raisonnement avec $B = \{x \in [a, v] \ ; \ f(x) = \alpha\}$ en considérant son plus grand élément u, et le segment $L = [u, v]$ répond à la question.
2. Le cas $b < a$ se traite de la même manière.

□

On démontre un second et dernier lemme :

Lemme 32. *On suppose qu'il existe n segments $I_0, I_1, \dots, I_{n-1}$ inclus dans I tels que $I_0 \subset f(I_{n-1})$ et $I_{k+1} \subset f(I_k)$ pour $k \in \{0, \dots, n-2\}$. Alors f^n a un point fixe x_0 tel que $f^k(x_0) \in I_k$ pour tout $k \in \{0, \dots, n-1\}$.*

Démonstration du lemme. 1. Si $n = 1$, on dispose par hypothèse d'un segment $I_0 = [a, b]$ tel que $I_0 \subset f(I_0)$. En particulier, il existe α et β dans I_0 tels que $f(\alpha) = a$ et $f(\beta) = b$. La fonction $g(x) = f(x) - x$ prend alors des valeurs de signes opposés en α et β et, comme elle est continue, s'annule par le théorème des valeurs intermédiaires. On en déduit l'existence d'un point fixe pour f dans l'intervalle I_0.

21. Un dessin suffit à l'oral.

2. Si $n = 2$, on a $I_0 \subset f(I_1)$ et $I_1 \subset f(I_0)$. En particulier, $I_0 \subset f(I_1) \subset f^2(I_0)$. Par le cas $n = 1$, le fait que $I_0 \subset f^2(I_0)$ implique l'existence d'un point fixe $x_0 \in I_0$ pour f^2. Mais *a priori* il n'y a pas de raison que $f(x_0)$ appartienne à I_1 (on a seulement l'inclusion $I_1 \subset f(I_0)$). On va raffiner un petit peu le choix du point fixe. D'après le lemme précédent, il existe un segment $J_1 \subset I_0$ tel que $f(J_1) = I_1$. On a alors $J_1 \subset I_0 \subset f(I_1) = f^2(J_1)$. Le même argument que précédemment assure l'existence d'un point fixe x_0 de f^2 dans J_1. Et celui-ci vérifie bien que $f(x_0) \in I_1$.
3. Dans le cas général, on applique la même démarche. Comme on a $I_1 \subset f(I_0)$, on peut choisir un segment $J_1 \subset I_0$ tel que $f(J_1) = I_1$. On a alors $I_2 \subset f(I_1) = f^2(J_1)$. On choisit $J_2 \subset J_1$ tel que $f^2(J_2) = I_2$. Et de proche en proche, on construit ainsi une suite finie de segments $J_{n-1} \subset \cdots \subset J_2 \subset J_1 \subset J_0$ telle que $f^k(J_k) = I_k$ pour tout $k \in \{1, \ldots, n-1\}$. On a enfin $I_0 \subset f(I_{n-1}) = f^n(J_{n-1})$ de sorte qu'il existe un $J_n \subset J_{n-1}$ tel que $f^n(J_n) = I_0$. Comme $J_n \subset f^n(J_n)$, f^n admet un point fixe x_0 dans J_n. Par construction des intervalles J_k, $f^k(x_0) \in I_k$ pour tout $k \in \{0, \ldots, n-1\}$.

□

Prouvons finalement le théorème :

Démonstration du théorème. Simplifions les notations en écrivant $I_1 \to I_2$ si jamais $I_1 \subset f(I_2)$. Le lemme précédent affirme donc que si $I_0 \to I_{n-1} \to \cdots \to I_1 \to I_0$, f^n admet un point fixe x_0 dans I_0 vérifiant $f^k(x_0) \in I_k$ pour tout $k \in \{0, \ldots, n-1\}$. Par hypothèse, f admet un point $3-$périodique a. Posons $b = f(a)$ et $c = f(b) = f^2(a)$. Les points b et c sont aussi $3-$périodiques, et quitte à remplacer a par b ou c, on peut supposer que que $a = \min(a, b, c)$. Deux éventualités se présentent selon les dispositions de b et c :

1. Si $a < b < c$, on pose $I_0 = [a, b]$ et $I_1 = [b, c]$. Comme $f(a) = b$ et $f(b) = c$, on a $I_1 \subset f(I_0)$, i.e. $I_1 \to I_0$. De la même manière, on a aussi $I_0 \to I_1$ et $I_1 \to I_1$. Cette dernière inclusion montre déjà que f admet un point fixe dans I_1. De même, le cycle $I_0 \to I_1 \to I_0$ montre que f^2 admet un point fixe x_0 dans I_0 tel que $f(x_0) \in I_1$. Comme x_0 ne peut pas être égal à b[22], $x_0 \notin I_1$ et $f(x_0) \neq x_0$. Ainsi, x_0 est un point 2-périodique. Soit maintenant $n \geq 4$. On écrit le cycle $I_0 \to I_1 \to I_1 \to \cdots \to I_1 \to I_0$, où l'intervalle I_1 figure $n-1$ fois. D'après le lemme précédent, f^n admet un point fixe x dans I_0 tel que $f^k(x) \in I_1$ pour $k < n$. Comme précédemment, x ne peut être égal à b et est donc un point $n-$périodique.
2. Si $a < c < b$, on pose $I_0 = [a, c]$ et $I_1 = [c, b]$. On a cette fois $I_1 \to I_0$, $I_0 \to I_0$ et $I_0 \to I_1$. On reprend l'idée précédente en changeant I_0 et I_1.

22. Auquel cas b ne serait pas $3-$périodique.

Dans tous les cas, f admet des points $n-$périodiques pour tout $n \geq 1$. □

2.19.2 Références

[FGN14c], pp. 92-94.

2.19.3 Questions classiques

1. *Donnez un exemple de fonction qui admette un point* $2-$*périodique mais aucun point* $n-$*périodique pour* $n \geq 3$: On peut penser à la fonction $f : x \mapsto 1 - x$ sur $I = [0, 1]$, en remarquant que $f^2 = \mathrm{id}_I$.

2.19.4 Remarques

— Le premier lemme sert à localiser plus précisément le point fixe que l'on souhaite exhiber dans le second lemme.

— Oleksandr Sarkovski : mathématicien ukrainien, 1936

2.20 Équation de la chaleur

2.20.1 Développement

Considérons une barre métallique. Connaissant, en tout point initial, la température en chaque point de la barre, et à tout instant, la température aux deux extrémités, peut-on déterminer, à tout moment et en tout point, la température de la barre ? Après modélisation, le problème prend la forme suivante : la barre est représentée par le segment $[0, L]$, on note $Q =]0, L[\times]0, +\infty[$, et il faut trouver une fonction $u \in C^0(\overline{Q}) \cap C^\infty(Q)$ telle que

$$\begin{cases} \frac{\partial u}{\partial t} - \frac{\partial^2 u}{\partial x^2} = 0 \text{ dans } Q \\ u(0,t) = u(L,t) = 0, t \in [0, +\infty[\\ u(x,0) = h(x), x \in [0, L] \end{cases}$$

où h est une fonction C^1 sur $]0, L[$, C^0 sur $[0, L]$ telle que $h(0) = h(L) = 0$.

Théorème 34. *Le problème précédent admet une solution.*

Démonstration. L'idée de départ est de chercher une solution de la forme $u(x,t) = f(x)g(t)$. Le problème se change en $f(x)g'(t) = f''(x)g(t)$. Cherchons une solution telle que $f(x) \neq 0$ pour tout $x \in]0, L[$ et $g(t) \neq 0$ pour tout $t \in]0, +\infty[$. L'égalité précédente équivaut alors à

$$\frac{f''(x)}{f(x)} = \frac{g'(t)}{g(t)} \forall x \in]0, L[, \forall t \in]0, +\infty[.$$

Ceci ne peut être satisfait que si les deux membres sont constants, i.e. s'il existe $\lambda \in \mathbb{R}$ tel que

$$f''(x) = \lambda f(x), \forall x \in]0, L[, g'(t) = \lambda g(t), \forall t \in]0, +\infty[.$$

Si $\lambda > 0$, la solution de la première équation différentielle est une fonction de la forme $f(x) = Ae^{\sqrt{\lambda}x} + Be^{-\sqrt{\lambda}x}$. Les conditions aux extrémités donnent $A + B = 0$ et $Ae^{\sqrt{\lambda}L} + Be^{-\sqrt{\lambda}L} = 0$, d'où $A = B = u(x,t) = 0$, ce qui ne respecte par la condition initiale dès que $h \not\equiv 0$. De même si $\lambda = 0$, on a $f(x) = Ax + B$ et à nouveau $u \equiv 0$. Prenons $\lambda = -\xi^2 < 0$, alors $f(x) = A\cos(\xi x) + B\sin(\xi x)$ et $g(t) = Ce^{-\xi^2 t}$. Les conditions aux extrémités donnent $A = 0$ et $B\sin(\xi L) = 0$, d'où $\xi = \frac{n\pi}{L}, n \in \mathbb{Z}$. On a donc une famille de solutions de la forme $u_n(x,t) = b_n \sin(\frac{n\pi}{L}x)e^{-\frac{n^2\pi^2}{L^2}t}$. Le problème est que ces solutions n'ont aucune raison de

vérifier la condition initiale. Cependant, l'équation de la chaleur étant linéaire, une somme de telles u_n est encore une solution. L'idée est de poser

$$u(x,t) = \sum_{n=1}^{+\infty} b_n \sin\left(\frac{n\pi}{L}x\right) e^{-\frac{n^2\pi^2}{L^2}t}.$$

Si on peut dériver u sous le signe somme, elle reste solution de l'équation car chaque u_n l'est déjà. La condition aux extrémités est elle aussi satisfaite : qu'a-t-on gagné en introduisant cet objet ? De cette manière, la condition initiale se reformule en $h(x) = \sum_{n=1}^{+\infty} b_n \sin(\frac{n\pi}{L}x)$. Cette égalité traduit le fait que les b_n doivent être les coefficients de Fourier d'une fonction impaire $\tilde{h}$ égale à h sur $[0, L]$. Continuons dans cette voie : soit h_1 la fonction définie par $h_1(x) = h(x)$ si $x \in [0, L]$ et $h_1(x) = -h(-x)$ si $x \in [-L, 0]$. Comme $h(0) = 0$, la fonction h_1 est de classe C^1 sur $]-L, L[$. Soit $\tilde{h}$ la fonction $2L-$périodique sur $\mathbb{R}$, égale à h_1 sur $[-L, L]$. Comme $h(L) = 0$, la fonction $\tilde{h}$ est continue sur $\mathbb{R}$ et C^1 par morceaux. Sous ces conditions, la série de Fourier de $\tilde{h}$ converge absolument vers $\tilde{h}$ en tout point de $\mathbb{R}$. Comme $\tilde{h}$ est impaire, on a

$$\tilde{h}(x) = \sum_{n=1}^{+\infty} b_n \sin\left(\frac{n\pi}{L}x\right), \forall x \in \mathbb{R},$$

$$\sum_{n=1}^{+\infty} |b_n| < +\infty, b_n = \frac{2}{L}\int_0^L h(x) \sin\left(\frac{n\pi}{L}x\right) dx.$$

Cette précédente égalité assure que la fonction u définie sur $\overline{Q}$ par

$$u(x,t) = \sum_{n=1}^{+\infty} b_n \sin\left(\frac{n\pi}{L}x\right) e^{-\frac{n^2\pi^2}{L^2}t}$$

est continue sur Q. Montrons qu'elle est C^∞ et qu'on peut dériver sous le signe somme. Pour cela il suffit de montrer que les séries dérivées convergent uniformément sur tout compact de Q. Si $t \in [\varepsilon, M]$, $\varepsilon > 0$, le terme général d'une série dérivée d'ordre k est est majoré en valeur absolue par $C_k|b_n|n^{2k}e^{-\frac{n^2\pi^2}{L^2}\varepsilon}$ qui est le terme général d'une série convergente. Il y a donc convergence normale, ce qui montre que $u \in C^\infty(Q)$. On a montré l'existence d'une solution. □

2.20.2 Références

[QZ13], pp. 105-109.

2.20.3 Questions classiques

1. Y a-t-il unicité de la solution : Oui, on la prouve avec la proposition suivante :

   Proposition 18 (Principe du maximum pour l'équation de la chaleur)**.** *Soit* $u \in C^0(\overline{Q}) \cap C^2(Q)$, *telle que* $Pu(x,t) \geq 0$ *sur* Q, *où* $P = \frac{\partial^2}{\partial x^2} - \frac{\partial}{\partial t}$; *soit* $T > 0$ *et* $K = [0,L] \times [0,T]$. *Alors* $\sup_K u = \sup_{K \cap \partial Q} u$.

   Démonstration. Soit $\varepsilon > 0$ et $u_\varepsilon(x,t) = u(x,t) + \varepsilon x^2$, qui vérifie $Pu_\varepsilon = Pu + 2\varepsilon \geq 2\varepsilon$ sur Q ; soit $m_\varepsilon = (x_\varepsilon, t_\varepsilon)$ un point de K où u_ε atteint son maximum sur K. Supposons que $m_\varepsilon \notin K \cap \partial Q$: alors

   $$0 < x_\varepsilon < L, \text{ donc } \frac{\partial u_\varepsilon}{\partial x}(m_\varepsilon) = 0 \text{ et } \frac{\partial^2 u_\varepsilon}{\partial x^2} \leq 0,$$

   $$0 < t_\varepsilon \leq T, \text{ donc } \frac{\partial u_\varepsilon}{\partial t}(m_\varepsilon) = \lim_{h \overset{>}{\to} 0} \frac{u_\varepsilon(x_\varepsilon, t_\varepsilon - h) - u_\varepsilon(x_\varepsilon, t_\varepsilon)}{-h} \geq 0.$$

   Il résulte de ces deux points que $Pu_\varepsilon(m_\varepsilon) \leq 0$, ce qui contredit $Pu_\varepsilon \geq 2\varepsilon$. Donc $m_\varepsilon \in K \cap \partial Q$, et $\sup_K \leq \sup_K u_\varepsilon = \sup_{K \cap \partial Q} u_\varepsilon \leq \sup_{K \cap \partial Q} u + \varepsilon L^2$; faisant tendre ε vers 0, on établit la proposition. □

   L'unicité découle alors du fait que, si u et v sont deux solutions, on pose $w = v - u$: w est solution de l'équation de la chaleur, et de plus

   $$w(x,t) = 0, \forall (x,t) \in \partial Q.$$

   Fixons $T > 0$; puisque $Pw = 0$ sur Q, le principe du maximum pour l'équation de la chaleur entraîne que $w(x,T) \leq 0$. Puisque $P(-w) = 0$ sur Q, on a de même $-w(x,T) \leq 0$. Finalement, $w(x,T) = 0$, et comme T est arbitraire, $w \equiv 0$ dans Q.

2.20.4 Remarques

—

2.21 Formule sommatoire de Poisson

2.21.1 Développement

Théorème 35. *Soit $F \in \mathcal{S}$. Alors on a la relation*

$$\sum_{n\in\mathbb{Z}} F(n) = \sum_{n\in\mathbb{Z}} \hat{F}(n),$$

où l'on a noté $\hat{F}(\xi) = \int_{\mathbb{R}} e^{-2i\pi xt} F(t)\,dt$ la transformée de Fourier de F.

Démonstration. On introduit la fonction $f(x) = \sum_{n\in\mathbb{Z}} F(x+n)$. On va justifier cette notation en montrant que cette série converge normalement sur tout compact de $\mathbb{R}$. En effet, si $A > 0$ et $|x| \leq A$, on a que

$$|n| \geq 2A \Longrightarrow |x+n| \geq |n| - |x| \geq |n| - A \geq \frac{|n|}{2}.$$

Comme $F \in \mathcal{S}$, on a d'autre part l'existence d'une constante M telle que $(1+|y|)^2|F(y)| \leq M$ pour tout $y \in \mathbb{R}$, et ainsi

$$|F(x+n)| \leq M\Big(1+\frac{|n|}{2}\Big)^{-2},$$

qui est le terme général d'une série normalement convergente. Comme F est continue, f l'est aussi. De plus, le changement d'indice $p = n+1$ montre que $f(x+1) = \sum_{n\in\mathbb{Z}} F(x+n+1) = \sum_{p\in\mathbb{Z}} F(x+p) = f(x)$. La fonction f est donc $1-$périodique, calculons son coefficient de Fourier d'indice m :

$$c_m(f) = \int_0^1 f(t)e^{-2i\pi mt}\,dt = \int_0^1 \sum_{n\in\mathbb{Z}} F(t+n)e^{-2i\pi mt}\,dt \quad = \sum_{n\in\mathbb{Z}} \int_0^1 F(t+n)e^{-2i\pi mt}\,dt$$

- l'interversion des deux signes étant justifiée par la convergence normale de $\sum_{n\in\mathbb{Z}} F(t+n)$ sur $[0,1]$ et par le fait que $|e^{-2i\pi mt}| = 1$ -

$$= \sum_{n\in\mathbb{Z}} \int_0^1 F(t+n)e^{-2i\pi m(t+n)}\,dt$$

- justifié cette fois-ci par le fait que $e^{-2i\pi mn} = 1$... -

$$= \sum_{n\in\mathbb{Z}} \int_n^{n+1} F(u)e^{-2i\pi mu}\,du = \int_{\mathbb{R}} F(u)e^{-2i\pi mu}\,du = \hat{F}(m).$$

Comme $F \in C^1$, le théorème de Dirichlet assure enfin que

$$f(x) = \sum_{m\in\mathbb{Z}} c_m(f)e^{2i\pi mx} = \sum_{m\in\mathbb{Z}} \hat{F}(m)e^{2i\pi mx},$$

soit encore

$$\sum_{n\in\mathbb{Z}} F(x+n) = \sum_{m\in\mathbb{Z}} \hat{F}(m)e^{2i\pi mx}.$$

En faisant $x = 0$ dans cette égalité, on obtient le résultat voulu. □

Corollaire 6. *Dans $\mathcal{S}'$, on a $\delta_{\mathbb{Z}} = \hat{\delta}_{\mathbb{Z}}$.*

Démonstration. Vérifions que ces sommes sont bien définies. Si $\varphi \in \mathcal{S}$, on a vu que $\sum_{n\in\mathbb{Z}} \varphi(n)$ était bien définie. Par conséquent, $\langle \delta_{\mathbb{Z}}, \varphi\rangle := \sum_{k\in\mathbb{Z}} \varphi(k)$ est bien définie. Vérifions à présent que $\delta_{\mathbb{Z}} \in \mathcal{S}'$, i.e. que $\delta_{\mathbb{Z}} : \mathcal{S} \longrightarrow \mathbb{C}$ est linéaire continue. Ici, on a

$$\begin{aligned}
|\langle \delta_{\mathbb{Z}}, \varphi\rangle| &\leq \sum_{n\in\mathbb{Z}} |\varphi(n)| \leq \sum_{n\in\mathbb{Z}^*} \frac{1}{n^2}|n^2\varphi(n)| + |\varphi(0)| \\
&\leq \underbrace{\sum_{n\in\mathbb{Z}^*} \frac{1}{n^2}}_{=2\cdot\frac{\pi^2}{6}} N_{2,0}(\varphi) + N_{0,0}(\varphi) \\
&\leq \frac{\pi^2}{3} \max_{0\leq\alpha,\beta\leq 2} N_{\alpha,\beta}(\varphi).
\end{aligned}$$

Ainsi, $\delta_{\mathbb{Z}}$ est bien une distribution tempérée et on peut calculer sa transformée de Fourier. On obtient :

$$\begin{aligned}
\langle \hat{\delta}_{\mathbb{Z}}, \varphi\rangle &= \langle \delta_{\mathbb{Z}}, \hat{\varphi}\rangle \\
&= \sum_{n\in\mathbb{Z}} \hat{\varphi}(n) \\
&= \sum_{n\in\mathbb{Z}} \varphi(n) \\
&= \langle \delta_{\mathbb{Z}}, \varphi\rangle.
\end{aligned}$$

Finalement, $\delta_{\mathbb{Z}} = \hat{\delta}_{\mathbb{Z}}$. □

2.21.2 Références

[QZ13], pp. 96-97.

2.21.3 Questions classiques

1.

2.21.4 Remarques

— Les hypothèses sous lesquelles on prouve le théorème peuvent être affaiblies.

— Il faut retenir par coeur le corollaire.

— Siméon Poisson : mathématicien, géomètre et physicien français, 1781-1840

2.22 Formule d'inversion de Fourier dans $\mathcal{S}$

2.22.1 Développement

Pour établir la formule d'inversion de Fourier, on aura besoin d'effectuer le calcul suivant :

Lemme 33. *Soit $\varepsilon > 0$ fixé et soit $g : t \mapsto e^{-\varepsilon t^2}$. On a que $\hat{g}(x) = \frac{\sqrt{\pi}}{\sqrt{\varepsilon}} e^{-\frac{x^2}{4\varepsilon}}$.*

Démonstration. On a $\hat{g}(x) = \int_{\mathbb{R}} e^{-itx} e^{-\varepsilon t^2}\, dt$. La fonction $(x,t) \mapsto e^{-itx}e^{-\varepsilon t^2}$ est C^1 en sa première variable, intégrable selon sa seconde et sa dérivée en x $(x,t) \mapsto -ite^{-itx}e^{-\varepsilon t^2}$ est dominée uniformément en t par $(x,t) \mapsto |t|e^{-\varepsilon t^2}$, qui est intégrable. Par théorème de dérivabilité sous le signe somme, on a que

$$\hat{g}'(x) = -i\int_{\mathbb{R}} te^{-itx}e^{-\varepsilon t^2}\, dt = \frac{i}{2\varepsilon}\int_{\mathbb{R}} e^{-itx}\frac{d}{dt}(e^{-\varepsilon t^2})\, dt = -\frac{i}{2\varepsilon}\int_{\mathbb{R}} \frac{d}{dt}(e^{-itx})e^{-\varepsilon t^2}\, dt,$$

cette dernière égalité étant obtenue par intégration par parties (le crochet s'annule bien), puis

$$\hat{g}'(x) = -\frac{x}{2\varepsilon}\int_{\mathbb{R}} e^{-itx}e^{-\varepsilon t^2}\, dt = -\frac{x}{2\varepsilon}\hat{g}(x).$$

Par facteur intégrant, $\hat{g}(x) = \hat{g}(0)e^{-\frac{x^2}{4\varepsilon}}$, et comme

$$\hat{g}(0) = \int_{\mathbb{R}} e^{-\varepsilon t^2}\, dt = \frac{1}{\sqrt{\varepsilon}}\int_{\mathbb{R}} e^{-t^2}\, dt = \frac{\sqrt{\pi}}{\sqrt{\varepsilon}}$$

par un changement de variables clair, on obtient pour finir $\hat{g}(x) = \frac{\sqrt{\pi}}{\sqrt{\varepsilon}} e^{-\frac{x^2}{4\varepsilon}}$. □

Prouvons à présent la formule :

Proposition 19 (Formule d'inversion de Fourier)**.** *Soit $f \in \mathcal{S}$. Alors, pour tout $x \in \mathbb{R}$,*

$$f(x) = \frac{1}{2\pi}\int_{\mathbb{R}} e^{itx}\hat{f}(t)\, dt.$$

Démonstration. Soit $\varepsilon > 0$. Par application du théorème de convergence dominée, on a

$$\frac{1}{2\pi}\int_{\mathbb{R}} e^{itx}\hat{f}(t)\, dt = \frac{1}{2\pi}\lim_{\varepsilon\to 0}\int_{\mathbb{R}} e^{itx}e^{-\varepsilon t^2}\hat{f}(t)\, dt.$$

La convergence ponctuelle est simple à vérifier et la condition de domination uniforme en ε est donnée par $|e^{itx}e^{-\varepsilon t^2}\hat{f}(t)| \leq |\hat{f}(t)| \in \mathcal{S} \subset \mathrm{L}^1$. Alors

$$\frac{1}{2\pi}\int_{\mathbb{R}} e^{itx-\varepsilon t^2}\hat{f}(t)\, dt = \frac{1}{2\pi}\int_{\mathbb{R}} e^{itx-\varepsilon t^2}\Big(\int_{\mathbb{R}} e^{-ity}f(y)\, dy\Big)\, dt.$$

D'après le théorème de Tonelli, la fonction $e^{itx-\varepsilon t^2}e^{ity}f(y)$ est dans L^1 pour la mesure produit puisque

$$\int_{\mathbb{R}}\Big(\int_{\mathbb{R}}|e^{it(x-y)}e^{-\varepsilon t^2}f(y)|\,dy\Big)\,dt=\int_{\mathbb{R}}e^{-\varepsilon t^2}\,dt\int_{\mathbb{R}}|f(y)|\,dy<+\infty.$$

Par le théorème de Fubini, on peut intervertir les intégrales et on obtient

$$\frac{1}{2\pi}\int_{\mathbb{R}}e^{itx-\varepsilon t^2}\hat{f}(t)\,dt=\frac{1}{2\pi}\int_{\mathbb{R}}f(y)\Big(\int_{\mathbb{R}}e^{-it(y-x)}e^{-\varepsilon t^2}\,dt\Big)\,dy=\frac{\sqrt{\pi}}{2\pi\sqrt{\varepsilon}}\int_{\mathbb{R}}f(y)e^{-\frac{(y-x)^2}{4\varepsilon}}\,dy,$$

où l'on a utilisé le lemme. Par le changement de variables $y=x+2\sqrt{\varepsilon}u$, on obtient

$$\frac{1}{2\pi}\int_{\mathbb{R}}e^{itx-\varepsilon t}\hat{f}(t)\,dt=\frac{1}{\sqrt{\pi}}\int_{\mathbb{R}}e^{-u^2}f(x+2\sqrt{\varepsilon}u)\,du.$$

Il ne reste plus qu'à appliquer le théorème de convergence dominée[23] pour conclure :

$$\frac{1}{2\pi}\lim_{\varepsilon\to 0}\int_{\mathbb{R}}e^{itx-\varepsilon t^2}\hat{f}(t)\,dt=\frac{1}{\sqrt{\pi}}\int_{\mathbb{R}}e^{-u^2}\,du\cdot f(x)=f(x).$$

□

2.22.2 Références

[QZ13], pp. 329-331.

2.22.3 Questions classiques

1. *Comment calculez-vous l'intégrale de Gauss* : En l'élevant au carré, puis en utilisant le théorème de Fubini et le passage en coordonnées polaires.
2. *Comment montrez-vous que la transformée de Fourier envoie l'espace de Schwartz dans l'espace de Schwartz* : La régularité se montre par théorème de régularité sous le signe somme, et par intégration par parties pour la décroissance rapide.
3. *Comment établissez-vous la formule dans* L^1 *lorsque* $\hat{f}$ *reste un élément de* L^1 : Toujours à l'aide du calcul de la transformée de Fourier de la gaussienne, et avec une approximation de l'identité pour pouvoir réutiliser ce que l'on vient de prouver.

23. La fonction f est dans $\mathcal{S}$, elle est donc bornée.

2.22.4 Remarques

— Le lemme laisse suggérer pourquoi la transformée de Fourier envoie $\mathcal{S}$ dans $\mathcal{S}$.

— L'idée de la preuve est de perturber notre fonction à l'aide d'une gaussienne pour pouvoir utiliser le théorème de Fubini et avancer dans le calcul.

— Le lemme n'est pas présent dans le livre, mais il est simple à retenir.

Chapitre 3

Leçons d'Algèbre

3.1 101 : Groupe opérant sur un ensemble. Exemples et applications.

- Théorème de Wedderburn ($\rightarrow$ action par conjugaison)
- Le cube et les représentations de $\mathfrak{S}_4$ ($\rightarrow$ représentations)

3.2 102 : Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications.

- Théorème de Wedderburn ($\rightarrow$ sous-groupe $\mathbb{U}_n$, polynômes cyclotomiques)
- Théorème de Kronecker ($\rightarrow$ polynômes cyclotomiques)

3.3 103 : Exemples de sous-groupes distingués et de groupes quotients. Applications.

- Groupe des K-automorphismes de $K(X)$ ($\rightarrow \mathrm{PGL}_2(K)$)
- Le cube et les représentations de $\mathfrak{S}_4$ ($\rightarrow$ caractères, sous-groupes distingués)
- (L'hexagone et les représentations de D_6)

3.4 104 : Groupes finis. Exemples et applications.

- Théorème de Burnside ($\rightarrow$ ordre et exposant)
- Le cube et les représentations de $\mathfrak{S}_4$ ($\rightarrow$ caractères, sous-groupes distingués)

3.5 105 : Groupe des permutations d'un ensemble fini. Applications.

- Automorphismes de $\mathfrak{S}_n$ ($\rightarrow$ structure de $\mathfrak{S}_n$)
- Le cube et les représentations de $\mathfrak{S}_4$ ($\rightarrow$ caractères, sous-groupes distingués)

3.6 106 : Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $\mathrm{GL}(E)$. Applications.

- Générateurs de $\mathrm{GL}_n(K)$ et de $\mathrm{SL}_n(K)$ ($\rightarrow$ générateurs de $\mathrm{GL}(E)$ et de $\mathrm{SL}(E)$)
- Théorème de Burnside ($\rightarrow$ sous-groupes finis de $\mathrm{GL}_n(\mathbb{C})$)

3.7 107 : Représentations et caractères d'un groupe fini sur un $\mathbb{C}$-espace vectoriel.

- Le cube et les représentations de $\mathfrak{S}_4$ ($\rightarrow$ caractères d'un groupe symétrique)
- L'hexagone et les représentations de D_6 ($\rightarrow$ caractères d'un groupe diédral)

3.8 108 : Exemples de parties génératrices d'un groupe. Applications.

- Générateurs de $\mathrm{GL}_n(K)$ et de $\mathrm{SL}_n(K)$ ($\rightarrow$ générateurs de $\mathrm{GL}(E)$ et de $\mathrm{SL}(E)$)
- Automorphismes de $\mathfrak{S}_n$ ($\rightarrow$ générateurs du groupe symétrique)

3.9 109 : Exemples et représentations de groupes finis de petit cardinal.

- Le cube et les représentations de $\mathfrak{S}_4$ ($\to$ caractères d'un groupe symétrique)
- L'hexagone et les représentations de D_6 ($\to$ caractères d'un groupe diédral)

3.10 110 : Caractère d'un groupe abélien fini et transformée de FOURIER discrète. Applications.

IMPASSE

3.11 120 : Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.

- Théorème des deux carrés ($\to$ carrés de $\mathbb{F}_p$)
- Loi de réciprocité quadratique ($\to$ carrés de $\mathbb{F}_p$)

3.12 121 : Nombres premiers. Applications.

- Dénombrement des polynômes irréductibles sur $\mathbb{F}_q$ ($\to$ fonction de Möbius)
- Théorème des deux carrés ($\to$ carrés de $\mathbb{F}_q$)

3.13 122 : Anneaux principaux. Exemples et applications.

- Un anneau principal non-euclidien ($\to$ principal $\not\Rightarrow$ euclidien)
- Théorème des deux carrés ($\to$ anneau $\mathbb{Z}[i\sqrt{d}]$)

3.14 123 : Corps finis. Applications.

- Théorème des deux carrés ($\to$ carrés de $\mathbb{F}_q$)
- Dénombrement des polynômes irréductibles sur $\mathbb{F}_q$ ($\to$ polynômes de $\mathbb{F}_q$)

3.15 124 : Anneau des séries formelles. Applications.

- Partitions d'un entier en parts fixées ($\to$ liens entre $K[[X]]$ et $K(X)$)
- SEUL DÉVELOPPEMENT

3.16 125 : Extensions de corps. Exemples et applications.

- Théorème de l'élément primitif ($\to$ corps de décomposition)
- Dénombrement des polynômes irréductibles sur $\mathbb{F}_q$ ($\to$ application à l'irréductibilité des polynômes)

3.17 126 : Exemples d'équations diophantiennes.

- Partitions d'un entier en parts fixées ($\to$ équation de degré 1)
- Théorème des deux carrés ($\to$ équation de degré 2)

3.18 127 : Droite projective et birapport.

- Groupe des K-automorphismes de $K(X)$ ($\to \mathrm{PGL}_2(K)$)
- SEUL DÉVELOPPEMENT

3.19 140 : Corps des fractions rationnelles à une indéterminée sur un corps commutatif. Applications.

- Partitions d'un entier en parts fixées ($\to$ décomposition en éléments simples)
- Groupe des K-automorphismes de $K(X)$ ($\to$ K-automorphismes de $K(X)$)

3.20 141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

- Théorème de l'élément primitif ($\to$ corps de décomposition)

- Dénombrement des polynômes irréductibles sur $\mathbb{F}_q$ ($\rightarrow$ corps de décomposition)

3.21 142 : Algèbre des polynômes à plusieurs indéterminées. Applications.

- Théorème de Kronecker ($\rightarrow$ polynômes symétriques)
- Groupe des K-automorphismes de $K(X)$ ($\rightarrow$ polynôme à deux indéterminées)

3.22 143 : Résultant. Applications.

- Théorème de Kronecker ($\rightarrow$ formule du résultant par les racines)
- SEUL DÉVELOPPEMENT

3.23 144 : Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.

- Dénombrement des polynômes irréductibles sur $\mathbb{F}_q$ ($\rightarrow$ corps de décomposition)
- Théorème de Kronecker ($\rightarrow$ polynômes symétriques)

3.24 150 : Exemples d'actions de groupes sur les espaces de matrices.

- Générateurs de $\mathrm{GL}_n(K)$ et de $\mathrm{SL}_n(K)$ ($\rightarrow$ pivot de Gauss)
- Topologie des orbites de l'action de Steinitz ($\rightarrow$ action de Steinitz)

3.25 151 : Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.

- Réduction des endomorphismes normaux ($\rightarrow$ récurrence sur la dimension)

- Théorème de Wedderburn (→ degré et corps finis)

3.26 152 : Déterminant. Exemples et applications.

- Théorème de Burnside (→ Vandermonde, polynôme caractéristique)
- Ellipsoïde de John-Loewner (→ changement de variables, log-concavité sur $S_n^{++}(\mathbb{R})$)

3.27 153 : Polynômes d'endomorphisme en dimension finie. Applications à la réduction d'un endomorphisme en dimension finie.

- Réduction des endomorphismes normaux (→ stabilité de $\mathrm{Im}\,(P(u))$ et $\ker\,(P(u))$ par u)
- Décomposition de Dunford (→ lemme des noyaux)

3.28 154 : Sous-espaces stables par un endomorphisme ou une famille d'endomorphismes d'un espace vectoriel en dimension finie. Applications.

- Décomposition de Dunford (→ trigonalisation améliorée)
- Réduction des endomorphismes normaux (→ F stable par $u \implies F^\perp$ stable par u^*)
- (Le cube et les représentations de $\mathfrak{S}_4$)

3.29 155 : Endomorphismes diagonalisables en dimension finie.

- Réduction des endomorphismes normaux (→ diagonalisabilité par bloc, matrice symétrique réelle $\implies$ diagonalisable)
- Décomposition de Dunford (→ $u = d + n$ avec d diagonalisable)

3.30 156 : Exponentielle de matrices. Applications.

- Décomposition de Dunford ($\rightarrow$ lemme du théorème de Liapounov)
- Théorème de Cartan-von Neumann ($\rightarrow$ sous-groupes à un paramètre de $\mathrm{GL}_n(\mathbb{R})$)

3.31 157 : Endomorphismes trigonalisables. Endomorphismes nilpotents.

- Décomposition de Dunford ($\rightarrow$ trigonalisation améliorée)
- Théorème de Burnside ($\rightarrow$ caractérisation des endomorphismes nilpotents en caractéristique nulle)

3.32 158 : Matrices symétriques réelles, matrices hermitiennes.

- Ellipsoïde de John-Loewner ($\rightarrow$ corrolaire du théorème spectral)
- Réduction des endomorphismes normaux ($\rightarrow$ extension du résultat aux endomorphismes remarquables)

3.33 159 : Formes linéaires et dualité en dimension finie. Exemples et applications.

- Générateurs de $\mathrm{GL}_n(K)$ et de $\mathrm{SL}_n(K)$ ($\rightarrow$ obtention d'équations d'hyperplans)
- Théorème des extrema liés ($\rightarrow$ formes linéaires en analyse)

3.34 160 : Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie).

- Réduction des endomorphismes normaux ($\rightarrow$ réduction des endomorphismes remarquables)
- Points extrémaux de la boule unité de $\mathcal{L}(E)$ ($\rightarrow$ étude de $O(E)$)

3.35 161 : Isométries d'un espace affine euclidien de dimension finie. Applications en dimensions 2 et 3.

- Points extrémaux de la boule unité de $\mathcal{L}(E)$ ($\rightarrow$ étude de $O(E)$)
- Le cube et les représentations de $\mathfrak{S}_4$ ($\rightarrow$ utilisation du groupe des isométries directes conservant le cube)

3.36 162 : Systèmes d'équations linéaires, opérations élémentaires, aspects algorithmiques et conséquences théoriques.

- Générateurs de $\mathrm{GL}_n(K)$ et de $\mathrm{SL}_n(K)$ ($\rightarrow$ pivot de Gauss)
- Méthode du gradient à pas optimal ($\rightarrow$ résoudre un système revient à minimiser une fonction elliptique)

3.37 170 : Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.

- Ellipsoïde de John-Loewner ($\rightarrow$ ellipses, pseudo-réduction simultanée)
- Lemme de Morse ($\rightarrow$ information à l'ordre deux en analyse)

3.38 171 : Formes quadratiques réelles. Exemples et applications.

- Ellipsoïde de John-Loewner ($\rightarrow$ ellipses, pseudo-réduction simultanée)
- Lemme de Morse ($\rightarrow$ information à l'ordre deux en analyse)

3.39 180 : Coniques. Applications.

- Ellipsoïde de John-Loewner ($\rightarrow$ ellipses)
- SEUL DÉVELOPPEMENT

3.40 181 : Barycentres dans un espace affine réel de dimension finie, convexité. Applications.

- Ellipsoïde de John-Loewner ($\rightarrow$ convexité)
- Points extrémaux de la boule unité de $\mathcal{L}(E)$ ($\rightarrow$ points extrémaux)

3.41 182 : Applications des nombres complexes à la géométrie. Homographies.

- Groupe des K-automorphismes de $K(X)$ ($\rightarrow$ homographies)
- L'hexagone et les représentations de D_6 ($\rightarrow$ angles)

3.42 183 : Utilisation des groupes en géométrie.

- Le cube et les représentations de $\mathfrak{S}_4$ ($\rightarrow \mathfrak{S}_4 \simeq \mathrm{Isom}^+(\text{cube})$)
- L'hexagone et les représentations de D_6 ($\rightarrow$ groupe des nombres complexes)

3.43 190 : Méthodes combinatoires, problèmes de dénombrements.

- Partitions d'un entier en parts fixées ($\rightarrow$ dénombrement des solutions d'une équation diophantienne)
- Dénombrement des polynômes irréductibles sur $\mathbb{F}_q$ ($\rightarrow$ dénombrement des polynômes irréductibles sur $\mathbb{F}_q$)

Chapitre 4

Leçons d'Analyse

4.1 201 : Espaces de fonctions : exemples et applications.

- Théorème d'approximation de Weierstrass par les polynômes de Bernstein ($\rightarrow$ densité dans $(C^0([a,b]), ||\cdot||_\infty)$)
- Théorème de Riesz-Fischer ($\rightarrow$ complétude)

4.2 202 : Exemples de parties denses et applications.

- Théorème d'approximation de Weierstrass par les polynômes de Bernstein ($\rightarrow$ densité dans $(C^0([a,b]), ||\cdot||_\infty)$)
- Densité des polynômes orthogonaux ($\rightarrow$ base hilbertienne)

4.3 203 : Utilisation de la notion de compacité.

- Théorème de Cauchy-Lipschitz global ($\rightarrow$ exhaustion compacte)
- Ellipsoïde de John-Loewner ($\rightarrow$ optimisation)

4.4 204 : Connexité. Exemples et applications.

- Théorème de Sarkovski ($\rightarrow$ théorème des valeurs intermédiaires)
- Théorème de Cauchy-Lipschitz global ($\rightarrow$ dérivées et connexité)

4.5 205 : Espaces complets. Exemples et applications.

- Théorème de Riesz-Fischer (→ preuve de complétude)
- Théorème de Cauchy-Lipschitz global (→ utilisation de la complétude)

4.6 206 : Théorèmes de point fixe. Exemples et applications.

- Théorème de Cauchy-Lipschitz global (→ application du théorème point fixe)
- Méthode de Newton (→ fabriquer une application contractante)

4.7 207 : Prolongement de fonctions. Exemples et applications.

- Densité des polynômes orthogonaux (→ analyticité)
- Théorèmes d'Abel angulaire et Taubérien faible (→ comportement au bord du disque)
- (Prolongement méromorphe de la fonction Γ)

4.8 208 : Espaces vectoriels normés, applications linéaires continues. Exemples.

- Théorème de Riesz-Fischer (→ Banach)
- Densité des polynômes orthogonaux (→ Hilbert, base hilbertienne)

4.9 209 : Approximation d'une fonction par des polynômes et des polynômes trigonométriques. Exemples et applications.

- Densité des polynômes orthogonaux (→ fonctions régulières)
- Théorème d'approximation de Weierstrass par les polynômes de Bernstein (→ moyenne quadratique)

4.10 213 : Espaces de HILBERT. Bases hilbertiennes. Exemples et applications.

- Théorème de projection dans un espace de Hilbert (→ projection)
- Densité des polynômes orthogonaux (→ base hilbertienne)

4.11 214 : Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications.

- Lemme de Morse (→ théorème d'inversion locale)
- Théorème de Cartan-von Neumann (→ sous-variétés)

4.12 215 : Applications différentiables définies sur un ouvert de $\mathbb{R}^n$. Exemples et applications.

- Lemme de Morse (→ théorème d'inversion locale)
- Théorème de Cartan-von Neumann (→ sous-variétés)

4.13 217 : Sous variétés de $\mathbb{R}^n$. Exemples.

- Théorème des extrema liés (→ espace tangent)
- Théorème de Cartan-von Neumann (→ sous-variétés dans les espaces de matrices)

4.14 218 : Applications des formules de TAYLOR.

- Théorème central limite (→ Taylor-Young)
- Lemme de Morse (→ Taylor avec reste intégral)

4.15 219 : Extremums : existence, caractérisation, recherche. Exemples et applications.

- Ellipsoïde de John-Loewner (→ compacité et convexité)
- Méthode du gradient à pas optimal (→ optimisation)

4.16 220 : Équations différentielles $X' = f(t, X)$. Exemples d'étude des solutions en dimension 1 et 2.

- Théorème de Cauchy-Lipschitz global ($\rightarrow$ existence et unicité des solutions)
- Théorème de Liapounov ($\rightarrow$ stabilité et linéarisé)

4.17 221 : Équations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications.

- Théorème de Cauchy-Lipschitz global ($\rightarrow$ existence et unicité des solutions)
- Théorème de Liapounov ($\rightarrow$ stabilité et linéarisé)

4.18 222 : Exemples d'équations aux dérivées partielles linéaires.

- Équation de la chaleur ($\rightarrow$ chaleur)
- SEUL DÉVELOPPEMENT

4.19 223 : Suites numériques. Convergence, valeurs d'adhérence. Exemples et applications.

- Méthode de Newton ($\rightarrow$ suite récurrente)
- Partitions d'un entier en parts fixées ($\rightarrow$ série génératrice)

4.20 224 : Exemples de développements asymptotiques de suites et de fonctions.

- Développement asymptotique de la série harmonique ($\rightarrow$ développement asymptotique)
- Partitions d'un entier en parts fixées ($\rightarrow$ dénombrement)

4.21 226 : Suites vectorielles et réelles définies par une relation de récurrence $u_{n+1} = f(u_n)$. Exemples et applications.

- Théorème de Sarkovski ($\to$ points fixes périodiques)
- Méthode du gradient à pas optimal ($\to$ optimisation)

4.22 228 : Continuité et dérivabilité des fonctions réelles d'une variable réelle. Exemples et contre-exemples.

- Une fonction continue, nulle part dérivable ($\to$ continue $\not\Rightarrow$ dérivable)
- Théorème d'approximation de Weierstrass par les polynômes de Bernstein ($\to$ convergence uniforme)

4.23 229 : Fonctions monotones. Fonctions convexes. Exemples et applications.

- Ellipsoïde de John-Loewner ($\to$ extrema et convexité)
- Méthode du gradient à pas optimal ($\to$ optimisation)

4.24 230 : Séries de nombres réels ou complexes. Comportement des restes ou des sommes partielles des séries numériques. Exemples.

- Développement asymptotique de la série harmonique ($\to$ développement asymptotique)
- Théorèmes d'Abel angulaire et Taubérien faible ($\to$ comportement au bord du disque)

4.25 232 : Méthodes d'approximation des solutions d'une équation $F(X) = 0$. Exemples.

- Méthode de Newton ($\to$ recherche de points critiques)

- Méthode du gradient à pas optimal (→ optimisation)

4.26 233 : Analyse numérique matricielle : résolution approchée de systèmes linéaires, recherche de vecteurs propres, exemples.

- Méthode du gradient à pas optimal (→ système linéaire, matrice symétrique définie positive)
- SEUL DÉVELOPPEMENT

4.27 234 : Espaces $L^p, 1 \leq p \leq +\infty$.

- Théorème de Riesz-Fischer (→ L^p est complet)
- Densité des polynômes orthogonaux (→ transformée de Fourier)

4.28 235 : Problèmes d'interversion de limites et d'intégrales.

- Théorèmes d'Abel angulaire et Taubérien faible (→ comportement au bord du disque)
- Prolongement méromorphe de la fonction Γ (→ méromorphie)

4.29 236 : Illustrer par des exemples quelques méthodes de calcul d'intégrales de fonctions d'une ou plusieurs variables réelles.

- Formule d'inversion de Fourier dans $\mathcal{S}$ (→ nombreuses méthodes utilisées)
- Prolongement méromorphe de la fonction Γ (→ nombreuses méthodes utilisées)

4.30 239 : Fonction définies par une intégrale dépendant d'un paramètre. Exemples et applications.

- Densité des polynômes orthogonaux (→ transformée de Fourier)
- Prolongement méromorphe de la fonction Γ (→ méromorphie)

4.31 240 : Produit de convolution, transformation de FOURIER. Applications.

- Densité des polynômes orthogonaux (→ injectivité de la transformée de Fourier)
- Formule sommatoire de Poisson (→ application aux distributions tempérées)

4.32 241 : Suites et séries de fonctions. Exemples et contre-exemples.

- Théorèmes d'Abel angulaire et Taubérien faible (→ comportement au bord du disque de convergence d'une série entière)
- Formule sommatoire de Poisson (→ série de Fourier)

4.33 243 : Convergence des séries entières, propriétés de la somme. Exemples et applications.

- Théorèmes d'Abel angulaire et Taubérien faible (→ comportement au bord du disque de convergence d'une série entière)
- Partitions d'un entier en parts fixées (→ série génératrice)

4.34 244 : Fonctions développables en série entière, fonctions analytiques. Exemples.

- Théorèmes d'Abel angulaire et Taubérien faible (→ comportement au bord du disque de convergence d'une série entière)
- Partitions d'un entier en parts fixées (→ série génératrice)

4.35 245 : Fonctions holomorphes sur un ouvert de $\mathbb{C}$. Exemples et applications.

- Densité des polynômes orthogonaux ($\rightarrow$ holomorphie sous le signe $\int$)
- Prolongement méromorphe de la fonction Γ ($\rightarrow$ méromorphie)

4.36 246 : Séries de FOURIER. Exemples et applications.

- Équation de la chaleur ($\rightarrow$ exemple historique)
- Formule sommatoire de Poisson ($\rightarrow$ application aux distributions tempérées)

4.37 247 : Exemples de problèmes d'interversion de limites.

- Théorèmes d'Abel angulaire et Taubérien faible ($\rightarrow$ comportement au bord du disque)
- Prolongement méromorphe de la fonction Γ ($\rightarrow$ holomorphie sous le signe $\int$)

4.38 249 : Suites de variables de BERNOULLI indépendantes.

- Marche aléatoire sur $\mathbb{Z}$ ($\rightarrow$ marche aléatoire)
- Inégalité de Hoeffding ($\rightarrow$ inégalité améliorée)

4.39 253 : Utilisation de la notion de convexité en analyse.

- Ellipsoïde de John-Loewner ($\rightarrow$ exitence et convexité)
- Méthode du gradient à pas optimal ($\rightarrow$ optimisation)

4.40 254 : Espaces de SCHWARTZ $\mathcal{S}(\mathbb{R}^d)$ et distributions tempérées. Transformation de FOURIER dans $\mathcal{S}(\mathbb{R}^d)$ et $\mathcal{S}'(\mathbb{R}^d)$.

- Formule d'inversion de Fourier dans $\mathcal{S}$ ($\rightarrow$ transformée de Fourier dans $\mathcal{S}$)
- Formule sommatoire de Poisson ($\rightarrow$ transformée de Fourier dans $\mathcal{S}$ et $\mathcal{S}'$)

4.41 260 : Espérance, variance et moments d'une variable aléatoire.

- Théorème central limite ($\rightarrow$ moments et fonction caractéristique)
- Théorème d'approximation de Weierstrass par les polynômes de Bernstein ($\rightarrow$ loi des grands nombres)

4.42 261 : Fonction caractéristique et transformée de LAPLACE d'une variable aléatoire. Exemples et applications.

- Théorème central limite ($\rightarrow$ fonction caractéristique)
- Inégalité de Hoeffding ($\rightarrow$ fonction caractéristique)

4.43 262 : Modes de convergence d'une suite de variables aléatoires. Exemples et applications.

- Théorème d'approximation de Weierstrass par les polynômes de Bernstein ($\rightarrow$ loi des grands nombres, convergence presque sûre)
- Théorème central limite ($\rightarrow$ convergence en loi)

4.44 263 : Variables aléatoires à densité. Exemples et applications.

- Théorème central limite ($\rightarrow$ loi normale)

- Inégalité de Hoeffding (→ lien avec TCL)

4.45 264 : Variables aléatoires discrètes. Exemples et applications.

- Marche aléatoire sur $\mathbb{Z}$ (→ Bernoulli)
- Théorème d'approximation de Weierstrass par les polynômes de Bernstein (→ binomiale)