Développements d'algèbre et d'analyse

Maxime Pouvreau

2013 – 2014

Table des matières

1 Couplages **3**
- 1.1 Algèbre . . . 3
- 1.2 Analyse . . . 6

2 Développements préparés pour les oraux **10**
- 2.1 Borne de Bézout . . . 10
- 2.2 Décomposition de Bruhat . . . 12
- 2.3 Décomposition de Dunford . . . 14
- 2.4 Densité des polynômes orthogonaux . . . 16
- 2.5 Ellipsoïde de John – Loewner . . . 18
- 2.6 Étude de la loi Gamma . . . 21
- 2.7 Formule d'inversion de Fourier . . . 22
- 2.8 Formule d'inversion de Fourier par la convolution . . . 24
- 2.9 Formule sommatoire de Poisson . . . 26
- 2.10 Générateurs de $O(E), SO(E)$ et $\mathrm{Isom}(\mathcal{E})$ . . . 29
- 2.11 Inégalité isopérimétrique . . . 31
- 2.12 Lemme de Morse . . . 33
- 2.13 Loi de réciprocité quadratique . . . 35
- 2.14 Méthode de Newton . . . 37
- 2.15 Méthode du gradient à pas optimal . . . 39
- 2.16 Partition d'un entier en parts fixées . . . 41
- 2.17 Prolongement méromorphe de Γ . . . 43
- 2.18 Réduction de Frobenius . . . 46
- 2.19 Sous-espaces de $\mathcal{C}(\mathbb{R}, \mathbb{C})$ de dimension finie stables par translations 50
- 2.20 Sous-groupes compacts de $GL_n(\mathbb{R})$ . . . 51
- 2.21 Sous-groupes finis de $SO(3, \mathbb{R})$ . . . 53
- 2.22 Surjectivité de l'exponentielle matricielle . . . 55
- 2.23 Table de caractères de $\mathfrak{S}_4$ . . . 57
- 2.24 Table de caractères du groupe diédral D_n . . . 60
- 2.25 Théorème d'Abel angulaire et théorème taubérien faible . . . 62
- 2.26 Théorème de Banach – Steinhaus . . . 64
- 2.27 Théorème de Bernstein . . . 66
- 2.28 Théorème de Cartan – Von Neumann . . . 70
- 2.29 Théorème de Cauchy – Lipschitz . . . 72

2.30 Théorème de Frobenius – Zolotarev 74
2.31 Théorème de Gauss – Wantzel 77
2.32 Théorème de Hahn – Banach géométrique 80
2.33 Théorème de Jordan 83
2.34 Théorème de Kronecker 86
2.35 Théorème de l'élément primitif 88
2.36 Théorème de Lie – Kolchin 90
2.37 Théorème de Molien 92
2.38 Théorème de Riesz – Fischer 94
2.39 Théorème de stabilité de Lyapunov 96
2.40 Théorème des deux carrés 98
2.40.1 Variante du théorème des deux carrés 100
2.41 Un homéomorphisme réalisé par l'exponentielle matricielle 102

3 Autres développements **105**
3.1 Classification des groupes de pavage du plan 105
3.2 Densité des fonctions continues nulle part dérivables 108
3.3 Espace de Sobolev $H^1(I)$ 110
3.4 Inégalités de Kolmogorov 113
3.5 Irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$ 115
3.6 Le folium de Descartes 117
3.7 Réduction des endomorphismes normaux 120
3.8 Théorème d'Ascoli 121
3.9 Théorème d'échantillonnage de Shannon 124
3.10 Théorème d'inversion locale 126
3.11 Théorème de Burnside 128
3.12 Théorème des fonctions implicites 130
3.13 Théorème taubérien fort 131

Chapitre 1

Couplages

1.1 Algèbre

- 101 – Groupes opérant sur un ensemble. Exemples et applications.
  - Décomposition de Bruhat
  - Sous-groupes finis de $SO(3,\mathbb{R})$ (en passant vite sur le dénombrement et en ne faisant pas $\mathfrak{S}_4$ et $\mathfrak{A}_5$)
- 102 – Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications.
  - Théorème de Kronecker
  - Théorème de Gauss – Wantzel
- 103 – Exemples et applications des notions de sous-groupe distingué et de groupe quotient.
  - Théorème de Frobenius – Zolotarev
  - Théorème de Lie – Kolchin
- 104 – Groupes finis. Exemples et applications.
  - Sous-groupes finis de $SO(3,\mathbb{R})$ (en passant vite sur le dénombrement et en ne faisant pas $\mathfrak{S}_4$ et $\mathfrak{A}_5$)
  - Table de caractères de $\mathfrak{S}_4$
- 105 – Groupes des permutations d'un ensemble fini. Applications.
  - Décomposition de Bruhat
  - Table de caractères de $\mathfrak{S}_4$
- 106 – Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $GL(E)$. Applications.
  - Sous-groupes compacts de $GL_n(\mathbb{R})$
  - Théorème de Frobenius – Zolotarev
- 107 – Représentations et caractères d'un groupe fini sur un $\mathbb{C}$-espace vectoriel.
  - Table de caractères de $\mathfrak{S}_4$
  - Table de caractères du groupe diédral D_n
- 108 – Exemples de parties génératrices d'un groupe. Applications.

  - Générateurs de $O(E), SO(E)$ et $\mathrm{Isom}(\mathcal{E})$ (seulement $O(E)$ et $SO(E)$)
  - Table de caractères du groupe diédral D_n
- 109 – Représentations de groupes finis de petit cardinal.
  - Table de caractères de $\mathfrak{S}_4$
  - Table de caractères du groupe diédral D_n
- 120 – Anneau $\mathbb{Z}/n\mathbb{Z}$. Applications.
  - Loi de réciprocité quadratique
  - Variante du théorème des deux carrés
- 121 – Nombres premiers. Applications.
  - Loi de réciprocité quadratique
  - Théorème des deux carrés
- 122 – Anneaux principaux. Applications.
  - Réduction de Frobenius
  - Théorème des deux carrés
- 123 – Corps finis. Applications.
  - Loi de réciprocité quadratique
  - Théorème de Frobenius – Zolotarev
- 124 – Anneau des séries formelles. Applications.
  - Théorème de Molien
  - Partition d'un entier en parts fixées
- 125 – Extensions de corps. Exemples et applications.
  - Théorème de l'élément primitif
  - Théorème de Gauss – Wantzel
- 126 – Exemples d'équations diophantiennes.
  - Variante du théorème des deux carrés
  - Partition d'un entier en parts fixées
- 140 – Corps des fractions rationnelles à une indéterminée sur un corps commutatif. Applications.
  - Loi de réciprocité quadratique
  - Partition d'un entier en parts fixées
- 141 – Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.
  - Théorème de Kronecker
  - Théorème de Gauss – Wantzel
- 142 – Algèbre des polynômes à plusieurs indéterminées. Applications.
  - Théorème de Kronecker
  - Théorème de Molien
- 143 – Résultant. Applications.
  - Loi de réciprocité quadratique
  - Borne de Bézout
- 144 – Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.
  - Loi de réciprocité quadratique
  - Théorème de Kronecker
- 150 – Exemples d'actions de groupes sur les espaces de matrices.
  - Décomposition de Bruhat

  - Sous-groupes compacts de $GL_n(\mathbb{R})$
- 151 – Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.
  - Théorème de Molien
  - Théorème de Gauss – Wantzel
- 152 – Déterminant. Exemples et applications.
  - Théorème de Frobenius – Zolotarev
  - Borne de Bézout
- 153 – Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.
  - Décomposition de Dunford
  - Réduction de Frobenius
- 154 – Sous-espaces stables par un endomorphisme ou une famille d'endomorphismes d'un espace vectoriel de dimension finie. Applications.
  - Réduction de Frobenius
  - Théorème de Lie – Kolchin
- 155 – Endomorphismes diagonalisables en dimension finie.
  - Décomposition de Dunford
  - Un homéomorphisme réalisé par l'exponentielle matricielle
- 156 – Exponentielle de matrices. Applications.
  - Un homéomorphisme réalisé par l'exponentielle matricielle
  - Surjectivité de l'exponentielle matricielle
- 157 – Endomorphismes trigonalisables. Endomorphismes nilpotents.
  - Décomposition de Dunford
  - Théorème de Lie – Kolchin
- 158 – Matrices symétriques réelles, matrices hermitiennes.
  - Un homéomorphisme réalisé par l'exponentielle matricielle
  - Lemme de Morse
- 159 – Formes linéaires et hyperplans en dimension finie. Exemples et applications.
  - Réduction de Frobenius
  - Théorème de Hahn – Banach géométrique
- 160 – Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie).
  - Un homéomorphisme réalisé par l'exponentielle matricielle
  - Générateurs de $O(E), SO(E)$ et $\mathrm{Isom}(\mathcal{E})$ (seulement $O(E)$ et $SO(E)$)
- 161 – Isométries d'un espace affine euclidien de dimension finie. Applications en dimensions 2 et 3.
  - Sous-groupes finis de $SO(3,\mathbb{R})$ (en passant vite sur le dénombrement et en ne faisant pas $\mathfrak{S}_4$ et $\mathfrak{A}_5$)
  - Générateurs de $O(E), SO(E)$ et $\mathrm{Isom}(\mathcal{E})$ (seulement $O(E)$ et $\mathrm{Isom}(\mathcal{E})$)
- 162 – Systèmes d'équations linéaires ; opérations, aspects algorithmiques et conséquences théoriques.
  - Décomposition de Bruhat
  - Méthode du gradient à pas optimal
- 170 – Formes quadratiques sur un espace vectoriel de dimension finie.

Orthogonalité, isotropie. Applications.
  - Ellipsoïde de John – Loewner
  - Lemme de Morse
- 171 – Formes quadratiques réelles. Exemples et applications.
  - Ellipsoïde de John – Loewner
  - Lemme de Morse
- 180 – Coniques. Applications.
  -
  -
- 181 – Barycentres dans un espace affine réel de dimension finie, convexité. Applications.
  - Sous-groupes compacts de $GL_n(\mathbb{R})$
  - Théorème de Hahn – Banach géométrique
- 182 – Applications des nombres complexes en géométrie.
  - Théorème de Jordan
  - Théorème de Gauss – Wantzel
- 183 – Utilisation des groupes en géométrie.
  - Sous-groupes finis de $SO(3,\mathbb{R})$ (en passant vite sur le dénombrement et en ne faisant pas $\mathfrak{S}_4$ et $\mathfrak{A}_5$)
  - Théorème de Gauss – Wantzel
- 190 – Méthodes combinatoires, problèmes de dénombrement.
  - Sous-groupes finis de $SO(3,\mathbb{R})$ (en ne faisant pas $D_n, \mathfrak{A}_4$ et $\mathfrak{S}_4$)
  - Partition d'un entier en parts fixées

1.2 Analyse

- 201 – Espaces de fonctions : exemples et applications.
  - Théorème de Riesz – Fischer
  - Densité des polynômes orthogonaux
- 202 – Exemples de parties denses et applications.
  - Densité des polynômes orthogonaux
  - Théorème de Bernstein
- 203 – Utilisation de la notion de compacité.
  - Ellipsoïde de John – Loewner
  - Théorème de Bernstein
- 204 – Connexité. Exemples et applications.
  - Théorème de Jordan
  - Surjectivité de l'exponentielle matricielle
- 205 – Espaces complets. Exemples et applications.
  - Théorème de Riesz – Fischer
  - Théorème de Banach – Steinhaus
- 206 – Théorèmes de point fixe. Exemples et applications.
  - Sous-groupes compacts de $GL_n(\mathbb{R})$
  - Théorème de Cauchy – Lipschitz
- 207 – Prolongement de fonctions. Exemples et applications.

  - Prolongement méromorphe de Γ
  - Théorème d'Abel angulaire et théorème taubérien faible
- 208 – Espaces vectoriels normés, applications linéaires continues. Exemples.
  - Théorème de Riesz – Fischer
  - Théorème de Banach – Steinhaus
- 209 – Approximation d'une fonction par des polynômes et des polynômes trigonométriques. Exemples et applications.
  - Densité des polynômes orthogonaux
  - Théorème de Bernstein
- 213 – Espaces de Hilbert. Bases hilbertiennes. Exemples et applications.
  - Densité des polynômes orthogonaux
  - Inégalité isopérimétrique
- 214 – Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications.
  - Lemme de Morse
  - Surjectivité de l'exponentielle matricielle
- 215 – Applications différentiables définies sur un ouvert de $\mathbb{R}^n$. Exemples et applications.
  - Lemme de Morse
  - Surjectivité de l'exponentielle matricielle
- 216 – Étude métrique de courbes. Exemples.
  - Théorème de Jordan
  - Inégalité isopérimétrique
- 217 – Sous-variétés de $\mathbb{R}^n$. Exemples.
  - Lemme de Morse
  - Théorème de Cartan – Von Neumann
- 218 – Applications des formules de Taylor.
  - Méthode de Newton
  - Lemme de Morse
- 219 – Extremums : existence, caractérisation, recherche. Exemples et applications.
  - Ellipsoïde de John – Loewner
  - Méthode du gradient à pas optimal
- 220 – Équations différentielles $X' = f(t, X)$. Exemples d'étude des solutions en dimension 1 et 2.
  - Théorème de stabilité de Lyapunov
  - Théorème de Cauchy – Lipschitz
- 221 – Équations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications.
  - Sous-espaces de $\mathcal{C}(\mathbb{R}, \mathbb{C})$ de dimension finie stables par translations
  - Théorème de stabilité de Lyapunov
- 223 – Suites numériques. Convergence, valeurs d'adhérence. Exemples et applications.
  - Méthode de Newton
  - Théorème d'Abel angulaire et théorème taubérien faible
- 224 – Exemples de développements asymptotiques de suites et de fonc-

tions.
  - Méthode de Newton
  - Partition d'un entier en parts fixées
- 226 – Suites vectorielles et réelles définies par une relation de récurrence $u_{n+1} = f(u_n)$. Exemples et applications.
  - Méthode du gradient à pas optimal
  - Méthode de Newton
- 228 – Continuité et dérivabilité des fonctions réelles d'une variable réelle. Exemples et contre-exemples.
  - Méthode de Newton
  - Théorème de Bernstein
- 229 – Fonctions monotones. Fonctions convexes. Exemples et applications.
  - Ellipsoïde de John – Loewner
  - Méthode de Newton
- 230 – Séries de nombres réels ou complexes. Comportement des restes ou des sommes partielles des séries numériques. Exemples.
  - Formule sommatoire de Poisson (avec le corollaire 2)
  - Théorème d'Abel angulaire et théorème taubérien faible
- 232 – Méthodes d'approximation des solutions d'une équation $F(X) = 0$. Exemples.
  - Méthode du gradient à pas optimal
  - Méthode de Newton
- 234 – Espaces $L^p, 1 \leq p \leq \infty$.
  - Théorème de Riesz – Fischer
  - Densité des polynômes orthogonaux
- 235 – Suites et séries de fonctions intégrables. Exemples et applications.
  - Théorème de Riesz – Fischer
  - Formule d'inversion de Fourier par la convolution
- 236 – Illustrer par des exemples quelques méthodes de calculs d'intégrales de fonctions d'une ou plusieurs variables réelles.
  - Formule d'inversion de Fourier
  - Étude de la loi Gamma
- 239 – Fonctions définies par une intégrale dépendant d'un paramètre. Exemples et applications.
  - Formule d'inversion de Fourier
  - Étude de la loi Gamma
- 240 – Produit de convolution, transformation de Fourier. Applications.
  - Formule d'inversion de Fourier par la convolution
  - Densité des polynômes orthogonaux
- 241 – Suites et séries de fonctions. Exemples et contre-exemples.
  - Théorème de Riesz – Fischer
  - Théorème d'Abel angulaire et théorème taubérien faible
- 243 – Convergence des séries entières, propriétés de la somme. Exemples et applications.
  - Partition d'un entier en parts fixées
  - Théorème d'Abel angulaire et théorème taubérien faible

- 244 – Fonctions développables en série entière, fonctions analytiques. Exemples.
  - Densité des polynômes orthogonaux
  - Partition d'un entier en parts fixées
- 245 – Fonctions holomorphes sur un ouvert de $\mathbb{C}$. Exemples et applications.
  - Théorème de Jordan
  - Prolongement méromorphe de Γ
- 246 – Séries de Fourier. Exemples et applications.
  - Formule sommatoire de Poisson (avec le corollaire 2)
  - Théorème de Banach – Steinhaus
- 247 – Exemples de problèmes d'interversion de limites.
  - Formule sommatoire de Poisson (avec le corollaire 2)
  - Théorème d'Abel angulaire et théorème taubérien faible
- 249 – Suites de variables de Bernoulli indépendantes.
  -
  -
- 253 – Utilisation de la notion de convexité en analyse.
  - Ellipsoïde de John – Loewner
  - Théorème de Hahn – Banach géométrique
- 254 – Espaces de Schwartz et distributions tempérées. Transformation de Fourier dans $\mathcal{S}(\mathbb{R}^d)$ et $\mathcal{S}'(\mathbb{R}^d)$.
  - Formule d'inversion de Fourier (dans $\mathcal{S}(\mathbb{R})$ puis dans $\mathcal{S}'(\mathbb{R})$)
  - Formule sommatoire de Poisson (avec le corollaire 1 et en se plaçant dans $\mathcal{S}(\mathbb{R})$)
- 255 – Espaces de Schwartz. Distributions. Dérivation au sens des distributions.
  - Formule d'inversion de Fourier (dans $\mathcal{S}(\mathbb{R})$ puis dans $\mathcal{S}'(\mathbb{R})$)
  - Formule sommatoire de Poisson (avec le corollaire 1 et en se plaçant dans $\mathcal{S}(\mathbb{R})$)
- 260 – Espérance, variance et moments d'une variable aléatoire.
  -
  -
- 261 – Fonction caractéristique et transformée de Laplace d'une variable aléatoire. Exemples et applications.
  -
  -
- 262 – Modes de convergence d'une suite de variables aléatoires. Exemples et applications.
  -
  -
- 263 – Variables aléatoires à densité. Exemples et applications.
  -
  -
- 264 – Variables aléatoires discrètes. Exemples et applications.
  -
  -

Chapitre 2

Développements préparés pour les oraux

2.1 Borne de Bézout

Référence :
– [SP99] page 157 exercice 8.

Théorème.
Soit k un corps infini et $P, Q \in k[X,Y]$ deux polynômes de degrés totaux respectifs d et d'. On suppose que P et Q sont premiers entre eux. Alors $|V(P) \cap V(Q)| \leq dd'$, avec $V(P) := \{(x,y) \in k^2 \mid P(x,y) = 0\}$.

Démonstration. Définissons $R(X) := \mathrm{Res}_Y(P,Q)$ et $S(Y) := \mathrm{Res}_X(P,Q)$. Montrons d'abord que $|V(P) \cap V(Q)| < +\infty$.

Si $(\alpha, \beta) \in V(P) \cap V(Q)$, alors $R(\alpha) = 0$ et $S(\beta) = 0$. Or P et Q sont premiers entre eux donc les polynômes R et S sont non nuls. On en déduit $|V(P) \cap V(Q)| \leq \deg(R)\deg(S)$.

Montrons que $\deg(R) \leq dd'$. On commence par écrire

$$P(X,Y) = \sum_{k=0}^{p} P_k(X) Y^{p-k} \quad \text{et} \quad Q(X,Y) = \sum_{k=0}^{q} Q_k(X) Y^{q-k}$$

avec p et q les degrés en Y respectifs de P et Q. On a

$$\begin{cases} \deg P_k \leq d - p + k, & 0 \leq k \leq p \\ \deg Q_k \leq d' - q + k, & 0 \leq k \leq q. \end{cases}$$

Notons M la matrice de Sylvester de P et Q comme polynômes en Y, on a

$$M = \begin{pmatrix} P_0 & \cdots & \cdots & \cdots & \cdots & P_p & 0 & \cdots & 0 \\ 0 & P_0 & \cdots & \cdots & \cdots & \cdots & P_p & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & & & \ddots & 0 \\ 0 & \cdots & 0 & P_0 & \cdots & \cdots & \cdots & \cdots & P_p \\ Q_0 & \cdots & \cdots & \cdots & Q_q & 0 & \cdots & \cdots & 0 \\ 0 & Q_0 & \cdots & \cdots & \cdots & Q_q & \ddots & & \vdots \\ \vdots & \ddots & \ddots & & & & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & & & & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & Q_0 & \cdots & \cdots & \cdots & Q_q \end{pmatrix}.$$

Pour $1 \leq i \leq q$, on a

$$M_{i,j} = \begin{cases} P_{j-i} & \text{si } 0 \leq j-i \leq p \\ 0 & \text{sinon} \end{cases}$$

donc pour tout $j \in \{1, \ldots, p+q\}, \deg(M_{i,j}) \leq d - p + j - i$.

De même, pour $q+1 \leq i \leq p+q$, on a

$$M_{i,j} = \begin{cases} Q_{j-i+q} & \text{si } 0 \leq j-i+q \leq q \\ 0 & \text{sinon} \end{cases}$$

donc pour tout $j \in \{1, \ldots, p+q\}, \deg(M_{i,j}) \leq d' - q + j - i + q = d' + j - i$.

On applique alors la formule du déterminant :

$$R = \sum_{\sigma \in \mathfrak{S}_{p+q}} \varepsilon(\sigma) \underbrace{\prod_{i=1}^{q} M_{i,\sigma(i)} \prod_{i=q+1}^{p+q} M_{i,\sigma(i)}}_{R_\sigma}.$$

Or, pour tout $\sigma \in \mathfrak{S}_{p+q}$, on a

$$\begin{aligned} \deg(R_\sigma) &\leq \sum_{i=1}^{q} (d - p + \sigma(i) - i) + \sum_{i=q+1}^{p+q} (d' + \sigma(i) - i) \\ &= q(d-p) + pd' + \underbrace{\sum_{i=1}^{p+q} (\sigma(i) - i)}_{=0} \\ &= q(d-p) + (p-d)d' + dd' \\ &= (q-d')(d-p) + dd' \\ &\leq dd'. \end{aligned}$$

On en déduit que $\deg(R) \leq dd'$ et, par le même raisonnement, $\deg(S) \leq dd'$. Donc $|V(P) \cap V(Q)| \leq (dd')^2$.

Nous allons maintenant affiner cette borne. Notons $(\alpha_1, \beta_1), \ldots, (\alpha_r, \beta_r)$ les différents points d'intersection de $V(P)$ et $V(Q)$. Si tous les α_i sont distincts alors, puisque les α_i sont racines de R, $|V(P) \cap V(Q)| = r \leq \deg(R) \leq dd'$. Si ce n'est pas le cas, on va effectuer un changement de variables pour s'y ramener.

Soit $u \in k$ tel que

$$\forall i \neq j \in \{1, \ldots, r\}, \quad \alpha_i + u\beta_i \neq \alpha_j + u\beta_j.$$

Un tel u existe car les droites d'équation $y = \alpha_i + x\beta_i$ ont deux à deux au plus un point d'intersection donc il existe un nombre fini de points dans l'intersection de deux droites, et k est infini.

Effectuons alors le changement de variables

$$\begin{cases} X' = X + uY \\ Y' = Y \end{cases}$$

et notons $\tilde{P}(X', Y') = P(X, Y), \tilde{Q}(X', Y') = Q(X, Y)$. On a alors

$$\begin{aligned} (\alpha, \beta) \in V(P) \cap V(Q) &\iff P(\alpha, \beta) = Q(\alpha, \beta) = 0 \\ &\iff \tilde{P}(\alpha + u\beta, \beta) = \tilde{Q}(\alpha + u\beta, \beta) = 0 \\ &\iff (\alpha + u\beta, \beta) \in V(\tilde{P}) \cap V(\tilde{Q}). \end{aligned}$$

On en déduit

$$V(\tilde{P}) \cap V(\tilde{Q}) = \{(\alpha_i + u\beta_i, \beta_i) \mid i \in \{1, \ldots, r\}\}$$

et puisque les $\alpha_i + u\beta_i$ sont distincts on peut appliquer la remarque faite précédemment qui nous permet de dire

$$|V(P) \cap V(Q)| = |V(\tilde{P}) \cap V(\tilde{Q})| \leq dd'.$$

□

2.2 Décomposition de Bruhat

Référence :
– [FGN07].

Définition. Un drapeau complet d'un espace vectoriel E de dimension finie n est une suite $\{0\} = F_0 \subsetneq F_1 \subsetneq \cdots \subsetneq F_n = E$ de sous-espaces vectoriels de E (on a en particulier $\dim F_i = i$ pour tout i).

On notera
– T_s l'ensemble des matrices triangulaires supérieures de $GL_n(\mathbb{K})$;
– P_σ la matrice de permutation associée à la permutation σ ;
– $\mathcal{D}$ l'ensemble des drapeaux de $\mathbb{K}^n$.

Théorème.
On a

$$GL_n(\mathbb{K}) = \bigsqcup_{\sigma \in \mathfrak{S}_n} T_s P_\sigma T_s.$$

Démonstration. On commence par quelques notations :

- $E_{i,j}$ est la matrice dont tous les coefficients sont nuls, sauf celui d'indices i, j ;
- pour $i \neq j$ et $\lambda \in \mathbb{K}, T_{i,j}(\lambda) = I_n + \lambda E_{i,j}$;
- pour $1 \leq i \leq n$ et $\alpha \neq 0, D_i(\alpha) = I_n + (\alpha - 1)E_{i,i}$.

Pour $A \in GL_n(\mathbb{K})$, multiplier à droite par $T_{i,j}(\lambda)$ revient à faire l'opération sur les colonnes $C_j \leftarrow C_j + \lambda C_i$, et multiplier à gauche revient à faire l'opération sur les lignes $L_i \leftarrow L_i + \lambda L_j$.

Multiplier à droite par $D_i(\alpha)$ revient à faire l'opération sur les colonnes $C_i \leftarrow \alpha C_i$, et multiplier à gauche revient à faire l'opération sur les lignes $L_i \leftarrow \alpha L_i$.

Le but est de transformer A en une matrice de permutation par des opérations élémentaires sur les lignes et les colonnes. On applique pour cela l'algorithme suivant :

Soit i_1 le plus grand indice k tel que $a_{k,1} \neq 0$ (qui existe car A est inversible). On effectue les opérations $L_i \leftarrow L_i - \frac{a_{i,1}}{a_{i_1,1}} L_{i_1}$ pour $i < i_1$ et $C_j \leftarrow C_j - \frac{a_{i_1,j}}{a_{i_1,1}} C_1$ pour $j \geq 2$. On termine par $C_1 \leftarrow \frac{1}{a_{i_1,1}} C_1$, de sorte qu'on soit dans la situation

$$\begin{pmatrix} 0 & & & \\ \vdots & & & \\ 0 & & & \\ 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & & \\ 0 & & & \end{pmatrix}.$$

Les opérations effectuées correspondent à des multiplications à gauche ou à droite par des éléments de T_s.

On prend ensuite i_2 le plus grand indice k tel que $a_{k,2} \neq 0$, on a $i_2 \neq i_1$. On effectue les mêmes opérations que précédemment pour annuler les coefficients de la colonne 2 et de la ligne i_2, cela ne modifie pas les éléments de la colonne 1 et de la ligne i_1.

En itérant le procédé, on obtient une matrice de permutation P_σ, où σ est la permutation qui à k associe i_k. On a donc une décomposition $A = T_1 P_\sigma T_2$, avec $T_1, T_2 \in T_s$.

Montrons que l'union du théorème est disjointe. Supposons que l'on ait deux décompositions $T_1 P_\sigma = P_\tau T_2$ avec $\sigma \neq \tau$. Il existe alors i tel que $\sigma(i) < \tau(i)$. $T_2(i,i) \neq 0$ car T_2 est inversible et, puisque $T_2 = P_{\tau^{-1}} T_1 P_\sigma$,

$$T_2(i,i) = T_1(\tau(i), \sigma(i)) = 0,$$

ce qui est une contradiction. □

Théorème.
L'action de $GL_n(\mathbb{K})$ sur $\mathcal{D} \times \mathcal{D}$ possède $n!$ orbites.

Démonstration. $GL_n(\mathbb{K})$ agit à gauche sur $\mathcal{D}$ de façon transitive. Le stabilisateur du drapeau canonique est T_s, donc $\mathcal{D}$ est en bijection avec le quotient $GL_n(\mathbb{K})/T_s$ et l'action de $GL_n(\mathbb{K})$ sur $\mathcal{D}$ correspond à l'action de $GL_n(\mathbb{K})$ sur $GL_n(\mathbb{K})/T_s$ par translation à gauche.

Soit $(A, B) \in GL_n(\mathbb{K})/T_s \times GL_n(\mathbb{K})/T_s$, alors

$$\begin{aligned}(A, B) &= A(I_n, A^{-1}B) \\ &= A(I_n, T_1 P_\sigma T_2) \\ &= AT_1(T_1^{-1}, P_\sigma T_2) \\ &= AT_1(I_n, P_\sigma).\end{aligned}$$

Chaque orbite a donc un élément de la forme (I_n, P_σ).

Supposons qu'il existe $\sigma, \tau \in \mathfrak{S}_n$ tel que (I_n, P_σ) et (I_n, P_τ) soient dans la même orbite, *i.e.* tel qu'il existe $A \in GL_n(\mathbb{K})$ vérifiant $(I_n, P_\sigma) = (A, AP_\tau)$. Alors $A \in T_s$ et il existe $T \in T_s$ tel que $AP_\tau = P_\sigma T$. Par unicité dans la décomposition de Bruhat, $\sigma = \tau$.

Il y a donc autant d'orbites que de permutations, soit $n!$. □

2.3 Décomposition de Dunford

Référence :
– [Gou09] page 194.
E est un espace vectoriel de dimension finie sur $\mathbb{K}$ un corps commutatif.

Théorème.
Soit $f \in \mathcal{L}(E)$ tel que χ_f soit scindé sur $\mathbb{K}$. Alors il existe un unique couple (d, n) d'endomorphismes tel que

(*i*) *d est diagonalisable, n est nilpotente.*

(*ii*) *$f = d + n$ et $d \circ n = n \circ d$.*

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

Lemme.
Soit $f \in \mathcal{L}(E)$ et $F \in \mathbb{K}[X]$ un polynôme annulateur de f unitaire. Soit $F = M_1^{\alpha_1} \cdots M_s^{\alpha_s}$ la décomposition en facteurs irréductibles de F sur $\mathbb{K}$. Pour tout i, on note $N_i := \ker M_i^{\alpha_i}(f)$.

Alors $E = \bigoplus_{i=1}^s N_i$ et pour tout i, la projection sur N_i parallèlement à $\bigoplus_{j \neq i} N_j$ est un polynôme en f.

Démonstration. Le lemme des noyaux donne $E = \bigoplus_{i=1}^s N_i$.

Pour tout i, notons $Q_i := \prod_{j \neq i} M_j^{\alpha_j}$, les Q_i sont premiers entre eux dans leur ensemble. Par l'identité de Bezout, il existe $U_1, \ldots, U_s \in \mathbb{K}[X]$ tels que

$U_1Q_1 + \cdots + U_sQ_s = 1$.
On note $P_i := U_iQ_i$ et $p_i := P_i(f)$, alors

$$\sum_{i=1}^{s} p_i = \mathrm{Id}. \tag{2.1}$$

Par ailleurs, pour tout $j \neq i$, F divise Q_iQ_j donc

$$\forall j \neq i, \quad p_i \circ p_j = Q_iQ_j(f) \circ U_iU_j(f) = 0. \tag{2.2}$$

On déduit de 2.1 que $p_i = \sum_{j=1}^{s} p_j \circ p_i$ et de 2.2 que $p_i = p_i^2$. Les p_i sont donc des projecteurs.

Montrons que pour tout i, $\operatorname{Im} p_i = N_i$. Soit $x \in E$, alors

$$M_i^{\alpha_i}(f)(p_i(x)) = M_i^{\alpha_i}(f) \circ P_i(f)(x) = U_i(f) \circ F(f)(x) = 0,$$

donc $\operatorname{Im} p_i \subset N_i$.
Soit $x \in N_i$, alors d'après 2.1, $x = p_1(x) + \cdots + p_s(x) = p_i(x)$ car, pour $j \neq i$, $p_j(x) = U_j(f) \circ Q_j(f)(x) = 0$ car $M_i^{\alpha_i}$ divise Q_j. On a donc $\operatorname{Im} p_i = N_i$.

Montrons que $\ker p_i = \bigoplus_{j \neq i} N_j$.
On a déjà montré que $N_j \subset \ker p_i$ pour $i \neq j$. Soit $x \in \ker p_i$, alors d'après 2.1, $x = \sum_{j \neq i} p_j(x)$ donc $x \in \bigoplus_{j \neq i} N_j$.

Les projecteurs p_i sont alors bien des polynômes en f. □

Démonstration du théorème. On commence par montrer l'existence. On écrit $\chi_f = (-1)^n \prod_{i=1}^{s} (X - \lambda_i)^{\alpha_i}$ et on note $N_i := \ker(f - \lambda_i)^{\alpha_i}$.
En reprenant les notations du lemme, on a alors que p_i est le projecteur sur N_i parallèlement à $\bigoplus_{j \neq i} N_j$. Posons

$$d := \sum_{i=1}^{s} \lambda_i p_i \quad \text{et} \quad n := f - d = \sum_{i=1}^{s} (f - \lambda_i \mathrm{Id}) p_i,$$

alors d est diagonalisable comme somme d'endomorphismes diagonalisables qui commutent deux à deux. Par ailleurs, en utilisant $p_i \circ p_j = 0$ si $i \neq j$ et p_i sinon, on obtient

$$\forall q \in \mathbb{N}^*, \quad n^q = \sum_{i=1}^{s} (f - \lambda_i \mathrm{Id})^q p_i.$$

Si $q := \sup \alpha_i$, on a $(f - \lambda_i \mathrm{Id})^q p_i = [(X - \lambda_i)^q P_i](f) = 0$ car χ_f divise $(X - \lambda_i)^q P_i$, donc $n^q = 0$.
d et n vérifient donc les hypothèses du théorème.

Montrons désormais l'unicité : Soit (d', n') un autre couple vérifiant (i) et (ii). Les endomorphismes d' et n' commutent avec $d' + n' = f$ donc avec d et n qui sont des polynômes en f. Ainsi, d et d' sont diagonalisables dans une même base, donc $d - d'$ est diagonalisable. Or $d - d' = n' - n$ est nilpotente, donc $d - d' = n' - n = 0$. □

Application (Calcul de l'exponentielle matricielle)**.** On suppose $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Soit $f \in \mathcal{L}(E)$ admettant une décomposition de Dunford $f = d + n$. On a alors

$$d = \sum_{i=1}^{s} \lambda_i p_i \quad \text{et} \quad n = \sum_{i=1}^{s} (f - \lambda_i \mathrm{Id}) p_i,$$

où les p_i sont les projecteurs définis dans la preuve ci-dessus. On en déduit

$$\exp(d) = \sum_{p=0}^{+\infty} \frac{d^p}{p!} = \sum_{p=0}^{+\infty} \sum_{i=1}^{s} \frac{\lambda_i^p}{p!} p_i = \sum_{i=1}^{s} \sum_{p=0}^{+\infty} \frac{\lambda_i^p}{p!} p_i = \sum_{i=1}^{s} e^{\lambda_i} p_i.$$

Par ailleurs,

$$\exp(n) = \sum_{p=0}^{+\infty} \frac{n^p}{p!} = \sum_{p=0}^{+\infty} \sum_{i=1}^{s} \frac{(f - \lambda_i \mathrm{Id})^p}{p!} p_i = \sum_{i=1}^{s} \sum_{p=0}^{\alpha_i - 1} \frac{(f - \lambda_i \mathrm{Id})^p}{p!} p_i.$$

On en déduit

$$\exp(f) = \exp(d) \exp(n) = \sum_{i=1}^{s} e^{\lambda_i} \sum_{p=0}^{\alpha_i - 1} \frac{(f - \lambda_i \mathrm{Id})^p}{p!} p_i$$

car d et n commutent.

2.4 Densité des polynômes orthogonaux

Référence :

– [BMP05] page 140.

Soit I un intervalle de $\mathbb{R}$. On appelle fonction poids une fonction $w : I \to \mathbb{R}$ mesurable, strictement positive et telle que

$$\forall n \in \mathbb{N}, \quad \int_I |x|^n w(x) \, \mathrm{d}x < +\infty.$$

On note $L^2(I, w)$ l'espace des fonctions de carré intégrable pour la mesure de densité w. Il s'agit d'un espace de Hilbert pour le produit scalaire

$$\langle f, g \rangle_w := \int_I f(x) g(x) w(x) \, \mathrm{d}x.$$

Par le procédé d'orthogonalisation de Gram-Schmidt appliqué à la base canonique de $\mathbb{R}[X]$, il existe une unique famille échelonnée de polynômes de norme 1 orthogonaux deux à deux. Cette famille s'appelle la famille des polynômes orthogonaux associée à la fonction poids w.

Théorème.
On suppose qu'il existe un réel $\alpha > 0$ tel que

$$\int_I e^{\alpha |x|} w(x) \, \mathrm{d}x < +\infty.$$

Alors les polynômes orthogonaux associés à w forment une base hilbertienne de $L^2(I,w)$.

Démonstration. La famille de polynômes orthogonaux associée à w est une base orthonormale de $\mathbb{R}[X]$, il s'agit donc de montrer qu'elle est totale, c'est-à-dire que son orthogonal est nul. Soit donc $f \in L^2(I,w)$ telle que pour tout $n \in \mathbb{N}$, $\int_I f(x)x^n w(x)\,\mathrm{d}x = 0$.

On commence par définir $\varphi : x \mapsto f(x)w(x)\mathbf{1}_I(x)$ sur $\mathbb{R}$. I est de mesure finie pour $w\mathrm{d}\lambda$ donc $L^2(I,w) \subset L^1(I,w)$, donc $\varphi \in L^1(I,w)$. On peut donc considérer la transformée de Fourier de φ :

$$\hat{\varphi}(\xi) = \int_I e^{-i\xi x} f(x)w(x)\,\mathrm{d}x.$$

Montrons que $\hat{\varphi}$ se prolonge sur $\Omega := \{z \in \mathbb{C} \mid |\Im\mathrm{m}\, z| < \alpha/2\}$. On définit pour cela $g : (z,x) \mapsto e^{-izx} f(x)w(x)$ et $F : z \mapsto \int_I g(z,x)\,\mathrm{d}x$ et on va montrer que F est holomorphe sur Ω.

- $g(z,\cdot)$ est mesurable pour tout $z \in \Omega$,
- $g(\cdot,x)$ est holomorphe pour tout $x \in I$,
- $\forall x \in I, \forall z \in \Omega$,

$$|g(z,x)| \leq e^{\alpha|x|/2}|f(x)|w(x) \in L^1(I)$$

car $x \mapsto e^{\alpha|x|/2}$ et f sont dans $L^2(I,w)$ donc leur produit est dans $L^1(I,w)$. On peut donc appliquer le théorème d'holomorphie sous l'intégrale qui prouve que F est holomorphe sur Ω. De plus, on calcule les dérivées de F en dérivant sous l'intégrale, ce qui donne

$$F^{(n)}(z) = (-i)^n \int_I x^n e^{-izx} f(x)w(x)\,\mathrm{d}x,$$

d'où

$$F^{(n)}(0) = (-i)^n \int_I x^n f(x)w(x)\,\mathrm{d}x = 0.$$

Par unicité du développement en série entière, $F = 0$ sur un voisinage de 0, donc sur Ω par prolongement analytique. On en déduit que $\hat{\varphi} = 0$ et donc $\varphi = 0$ par injectivité de la transformée de Fourier. Finalement, $f = 0$ sur I car $w > 0$. □

Remarque. Donnons un contre-exemple dans le cas où l'hypothèse du théorème n'est pas vérifiée.

On pose $I :=]0,+\infty[$ et $w : x \mapsto x^{-\ln x}$ qui est bien une fonction poids. On pose aussi $f : x \mapsto \sin(2\pi \ln(x))$ et on va montrer que $\langle f, x^n\rangle_w = 0$ pour tout $n \in \mathbb{N}$.

$$\langle f, x^n\rangle_w = \int_I x^n \sin(2\pi \ln x) x^{-\ln x}\,\mathrm{d}x.$$

On effectue le changement de variables $y = \ln x$:

$$\langle f, x^n\rangle_w = \int_{\mathbb{R}} e^{(n+1)y} \sin(2\pi y) e^{-y^2}\,\mathrm{d}y = e^{\frac{(n+1)^2}{4}} \int_{\mathbb{R}} e^{-\left(y-\frac{n+1}{2}\right)^2} \sin(2\pi y)\,\mathrm{d}y.$$

On effectue alors le changement de variables $t = y - \frac{n+1}{2}$:

$$\langle f, x^n \rangle_w = e^{\frac{(n+1)^2}{4}} \int_{\mathbb{R}} e^{-t^2} \sin(2\pi t + (n+1)\pi)\, \mathrm{d}t = (-1)^{n+1} e^{\frac{(n+1)^2}{4}} \int_{\mathbb{R}} e^{-t^2} \sin(2\pi t)\, \mathrm{d}t = 0$$

car l'intégrande est impaire. Donc la famille des polynômes orthogonaux associée à w n'est pas totale.

2.5 Ellipsoïde de John – Loewner

Référence :
– [FGN08] page 229.

Théorème.
Soit $K \subset \mathbb{R}^n$ un compact d'intérieur non vide. Alors il existe un unique ellipsoïde centré en 0 de volume minimal contenant K.

Démonstration. Un ellipsoïde plein centré en 0 admet une équation du type $q(x) \leq 1$ où q est une forme quadratique définie positive.
On note $\mathcal{Q}$ (resp. $\mathcal{Q}_+$, resp. $\mathcal{Q}_{++}$) l'ensemble des formes quadratiques (resp. positives, resp. définies positives) de $\mathbb{R}^n$ et on pose

$$\mathcal{E}_q := \{x \in \mathbb{R}^n \mid q(x) \leq 1\}.$$

Par théorème spectral, il existe une base orthonormale $\mathcal{B} = (e_1, \ldots, e_n)$ dans laquelle q s'écrit

$$q(x) = \sum_{i=1}^n a_i x_i^2 \quad \text{avec} \quad x = \sum_{i=1}^n x_i e_i,$$

où $a_i > 0$ car q est définie positive.
On note V_q le volume de $\mathcal{E}_q$, on a

$$V_q = \int_{\sum_{i=1}^n a_i x_i^2 \leq 1} \mathrm{d}x_1 \cdots \mathrm{d}x_n.$$

On effectue le changement de variable $x_i = \frac{t_i}{\sqrt{a_i}}$ dont le jacobien est $\frac{1}{\sqrt{a_1 \cdots a_n}}$, on a alors

$$V_q = \frac{1}{\sqrt{a_1 \cdots a_n}} \int_{\sum_{i=1}^n x_i^2 \leq 1} \mathrm{d}x_1 \cdots \mathrm{d}x_n = \frac{V_0}{\sqrt{a_1 \cdots a_n}}$$

où V_0 est le volume de la boule unité euclidienne.

Montrons que $a_1 \cdots a_n$ ne dépend que de q. Soit S la matrice de q dans une base orthonormée, alors il existe $P \in GL_n(\mathbb{R})$ telle que

$$S = P \mathrm{diag}(a_1, \ldots, a_n)\, {}^tP$$

et $P \in O_n(\mathbb{R})$ car les deux bases sont orthonormées. On a donc

$$\det S = \det \operatorname{diag}(a_1, \dots, a_n) = a_1 \cdots a_n =: D(q)$$

qui ne dépend que de q. On a alors

$$V_q = \frac{V_0}{\sqrt{D(q)}}.$$

On doit donc montrer qu'il existe un unique $q \in \mathcal{Q}_{++}$ tel que $D(q)$ soit maximal et $\forall x \in K, q(x) \leq 1$.

On munit $\mathcal{Q}$ de la norme N définie par

$$N(q) := \sup_{\|x\| \leq 1} |q(x)|.$$

On cherche à maximiser D sur $A := \{q \in \mathcal{Q}_+ \mid \forall x \in K, q(x) \leq 1\}$. Montrons que A est un compact convexe non vide de Q.

– A est convexe : soit $q, q' \in A$ et $\lambda \in [0,1]$. Pour tout $x \in \mathbb{R}^n$,

$$(\lambda q + (1-\lambda)q')(x) = \lambda q(x) + (1-\lambda)q'(x) \geq 0$$

donc $\lambda q + (1-\lambda)q' \in \mathcal{Q}_+$.
De plus, si $x \in K$,

$$\lambda q(x) + (1-\lambda)q'(x) \leq \lambda + 1 - \lambda = 1$$

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

– A est fermé : soit $(q_n)_{n\in\mathbb{N}}$ une suite de A convergeant dans $\mathcal{Q}$ vers q. Alors pour tout $x \in \mathbb{R}^n$,

$$|q(x) - q_n(x)| \leq N(q - q_n)\|x\|^2$$

donc $\lim_{n\to+\infty} q_n(x) = q(x)$. On en déduit

$$\forall x \in \mathbb{R}^n, \quad q(x) \geq 0 \quad \text{et} \quad \forall x \in K, \quad q(x) \leq 1$$

donc $q \in A$.

– A est borné : K est d'intérieur non vide donc il existe $a \in K$ et $r > 0$ tels que $\bar{B}(a, r) \subset K$.
Soit $q \in A$, si $\|x\| \leq r$ alors $a + x \in K$ donc $q(a+x) \leq 1$ et $q(-a) = q(a) \leq 1$. Par l'inégalité de Minkowski, on a

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

donc $q(x) \leq 4$.
Si $\|x\| \leq 1$,

$$|q(x)| = q(x) = \frac{1}{r^2} q(rx) \leq \frac{4}{r^2},$$

d'où $N(q) \leq \frac{4}{r^2}$.

– $A \neq \varnothing$: K est compact donc est borné. Soit $M > 0$ tel que $\forall x \in K, \|x\| \leq M$.

Si $q(x) := \frac{\|x\|^2}{M^2}$, alors pour tout $x \in K$, $q(x) \leq 1$ donc $q \in A$.

det est continue donc $q \mapsto D(q)$ est continue sur A donc atteint son maximum sur A en q_0.

A contient $x \mapsto \frac{\|x\|^2}{M^2}$ qui est définie positive donc $D(q_0) > 0$, donc $q_0 \in \mathcal{Q}_{++}$. Il existe donc un ellipsoïde $\mathcal{E}_{q_0}$ de volume minimal centré en 0 qui contient K.

Unicité : soit $q \in A$ tel que $D(q) = D(q_0)$ et $q \neq q_0$. Soit S et S_0 les matrices respectives de q et q_0 dans la base canonique de $\mathbb{R}^n$.
A est convexe donc $\frac{1}{2}(q + q_0) \in A$ et on a, par stricte concavité logarithmique du det sur $\mathcal{Q}_{++}$,

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

ce qui contredit la maximalité de $D(q_0)$. □

Détails supplémentaires

Stricte concavité logarithmique du déterminant sur $\mathcal{S}_n^{++}(\mathbb{R})$:

Proposition.
Soit $A, B \in \mathcal{S}_n^{++}(\mathbb{R})$ distinctes et $t \in]0,1[$, alors on a

$$\det(tA + (1-t)B) > (\det A)^t (\det B)^{1-t}.$$

Démonstration. $A, B \in \mathcal{S}_n^{++}(\mathbb{R})$ donc par pseudo-réduction simultanée, il existe $P \in GL_n(\mathbb{R})$ et $D = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ avec $\lambda_i > 0$ telles que

$$A = {}^tPP \quad \text{et} \quad B = {}^tPDP.$$

Alors

$$\begin{aligned}\det(tA + (1-t)B) &= (\det P)^2 \det(tI_n + (1-t)D) \\ &= (\det P)^2 \prod_{i=1}^{n}(t + (1-t)\lambda_i)\end{aligned}$$

et

$$(\det A)^t (\det B)^{1-t} = (\det P)^2 \left(\prod_{i=1}^{n} \lambda_i\right)^{1-t}.$$

A et B sont distinctes donc il existe i, disons $i = 1$, tel que $\lambda_i \neq 1$. Alors par stricte concavité du logarithme on a

$$\ln(t + (1-t)\lambda_1) > (1-t)\ln(\lambda_1)$$

et on a l'inégalité large pour les autres valeurs de i, donc

$$\sum_{i=1}^{n} \ln(t + (1-t)\lambda_i) > (1-t)\sum_{i=1}^{n} \ln(\lambda_i),$$

d'où le résultat. □

2.6 Étude de la loi Gamma

Référence :
– [CGCDM11].
Soit $a > 0$ et $\lambda > 0$. Soit X une variable aléatoire de loi $\Gamma(a, \lambda)$, de densité

$$f(x) = \frac{\lambda^a}{\Gamma(a)} e^{-\lambda x} x^{a-1} \mathbf{1}_{[0,+\infty[}(x).$$

Calcul de $\mathbb{E}[X]$.

$$\begin{aligned}
\mathbb{E}[X] &= \frac{\lambda^a}{\Gamma(a)} \int_0^{+\infty} e^{-\lambda x} x^a \, \mathrm{d}x \\
&= \frac{\lambda^a}{\Gamma(a)} \int_0^{+\infty} e^{-u} \frac{u^a}{\lambda^a} \frac{\mathrm{d}u}{\lambda} \\
&= \frac{\Gamma(a+1)}{\lambda \Gamma(a)} \\
&= \frac{a}{\lambda}.
\end{aligned}$$

Calcul de $\mathrm{Var}(X)$.

Le même calcul donne $\mathrm{Var}(X) = \frac{a}{\lambda^2}$.

Calcul de la transformée de Laplace L_X de X.

$$L_X(t) = \mathbb{E}[e^{tX}] = \frac{\lambda^a}{\Gamma(a)} \int_0^{+\infty} e^{(t-\lambda)x} x^{a-1} \, \mathrm{d}x$$

lorsque cette intégrale existe. L'intégrande est intégrable en 0 car $e^{(t-\lambda)x} x^{a-1} \sim x^{a-1}$ avec $a - 1 > -1$.

En $+\infty$, l'intégrande n'est intégrable que pour $t - \lambda < 0$, donc L_X est définie sur $]-\infty, \lambda[$. On a alors, pour $t < \lambda$, en effectuant le changement de variables $x = \frac{u}{\lambda - t}$,

$$L_X(t) = \frac{\lambda^a}{\Gamma(a)} \int_0^{+\infty} e^u \frac{u^{a-1}}{(\lambda - t)^{a-1}} \frac{\mathrm{d}u}{\lambda - t} = \left(\frac{\lambda}{\lambda - t} \right)^a.$$

Calcul de la fonction caractéristique φ_X de X.

$$\varphi_X(t) = \mathbb{E}[e^{itX}] = \frac{\lambda^a}{\Gamma(a)} \int_0^{+\infty} e^{(it-\lambda)x} x^{a-1} \, \mathrm{d}x.$$

Montrons que φ_X peut se prolonger en une fonction holomorphe sur $D := \{z \in \mathbb{C} \mid \Re(z) < \lambda\}$. Pour $z \in D$, on pose

$$F(z) := \frac{\lambda^a}{\Gamma(a)} \int_0^{+\infty} e^{(z-\lambda)x} x^{a-1} \, \mathrm{d}x.$$

Appliquons le théorème d'holomorphie sous l'intégrale pour montrer que F est bien définie et holomorphe sur D. On pose $g(x,z) := e^{(z-\lambda)x} x^{a-1}$, on a alors

- pour tout $z \in D, g(\cdot, z)$ est mesurable ;
- pour tout $x > 0, g(x, \cdot)$ est holomorphe sur D ;
- soit $\varepsilon > 0$, pour $x > 0$ et $z \in D$ tel que $\Re(z) < \lambda - \varepsilon$, on a

$$|g(x,z)| = e^{(\Re(z)-\lambda)x} x^{a-1} \leq e^{-\varepsilon x} x^{a-1} \in L^1(\mathbb{R}_+).$$

On en déduit que F est bien définie et holomorphe sur D.

D'autre part, pour tout $z \in D, \Re(\lambda - z) > 0$, donc on peut définir $(\lambda - z)^a = e^{a \log(\lambda - z)}$ avec log la détermination principale du logarithme sur $\mathbb{C} \setminus \mathbb{R}_-$. La fonction G définie sur D par

$$G(z) = \left(\frac{\lambda}{\lambda - z}\right)^a$$

prolonge ainsi la fonction L_X sur D.

Finalement, F et G coïncident sur $]-\infty, \lambda[$ donc, par le principe de prolongement analytique, $F = G$ sur D, d'où

$$\forall t \in \mathbb{R}, \quad \varphi_X(t) = F(it) = \left(\frac{\lambda}{\lambda - it}\right)^a.$$

2.7 Formule d'inversion de Fourier

Référence :

- [QZ06] page 331.

Pour $f \in L^1(\mathbb{R})$ on définit la transformée de Fourier de f par

$$\hat{f}(t) = \int_{\mathbb{R}} \mathrm{e}^{-itx} f(x) \, \mathrm{d}x.$$

Théorème.
Soit $f \in L^1(\mathbb{R}) \cap \mathcal{C}_b(\mathbb{R})$ telle que $\hat{f} \in L^1(\mathbb{R})$, alors pour tout $x \in \mathbb{R}$,

$$f(x) = \frac{1}{2\pi} \int_{\mathbb{R}} \mathrm{e}^{itx} \hat{f}(t) \, \mathrm{d}t.$$

Démonstration. Soit $\varepsilon > 0$, alors

$$|\mathrm{e}^{itx} \mathrm{e}^{-\varepsilon t^2} \hat{f}(t)| \leq |\hat{f}(t)| \in L^1$$

donc, d'après le théorème de convergence dominée,

$$\frac{1}{2\pi}\int_{\mathbb{R}} \mathrm{e}^{itx}\hat{f}(t)\,\mathrm{d}t = \lim_{\varepsilon\to 0}\frac{1}{2\pi}\int_{\mathbb{R}} \mathrm{e}^{itx}\mathrm{e}^{-\varepsilon t^2}\hat{f}(t)\,\mathrm{d}t.$$

On a

$$\frac{1}{2\pi}\int_{\mathbb{R}} \mathrm{e}^{itx-\varepsilon t^2}\hat{f}(t)\,\mathrm{d}t = \frac{1}{2\pi}\int_{\mathbb{R}} \mathrm{e}^{itx-\varepsilon t^2}\left(\int_{\mathbb{R}} \mathrm{e}^{-ity}f(y)\,\mathrm{d}y\right)\,\mathrm{d}t.$$

Or

$$\int_{\mathbb{R}}\left(\int_{\mathbb{R}}\left|\mathrm{e}^{it(x-y)}\mathrm{e}^{-\varepsilon t^2}f(y)\right|\,\mathrm{d}y\right)\,\mathrm{d}t = \int_{\mathbb{R}}\mathrm{e}^{-\varepsilon t^2}\,\mathrm{d}t\int_{\mathbb{R}}|f(y)|\,\mathrm{d}y < +\infty$$

donc la fonction $\mathrm{e}^{itx-\varepsilon t^2}\mathrm{e}^{-ity}f(y)$ est dans L^1 pour la mesure produit et d'après le théorème de Fubini on peut intervertir les intégrales :

$$\frac{1}{2\pi}\int_{\mathbb{R}} \mathrm{e}^{itx-\varepsilon t^2}\hat{f}(t)\,\mathrm{d}t = \frac{1}{2\pi}\int_{\mathbb{R}} f(y)\left(\int_{\mathbb{R}} \mathrm{e}^{-it(y-x)}\mathrm{e}^{-\varepsilon t^2}\,\mathrm{d}t\right)\,\mathrm{d}y.$$

Posons

$$I(x) := \int_{\mathbb{R}} \mathrm{e}^{-itx}\mathrm{e}^{-\varepsilon t^2}\,\mathrm{d}t.$$

Alors l'intégrande est de classe $\mathcal{C}^1$ selon x, intégrable selon t et sa dérivée par rapport à x est majorée en module par $|t|\mathrm{e}^{-\varepsilon t^2}$ qui est intégrable. D'après le théorème de dérivation sous l'intégrale, I est de classe $\mathcal{C}^1$ et on a

$$\begin{aligned} I'(x) &= -i\int_{\mathbb{R}} t\mathrm{e}^{-itx}\mathrm{e}^{-\varepsilon t^2}\,\mathrm{d}t \\ &= \frac{i}{2\varepsilon}\left(\left[\mathrm{e}^{-itx}\mathrm{e}^{-\varepsilon t^2}\right]_{\mathbb{R}} + ix\int_{\mathbb{R}}\mathrm{e}^{-itx}\mathrm{e}^{-\varepsilon t^2}\,\mathrm{d}t\right) \\ &= -\frac{x}{2\varepsilon}I(x). \end{aligned}$$

On en déduit $I(x) = I(0)\mathrm{e}^{-\frac{x^2}{4\varepsilon}}$. Or

$$I(0) = \int_{\mathbb{R}}\mathrm{e}^{-\varepsilon t^2}\,\mathrm{d}t = \frac{1}{\sqrt{\varepsilon}}\int_{\mathbb{R}}\mathrm{e}^{-t^2}\,\mathrm{d}t = \sqrt{\frac{\pi}{\varepsilon}}.$$

D'où $I(x) = \sqrt{\frac{\pi}{\varepsilon}}\mathrm{e}^{-\frac{x^2}{4\varepsilon}}$. On en déduit

$$\begin{aligned} \frac{1}{2\pi}\int_{\mathbb{R}} \mathrm{e}^{itx-\varepsilon t^2}\hat{f}(t)\,\mathrm{d}t &= \frac{1}{2\pi}\sqrt{\frac{\pi}{\varepsilon}}\int_{\mathbb{R}} f(y)\mathrm{e}^{-\frac{(y-x)^2}{4\varepsilon}}\,\mathrm{d}y \\ &= \frac{1}{\sqrt{\pi}}\int_{\mathbb{R}}\mathrm{e}^{-u^2}f(x+2\sqrt{\varepsilon}u)\,\mathrm{d}u \end{aligned}$$

par changement de variables $y = x + 2\sqrt{\varepsilon}u$. En appliquant le théorème de convergence dominée (car f est bornée) on obtient alors

$$\lim_{\varepsilon\to 0}\frac{1}{2\pi}\int_{\mathbb{R}} \mathrm{e}^{itx-\varepsilon t^2}\hat{f}(t)\,\mathrm{d}t = \frac{1}{\sqrt{\pi}}\int_{\mathbb{R}}\mathrm{e}^{-u^2}f(x)\,\mathrm{d}u = f(x).$$

□

Remarque. Si $f \in \mathcal{S}(\mathbb{R})$, alors f vérifie les hypothèses du théorème. Si l'on sait que $\mathcal{S}(\mathbb{R})$ est stable par transformée de Fourier, on en déduit l'inversion de Fourier dans $\mathcal{S}'(\mathbb{R})$. En effet, si $\mathcal{F}$ et $\overline{\mathcal{F}}$ désignent respectivement la transformée de Fourier et la transformée de Fourier inverse sur $\mathcal{S}(\mathbb{R})$, on a, pour $\varphi \in \mathcal{S}(\mathbb{R})$ et $T \in \mathcal{S}'(\mathbb{R})$,

$$\langle \overline{\mathcal{F}} \circ \mathcal{F}(T), \varphi \rangle = \langle T, \mathcal{F} \circ \overline{\mathcal{F}}(\varphi) \rangle = \langle T, \varphi \rangle.$$

2.8 Formule d'inversion de Fourier par la convolution

Référence :
– [BP06] page 279.
Pour $f \in L^1(\mathbb{R})$ on définit la transformée de Fourier de f par

$$\hat{f}(t) = \int_{\mathbb{R}} \mathrm{e}^{-itx} f(x)\,\mathrm{d}x.$$

On donne aussi la définition d'une approximation de l'unité :

Définition. Une suite $(\alpha_n)_{n\geq 1}$ d'éléments de $L^1(\mathbb{R})$ est une approximation de l'unité si elle vérifie

(i) pour tout $n \geq 1$, $\displaystyle\int_{\mathbb{R}} \alpha_n = 1$,

(ii) $\displaystyle\sup_{n\geq 1} \int_{\mathbb{R}} |\alpha_n| < +\infty$,

(iii) pour tout $\varepsilon > 0$, $\displaystyle\lim_{n\to+\infty} \int_{|t|\geq\varepsilon} |\alpha_n| = 0$.

On rappelle le théorème suivant :

Théorème.
Soit $(\alpha_n)_{n\geq 1}$ une approximation de l'unité, $p \in [1, +\infty[$ et $f \in L^p(\mathbb{R})$. Alors

$$\forall n \geq 1, \quad f * \alpha_n \in L^p(\mathbb{R}) \quad \textit{et} \quad f * \alpha_n \xrightarrow{\|\cdot\|_p} f.$$

Le résultat à démontrer est le suivant :

Théorème.
Soit $f \in L^1(\mathbb{R})$ telle que $\hat{f} \in L^1(\mathbb{R})$. Alors pour presque tout $x \in \mathbb{R}$,

$$f(x) = \frac{1}{2\pi} \int_{\mathbb{R}} \hat{f}(t) \mathrm{e}^{ixt}\,\mathrm{d}t = \frac{1}{2\pi} \hat{\hat{f}}(-x).$$

Démonstration. On pose

$$a_n(x) := \frac{1}{2\pi} \mathrm{e}^{-\frac{|x|}{n}}$$

et on introduit $\alpha_n := \widehat{a_n}$. Montrons que $(\alpha_n)_{n\geq 1}$ est une approximation de l'unité.

$$\begin{aligned}
\alpha_n(t) &= \frac{1}{2\pi}\int_{\mathbb{R}} \mathrm{e}^{-\frac{|x|}{n}-itx}\,\mathrm{d}x \\
&= \frac{1}{2\pi}\int_{-\infty}^{0} \mathrm{e}^{\frac{x}{n}-itx}\,\mathrm{d}x + \frac{1}{2\pi}\int_{0}^{+\infty} \mathrm{e}^{-\frac{x}{n}-itx}\,\mathrm{d}x \\
&= \frac{1}{2\pi}\left[\frac{\mathrm{e}^{\frac{x}{n}-itx}}{\frac{1}{n}-it}\right]_{-\infty}^{0} + \frac{1}{2\pi}\left[\frac{\mathrm{e}^{-\frac{x}{n}-itx}}{-\frac{1}{n}-it}\right]_{0}^{+\infty} \\
&= \frac{1}{2\pi}\left(\frac{1}{\frac{1}{n}-it}+\frac{1}{\frac{1}{n}+it}\right) \\
&= \frac{n}{\pi}\frac{1}{1+(nt)^2}.
\end{aligned}$$

On a alors

$$\begin{aligned}
\int_{\mathbb{R}} \alpha_n(t)\,\mathrm{d}t &= \frac{n}{\pi}\int_{\mathbb{R}} \frac{\mathrm{d}t}{1+(nt)^2} \\
&= \frac{1}{\pi}\int_{\mathbb{R}} \frac{\mathrm{d}u}{1+u^2} = 1.
\end{aligned}$$

Par ailleurs, pour $\varepsilon > 0$,

$$\begin{aligned}
\int_{|t|\geq\varepsilon} \alpha_n(t)\,\mathrm{d}t &= \frac{n}{\pi}\int_{|t|\geq\varepsilon} \frac{\mathrm{d}t}{1+(nt)^2} \\
&= \frac{1}{\pi}\int_{|u|\geq n\varepsilon} \frac{\mathrm{d}u}{1+u^2} \\
&= \frac{1}{\pi}\int_{\mathbb{R}} \frac{1}{1+u^2}\mathbf{1}_{\{|u|\geq n\varepsilon\}}(u)\,\mathrm{d}u \xrightarrow[n\to+\infty]{} 0
\end{aligned}$$

par convergence dominée.

$(\alpha_n)_{n\geq 1}$ est donc une approximation de l'unité. On a alors

$$\begin{aligned}
\alpha_n * f(x) &= \int_{\mathbb{R}} \alpha_n(x-t)f(t)\,\mathrm{d}t \\
&= \int_{\mathbb{R}}\int_{\mathbb{R}} a_n(u)\mathrm{e}^{-iu(x-t)}\,\mathrm{d}u f(t)\,\mathrm{d}t \\
&= \int_{\mathbb{R}} a_n(u)\mathrm{e}^{-iux}\int_{\mathbb{R}} f(t)\mathrm{e}^{iut}\,\mathrm{d}t\,\mathrm{d}u
\end{aligned}$$

par application du théorème de Fubini, car $|a_n(u)\mathrm{e}^{-iu(x-t)}f(t)| = |a_n(u)f(t)|$ est intégrable pour la mesure produit $\mathrm{d}t\,\mathrm{d}u$ d'après le théorème de Fubini-Tonelli.

On en déduit, par parité de a_n,

$$\begin{aligned}\alpha_n * f(x) &= \int_{\mathbb{R}} a_n(u)\mathrm{e}^{iux}\int_{\mathbb{R}} f(t)\mathrm{e}^{-iut}\,\mathrm{d}t\,\mathrm{d}u \\ &= \int_{\mathbb{R}} a_n(u)\mathrm{e}^{iux}\hat{f}(u)\,\mathrm{d}u.\end{aligned}$$

Or $|a_n(u)\mathrm{e}^{iux}\hat{f}(u)| \leq |\hat{f}(u)| \in L^1(\mathbb{R})$ et $\lim_{n\to+\infty} a_n(u) = \frac{1}{2\pi}$ pour tout u. En appliquant le théorème de convergence dominée on a donc

$$\lim_{n\to+\infty} \alpha_n * f(x) = \frac{1}{2\pi}\int_{\mathbb{R}} \hat{f}(u)\mathrm{e}^{iux}\,\mathrm{d}u = \frac{1}{2\pi}\hat{\hat{f}}(-x).$$

Par ailleurs, $f \in L^1(\mathbb{R})$ et (α_n) est une approximation de l'unité donc $\lim_{n\to+\infty} \|\alpha_n * f - f\|_1 = 0$. D'après le théorème de Riesz-Fischer, il existe une sous-suite $(\alpha_{\varphi(n)})$ telle que $\alpha_{\varphi(n)} * f$ converge presque partout vers f. D'où $f = \hat{\hat{f}}(-\cdot)$ presque partout. □

Remarque. Si on prend pour convention

$$\hat{f}(t) = \int_{\mathbb{R}} f(x)e^{-2i\pi tx}\,\mathrm{d}x,$$

il faut prendre $a_n(x) := e^{-\frac{|x|}{n}}$.

2.9 Formule sommatoire de Poisson

Référence :
– [Gou08] page 273.
Pour $F \in L^1(\mathbb{R})$ on définit la transformée de Fourier de F par

$$\hat{F}(x) := \int_{\mathbb{R}} F(t)e^{-2i\pi xt}\,\mathrm{d}t.$$

Pour f 1-périodique et intégrable sur $[0,1]$ on définit les coefficients de Fourier de f par

$$\forall n \in \mathbb{Z}, \quad c_n(f) := \int_0^1 f(t)e^{-2i\pi nt}\,\mathrm{d}t.$$

Théorème.
Soit $F \in \mathcal{C}^1(\mathbb{R})$ telle que $F(x) = O\left(\frac{1}{|x|^\alpha}\right)$ et $F'(x) = O\left(\frac{1}{|x|^\alpha}\right)$ pour $|x| \to +\infty$ et $\alpha > 1$. Alors

$$\forall x \in \mathbb{R}, \quad \sum_{n\in\mathbb{Z}} F(x+n) = \sum_{n\in\mathbb{Z}} \hat{F}(n)e^{2i\pi nx}.$$

Démonstration. On introduit la fonction

$$f(x) := \sum_{n\in\mathbb{Z}} F(x+n).$$

Cette série est normalement convergente sur tout compact de $\mathbb{R}$: soit $M > 0$ tel que $|F(x)| \leq M(1+|x|)^{-\alpha}$ pour tout $x \in \mathbb{R}$, soit $A > 0$ et $|x| \leq A$, alors A

$$\begin{aligned}
|F(x+n)| &\leq M(1+|x+n|)^{-\alpha} \\
&\leq M(1+|n|-|x|)^{-\alpha} \quad \text{pour } |n| \geq A \\
&\leq M(1+|n|-A)^{-\alpha}.
\end{aligned}$$

On prouve de la même façon que $\sum_{n\in\mathbb{Z}} F'(x+n)$ converge uniformément sur tout compact de $\mathbb{R}$ donc, d'après le théorème de dérivation sous le signe somme, f est de classe $\mathcal{C}^1$ sur $\mathbb{R}$.

De plus f est clairement 1-périodique par changement d'indice. On a alors

$$\begin{aligned}
c_m(f) &= \int_0^1 f(t)e^{-2i\pi mt}\,\mathrm{d}t \\
&= \int_0^1 \sum_{n\in\mathbb{Z}} F(t+n)e^{-2i\pi mt}\,\mathrm{d}t \\
&= \sum_{n\in\mathbb{Z}} \int_0^1 F(t+n)e^{-2i\pi mt}\,\mathrm{d}t,
\end{aligned}$$

la permutation étant justifiée par la convergence normale de $\sum_{n\in\mathbb{Z}} F(t+n)$ sur $[0,1]$. D'où

$$\begin{aligned}
c_m(f) &= \sum_{n\in\mathbb{Z}} \int_n^{n+1} F(u)e^{-2i\pi m(u-n)}\,\mathrm{d}u \\
&= \int_{\mathbb{R}} F(u)e^{-2i\pi mu}\,\mathrm{d}u \\
&= \hat{F}(m).
\end{aligned}$$

Finalement, f est de classe $\mathcal{C}^1$ donc, d'après le théorème de Dirichlet, elle est égale à sa série de Fourier :

$$f(x) = \sum_{n\in\mathbb{Z}} c_n(f)e^{2i\pi nx} = \sum_{n\in\mathbb{Z}} \hat{F}(n)e^{2i\pi nx},$$

d'où le résultat. En particulier, pour $x = 0$,

$$\sum_{n\in\mathbb{Z}} F(n) = \sum_{n\in\mathbb{Z}} \hat{F}(n).$$

□

Remarque. Si $F \in \mathcal{S}$, alors F vérifie les hypothèses du théorème.

Corollaire.
Soit $N \geq 0$, on pose

$$T_n := \sum_{n=-N}^{N} \delta_n \in \mathcal{S}'(\mathbb{R}).$$

Alors la suite $(T_N)_N$ converge dans $\mathcal{S}'(\mathbb{R})$ vers une distribution $\delta_{\mathbb{Z}}$ qui vérifie $\widehat{\delta_{\mathbb{Z}}} = \delta_{\mathbb{Z}}$.

Démonstration. Soit $\varphi \in \mathcal{S}(\mathbb{R})$. La somme $\sum_{n\in\mathbb{Z}} \varphi(n)$ est bien définie donc

$$\langle T_N, \varphi\rangle \xrightarrow[N\to+\infty]{} \langle \delta_{\mathbb{Z}}, \varphi\rangle := \sum_{n\in\mathbb{Z}} \varphi(n).$$

Vérifions que $\delta_{\mathbb{Z}}$ est bien une distribution tempérée. Si $\varphi \in \mathcal{S}(\mathbb{R})$, on a

$$\begin{aligned}
|\langle \delta_{\mathbb{Z}}, \varphi\rangle| &\leq \sum_{n\in\mathbb{Z}} |\varphi(n)| \\
&= \sum_{n\in\mathbb{Z}^*} \frac{1}{n^2} n^2 \varphi(n) + \varphi(0) \\
&\leq \frac{\pi^2}{3} \|\varphi\|_{2,0} + \|\varphi\|_{0,0},
\end{aligned}$$

avec $\|\varphi\|_{n,p} = \sup_{x\in\mathbb{R}} |x^n \varphi^{(p)}(x)|$. On a donc $\delta_{\mathbb{Z}} \in \mathcal{S}'(\mathbb{R})$. La formule sommatoire de Poisson nous donne alors

$$\begin{aligned}
\langle \widehat{\delta_{\mathbb{Z}}}, \varphi\rangle &= \langle \delta_{\mathbb{Z}}, \hat{\varphi}\rangle \\
&= \sum_{n\in\mathbb{Z}} \hat{\varphi}(n) \\
&= \sum_{n\in\mathbb{Z}} \varphi(n) \\
&= \langle \delta_{\mathbb{Z}}, \varphi\rangle.
\end{aligned}$$

□

Corollaire.
Pour tout $s > 0$,

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

Démonstration. Soit $\alpha > 0$, on pose $F : x \mapsto e^{-\alpha x^2}$. Alors F vérifie les hypothèses du théorème et on a, pour $n \in \mathbb{Z}$,

$$\hat{F}(n) = \int_{\mathbb{R}} e^{-\alpha t^2} e^{-2i\pi n t}\, \mathrm{d}t = \frac{1}{\sqrt{\alpha}} \int_{\mathbb{R}} e^{-u^2} e^{-\frac{2i\pi n u}{\sqrt{\alpha}}}\, \mathrm{d}u.$$

Or on montre facilement que la transformée de Fourier de $u \mapsto e^{-u^2}$ est $z \mapsto \sqrt{\pi}e^{-\pi^2 z^2}$, donc

$$\hat{F}(n) = \sqrt{\frac{\pi}{\alpha}} e^{-\frac{\pi^2 n^2}{\alpha}}.$$

On a donc, par la formule sommatoire de Poisson,

$$\sum_{n\in\mathbb{Z}} e^{-\alpha n^2} = \sqrt{\frac{\pi}{\alpha}} \sum_{n\in\mathbb{Z}} e^{-\frac{\pi^2 n^2}{\alpha}}.$$

□

2.10 Générateurs de $O(E), SO(E)$ et Isom$(\mathcal{E})$

Références :
- [Cog02] ;
- [Tau05].

Théorème (Générateurs de $O(E)$ et $SO(E)$)**.**
Soit E un espace vectoriel euclidien de dimension n et $u \in O(E)$.
Notons $F_u := \ker(u - Id_E)$ et $p_u := n - \dim F_u$ la codimension de l'espace des invariants de u.

(i) L'élément u est exactement la composée de p_u réflexions de E.

(ii) Si $u \in SO(E)$ et si $n \geq 3$, alors u est la composée de p_u renversements de E et p_u est pair.

Démonstration. (i) La proposition est vraie si $p_u = 0$ car dans ce cas $u = \mathrm{Id}_E$.
Supposons que la proposition est vraie pour tout élément $v \in O(E)$ tel que $p_v \leq k$ et soit $u \in O(E)$ tel que $p_u = k + 1$.
Nous allons exhiber une réflexion σ telle que $p_{\sigma\circ u} \leq k$ pour appliquer l'hypothèse de récurrence.
$u \neq \mathrm{Id}_E$ car $k+1 \geq 1$ donc $F_u \neq E$ et donc $F_u^\perp \neq \{0\}$. On considère alors $a \in F_u^\perp$ non nul.
La réflexion $\sigma := \sigma_{a-u(a)}$ de vecteur $a - u(a)$ transforme $u(a)$ en a, *i.e.* $a \in F_{\sigma\circ u}$. En effet,

$$\langle a - u(a), a + u(a)\rangle = \|a\|^2 - \|u(a)\|^2 = 0,$$

donc $a + u(a)$ est fixe par σ et donc

$$\begin{aligned}\sigma(u(a)) &= \frac{1}{2}(\sigma(a + u(a)) - \sigma(a - u(a))) \\ &= \frac{1}{2}(a + u(a) + a - u(a)) \\ &= a.\end{aligned}$$

D'autre part, puisque F_u est stable par u, alors $F_u^\perp$ est aussi stable par u car $u \in O(E)$, donc $a - u(a) \in F_u^\perp$. On en déduit

$$F_u \subset \{a - u(a)\}^\perp = F_\sigma,$$

d'où

$$F_u \oplus \mathbb{R}a \subset F_{\sigma\circ u}.$$

On a alors

$$p_{\sigma\circ u} = n - \dim F_{\sigma\circ u} \leq n - \dim(F_u \oplus \mathbb{R}a) = p_u - 1 = k.$$

En appliquant l'hypothèse de récurrence pour $\sigma \circ u$, on en déduit que $\sigma \circ u$ est la composée de $p_{\sigma\circ u}$ réflexions de E, et donc que u est la composée d'au plus $p_{\sigma\circ u} + 1 = k + 1$ réflexions de E.
Montrons maintenant que ce nombre de symétries orthogonales dans la décomposition de u est optimal. On suppose que u est la composée de q réflexions : $u = \sigma_{a_1} \circ \cdots \circ \sigma_{a_q}$ avec $1 \leq q \leq k + 1$. Alors

$$\bigcap_{1\leq j\leq q} \{a_j\}^\perp \subset F_u.$$

Or $\bigcap_{1\leq j\leq q}\{a_j\}^\perp = \mathrm{vect}(a_1, \ldots, a_q)^\perp$ donc est de dimension $\geq n-q$. Ainsi,

$$\dim F_u = n - (k + 1) \geq n - q,$$

donc $q \geq k+1$. Finalement $q = k+1$, ce qui montre que u est la composée d'exactement $p_u + 1$ réflexions.

(*ii*) On suppose ici que $u \in SO(E) \setminus \{\mathrm{Id}_E\}$, on a d'après ce qui précède que u est la composée de p_u réflexions.
Une réflexion étant une isométrie de déterminant -1, on a $\det u = (-1)^{p_u}$, donc p_u est pair.
Si $\dim E = 3$, on a alors $p_u = 2$ et donc $u = \sigma_1 \circ \sigma_2 = (-\sigma_1) \circ (-\sigma_2)$ avec σ_i une réflexion, donc u est la composée des deux renversements $-\sigma_1$ et $-\sigma_2$.
Si $\dim E \geq 4$, montrons que la composée de deux réflexions est la composée de deux renversements en se ramenant à la dimension 3.
Soit $x, y \in E$ tels que $\sigma_x \neq \sigma_y$, *i.e.* (x, y) est libre. On note $F = \mathrm{vect}(\{x, y\})$, on a alors $\dim F^\perp = n - 2 \geq 2$.
Soit $z \in F^\perp$ non nul, en posant $G := \mathrm{vect}(\{x, y, z\})$, on a

$$G^\perp \subset \{x\}^\perp \cap \{y\}^\perp \quad \text{donc} \quad (\sigma_x)_{|G^\perp} = (\sigma_y)_{|G^\perp} = \mathrm{Id}_E,$$

donc en choisissant une base orthogonale adaptée à la décomposition $E = G \oplus G^\perp$ on obtient que $(\sigma_x)_{|G}$ et $(\sigma_y)_{|G}$ sont des isométries de déterminant -1, donc $(\sigma_x)_{|G} \circ (\sigma_y)_{|G} \in SO(G)$.
Or $\dim G = 3$ donc on peut appliquer ce qu'on a fait précédemment pour conclure.

□

Théorème (Générateurs de Isom($\mathcal{E}$))**.**
Soit $\mathcal{E}$ un espace affine euclidien de direction E et φ une isométrie affine de $\mathcal{E}$. Alors

- *si φ a un point fixe, φ est exactement la composée de $p_{\vec{\varphi}}$ réflexions affines,*
- *si φ n'a pas de point fixe, φ est la composée d'au plus $p_{\vec{\varphi}} + 2$ réflexions affines, et alors $p_{\vec{\varphi}} \leq n - 1$.*

Démonstration. Notons $p := p_{\vec{\varphi}}$.

- On suppose que φ a un point fixe O, alors

  $$\vec{\varphi} = \sigma_1 \circ \cdots \circ \sigma_p.$$

  En notant s_i l'isométrie affine de partie linéaire σ_i telle que $s_i(O) = O$, s_i est une réflexion et

  $$\varphi = s_1 \circ \cdots \circ s_p.$$

- On suppose que φ n'a pas de point fixe. Alors on peut écrire $\varphi = \tau \circ \psi$ où τ est une translation et ψ possède un point fixe. De plus, $\vec{\varphi} = \vec{\psi}$ donc ψ s'écrit comme le produit de p réflexions. On conclut en disant que τ s'écrit comme le produit de 2 réflexions.
  Par ailleurs, φ n'a pas de point fixe donc $\dim F_{\vec{\varphi}} \geq 1$ et donc $p_{\vec{\varphi}} \leq n - 1$.
  □

2.11 Inégalité isopérimétrique

Références :

- [FGN12] page 324 ;
- [QZ06].

Théorème.
Soit $\gamma : [0, 1] \to \mathbb{C}$ une application de classe $\mathcal{C}^1$ telle que $\gamma(0) = \gamma(1)$, $\gamma_{[0,1[}$ est injective et $\gamma'(t) \neq 0$ pour tout t. Ainsi, $\Gamma := \gamma([0, 1])$ est une courbe simple fermée, on note L sa longueur et S la surface enfermée par Γ. Alors

$$L^2 \geq 4\pi S$$

et $L^2 = 4\pi S$ si et seulement si Γ est un cercle.

Démonstration. On commence par quelques simplifications.

Montrons que l'on peut se ramener au cas où $|\gamma'(t)| = L$ pour tout t. Pour $t \in [0, 1]$, on définit l'abscisse curviligne de γ par

$$s(t) = \int_0^t |\gamma'(u)| \, \mathrm{d}u$$

et on pose

$$\varphi(t) := \frac{1}{L} s(t).$$

φ est de classe $\mathcal{C}^1$, $\varphi(0) = 0$ et $\varphi(1) = 1$ et $\gamma'(t) \neq 0$ pour tout t donc φ est strictement croissante, il s'agit donc d'un $\mathcal{C}^1$-difféomorphisme de $[0,1]$ dans $[0,1]$. On note $\tilde{\gamma} := \gamma \circ \varphi^{-1}$, alors

$$\begin{aligned}\tilde{\gamma}'(t) &= (\varphi^{-1})'(t)\gamma'(\varphi^{-1}(t)) \\ &= \frac{1}{\varphi'(\varphi^{-1}(t))}\gamma'(\varphi^{-1}(t)) \\ &= L\frac{\gamma'(\varphi^{-1}(t))}{|\gamma'(\varphi^{-1}(t))|}.\end{aligned}$$

On a donc $|\tilde{\gamma}'(t)| = L$ pour tout t. De plus, pour $t < u$,

$$\begin{aligned}\tilde{\gamma}(t) = \tilde{\gamma}(u) &\iff \gamma(\varphi^{-1}(t)) = \gamma(\varphi^{-1}(u)) \\ &\iff \varphi^{-1}(t) = 0 \text{ et } \varphi^{-1}(u) = 1 \quad \text{car } \gamma \text{ est simple et fermée} \\ &\iff t = \varphi(0) = 0 \text{ et } u = \varphi(1) = 1.\end{aligned}$$

Finalement, $\tilde{\gamma}$ est une courbe simple fermée de classe $\mathcal{C}^1$ sur $[0,1]$, vérifiant $|\tilde{\gamma}(t)| = L$ pour tout t et de même support que γ. On peut donc supposer que γ vérifie les propriétés de $\tilde{\gamma}$.

Par ailleurs, quitte à remplacer γ par $\gamma(1 - \cdot)$, on peut supposer que γ est positivement orientée.

On peut maintenant prouver le théorème. Pour calculer S, on utilise la formule de Green-Riemann qui s'écrit, si le domaine A enfermé par γ est vue dans $\mathbb{R}^2$,

$$\int\int_A \left(\frac{\partial Q}{\partial x}(x,y) - \frac{\partial P}{\partial y}(x,y)\right) \mathrm{d}x\,\mathrm{d}y = \int_\gamma P(x,y)\,\mathrm{d}x + Q(x,y)\,\mathrm{d}y.$$

En particulier, si on prend $Q : (x,y) \mapsto \frac{x}{2}$ et $P : (x,y) \mapsto -\frac{y}{2}$, on a $\frac{\partial Q}{\partial x} - \frac{\partial P}{\partial y} = 1$ donc

$$\int\int_A \mathrm{d}x\,\mathrm{d}y = S = \frac{1}{2}\int_\gamma x\,\mathrm{d}y - y\,\mathrm{d}x = \frac{1}{2}\int_0^1 (x(t)y'(t) - y(t)x'(t))\,\mathrm{d}t,$$

où $\gamma(t) = x(t) + iy(t)$. On en déduit

$$S = \frac{1}{2}\mathrm{Im}\int_0^1 \gamma'(t)\overline{\gamma(t)}\,\mathrm{d}t.$$

Donnons désormais une expression de L^2. On a

$$L^2 = \int_0^1 |\gamma'(t)|^2\,\mathrm{d}t.$$

On souhaite maintenant utiliser la formule de Parseval sur γ'. Pour cela, remarquons, puisque $\gamma(0) = \gamma(1)$, que l'on peut prolonger γ en une fonction 1-périodique continue de classe $\mathcal{C}^1$ par morceaux sur $\mathbb{R}$, que l'on note toujours

γ. En appliquant la formule de Parseval à γ' (qui est continue sur $[0,1]$ donc L^2), on obtient alors, si c_n désignent les coefficients de Fourier,

$$L^2 = \sum_{n\in\mathbb{Z}} |c_n(\gamma')|^2 = 4\pi^2 \sum_{n\in\mathbb{Z}} n^2 |c_n(\gamma)|^2$$

car $c_n(\gamma') = 2i\pi n c_n(\gamma)$.

Par ailleurs, la formule de Parseval donne aussi

$$\int_0^1 \gamma'(t)\overline{\gamma(t)}\,\mathrm{d}t = \sum_{n\in\mathbb{Z}} c_n(\gamma')\overline{c_n(\gamma)} = 2i\pi \sum_{n\in\mathbb{Z}} n|c_n(\gamma)|^2.$$

On en déduit

$$S = \frac{1}{2}\mathrm{Im}\int_a^b \gamma'(t)\overline{\gamma(t)}\,\mathrm{d}t = \pi \sum_{n\in\mathbb{Z}} n|c_n(\gamma)|^2.$$

D'où

$$L^2 - 4\pi S = 4\pi^2 \sum_{n\in\mathbb{Z}} (n^2 - n)|c_n(\gamma)|^2 \geq 0.$$

Par ailleurs, pour tout n différent de 0 et 1, $n^2 - n > 0$ donc $L^2 = 4\pi S$ si et seulement si $c_n(\gamma) = 0$ pour n différent de 0 et 1, c'est-à-dire si et seulement si

$$\forall t \in [0,1], \quad \gamma(t) = c_0(\gamma) + c_1(\gamma)e^{2i\pi t},$$

ce qui est une paramétrisation du cercle de centre $c_0(\gamma)$ et de rayon $|c_1(\gamma)|$. □

2.12 Lemme de Morse

Référence :
– [Rou09] page 354.

Théorème (Lemme de Morse)**.**
Soit $U \subseteq \mathbb{R}^n$ un ouvert contenant 0.
Soit $f \in \mathcal{C}^3(U,\mathbb{R})$ telle que :
– *$Df(0) = 0$*
– *la forme hessienne $D^2f(0)$ est non dégénérée de signature $(p, n-p)$.*
Alors il existe $\varphi : x \mapsto u$ un $\mathcal{C}^1$-difféomorphisme entre deux voisinages de 0 dans $\mathbb{R}^n$ tel que :
– *$\varphi(0) = 0$*
– *$f(x) - f(0) = u_1^2 + \cdots + u_p^2 - u_{p+1}^2 - \cdots - u_n^2$ au voisinage de 0.*

Lemme.
Soit $A_0 \in GL_n(\mathbb{R}) \cap S_n(\mathbb{R})$.
Alors il existe un voisinage V de A_0 dans $S_n(\mathbb{R})$ et $\phi \in \mathcal{C}^1(V, GL_n(\mathbb{R}))$ tels que :

$$\forall A \in V, \qquad A = {}^t\phi(A) A_0 \phi(A)$$

Démonstration. On considère :

$$\begin{aligned}\varphi : M_n(\mathbb{R}) &\longrightarrow S_n(\mathbb{R}) \\ M &\longmapsto {}^tMA_0M\end{aligned}$$

φ est polynomiale donc de classe $\mathcal{C}^1$.

Pour $H \in M_n(\mathbb{R})$, on a :

$$\begin{aligned}\varphi(I_n + H) - \varphi(I_n) &= {}^tHA_0 + A_0H + {}^tHA_0H \\ &= {}^t(A_0H) + A_0H + o\left(\|H\|\right)\end{aligned}$$

D'où :

$$D\varphi(I_n).H = {}^t(A_0H) + A_0H$$

$D\varphi(I_n)$ est surjective car, pour $A \in S_n(\mathbb{R})$, on a :

$$D\varphi(I_n).\left(\frac{1}{2}A_0^{-1}A\right) = A$$

Par ailleurs :

$$\ker D\varphi(I_n) = \{H \in M_n(\mathbb{R}) \mid A_0H \in \mathcal{A}_n(\mathbb{R})\}$$

Or $M_n(\mathbb{R}) = S_n(\mathbb{R}) \oplus \mathcal{A}_n(\mathbb{R})$ donc, si on pose $F := \{H \in M_n(\mathbb{R}) \mid A_0H \in S_n(\mathbb{R})\}$, on a :

$$M_n(\mathbb{R}) = F \oplus \ker D\varphi(I_n)$$

et $I_n \in F$.

Soit $\psi : F \to S_n(\mathbb{R})$ la restriction de φ à F. Alors $D\psi(I_n)$ est bijective car :

$$\ker D\varphi(I_n) \cap F = \{0\} = \ker D\psi(I_n)$$

Par le théorème d'inversion locale, il existe un voisinage ouvert U de I_n dans F (que l'on peut supposer inclus dans l'ouvert $GL_n(\mathbb{R})$) tel que ψ soit un $\mathcal{C}^1$-difféomorphisme de U sur $V := \psi(U)$.

V est un voisinage ouvert de $A_0 = \psi(I_n)$ dans $S_n(\mathbb{R})$ et :

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

D'où le résultat en posant $\phi := \psi^{-1}$. □

Démonstration du lemme de Morse. La formule de Taylor avec reste intégral à l'ordre 1 s'écrit au voisinage de 0 :

$$f(x) - f(0) = {}^txQ(x)x$$

où $Q(x)$ est la matrice symétrique suivante (quitte à restreindre, on peut supposer U convexe pour que $D^2f(tx)$ soit définie) :

$$Q(x) = \int_0^1 (1-t)D^2f(tx)\,\mathrm{d}t$$

et Q est de classe $\mathcal{C}^1$.

De plus, $Q(0) \in GL_n(\mathbb{R}) \cap S_n(\mathbb{R})$ donc d'après le lemme, il existe $M(x) \in GL_n(\mathbb{R})$ avec M de classe $\mathcal{C}^1$ au voisinage de 0 telle que :

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

D'où, en posant $y := M(x)x$,

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

Or $Q(0) = \frac{1}{2}D^2f(0)$ est de signature $(p, n-p)$, donc par la loi d'inertie de Sylvester, il existe $A \in GL_n(\mathbb{R})$ telle que, si on pose $u := A^{-1}y$, on ait :

$$\begin{aligned} {}^tyQ(0)y &= {}^tu{}^tAQ(0)Au \\ &= u_1^2 + \cdots + u_p^2 - u_{p+1}^2 - \cdots - u_n^2 \end{aligned}$$

Enfin, $x \mapsto u = A^{-1}M(x)x$ a pour différentielle à l'origine $A^{-1}M(0) \in GL_n(\mathbb{R})$ donc, d'après le théorème d'inversion locale, c'est un $\mathcal{C}^1$-difféomorphisme entre deux voisinages de 0 dans $\mathbb{R}^n$. □

2.13 Loi de réciprocité quadratique

Référence :
– [Mér06].
Il s'agit ici de démontrer la loi de réciprocité quadratique :

Théorème.
Si p et q sont deux nombres premiers impairs distincts, alors

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

On commence par deux résultats préliminaires.

Définition. Soit A un anneau commutatif. On appelle polynôme de Laurent toute fraction rationnelle de la forme $\sum_{i\in\mathbb{Z}} a_iX^i \in A(X)$ telle que les $a_i \in A$ soient presque tous nuls. Les polynômes de Laurent forment un sous-anneau de $A(X)$.

Proposition.
Tout polynôme de Laurent de la forme $P := \sum_{i=-n}^{n} a_iX^i$ avec $a_{-i} = a_i$ pour tout i et $a_n \neq 0$ s'écrit de manière unique sous la forme $Q(X + \frac{1}{X})$ avec $Q \in A[X]$ de degré n.

Démonstration. Si $Q = b_0 + b_1X + \cdots + b_nX^n$ avec $b_n \neq 0$, alors $Q(X + \frac{1}{X}) = b_nX^{-n} + \cdots + b_nX^n$ où les monômes dans les $\cdots$ ont un exposant compris entre

$-(n-1)$ et $n-1$. On en déduit que si Q est non nul, alors $Q(X+\frac{1}{X})$ aussi, ce qui montre l'unicité de Q.

Montrons l'existence de Q par récurrence sur n.
Si $P = a_0$, $Q := a_0$ convient.
Supposons le résultat connu pour des polynômes de Laurent faisant intervenir des exposants compris entre $-(n-1)$ et $n-1$. Soit $P := \sum_{i=-n}^{n} a_i X^i$ avec $a_{-i} = a_i$ et $a_n \neq 0$. Le polynôme de Laurent $P - a_n(X+\frac{1}{X})^n$ a des coefficients symétriques donc, par hypothèse de récurrence, il existe $R \in A[X]$ de degré inférieur à $n-1$ tel que $P - a_n(X+\frac{1}{X})^n = R(X+\frac{1}{X})$. Le polynôme $Q := R + a_n X^n$ vérifie $P = Q(X+\frac{1}{X})$ et est de degré n. □

Proposition.
Pour p un nombre premier impair, on note $V_p \in \mathbb{Z}[X]$ le polynôme de degré $\frac{p-1}{2}$ tel que

$$V_p\left(X+\frac{1}{X}\right) = \sum_{i=-\frac{p-1}{2}}^{\frac{p-1}{2}} X^i.$$

Son existence et son unicité sont garanties par la proposition précédente.

Si q est un autre nombre premier impair distinct de p, alors

$$\left(\frac{q}{p}\right) = Res(V_p, V_q).$$

Démonstration. Montrons que ces deux quantités sont congrues modulo p. Pour cela, établissons d'abord que V_p est congru à $(X-2)^{\frac{p-1}{2}}$ modulo p.

V_p étant unitaire, un représentant $\overline{V_p}$ de la classe de V_p dans $\mathbb{F}_p[X]$ est un polynôme unitaire de degré $\frac{p-1}{2}$. Pour montrer que $\overline{V_p} = (X-2)^{\frac{p-1}{2}}$, il suffit de montrer que si K est un corps de décomposition de $\overline{V_p}$ sur $\mathbb{F}_p$, alors 2 est l'unique racine de $\overline{V_p}$ dans K.
Soit $x \in K$ tel que $\overline{V_p}(x) = 0$. Dans une certaine extension L de K, il existe ζ tel que $x = \zeta + \frac{1}{\zeta}$ (ζ vérifie $\zeta^2 - x\zeta + 1 = 0$). On a alors

$$\overline{V_p}(x) = \overline{V_p}\left(\zeta+\frac{1}{\zeta}\right) = \sum_{i=-\frac{p-1}{2}}^{\frac{p-1}{2}} \zeta^i = 0.$$

D'où

$$\sum_{i=0}^{p-1} \zeta^i = 0 \quad \text{et} \quad \sum_{i=1}^{p} \zeta^i = 0,$$

d'où $\zeta^p - 1 = 0$. On en déduit $(\zeta-1)^p = 0$ et donc $\zeta = 1$ et $x = 2$.

La réduction modulo p de $\mathrm{Res}(V_p, V_q)$ donne

$$\begin{aligned}\overline{\mathrm{Res}(V_p, V_q)} &= \mathrm{Res}(\overline{V_p}, \overline{V_q}) \\ &= \overline{V_q}(2)^{\frac{p-1}{2}} \\ &= q^{\frac{p-1}{2}} \\ &= \left(\frac{q}{p}\right)\end{aligned}$$

dans $\mathbb{F}_p$.

Il reste à montrer que $\mathrm{Res}(V_p, V_q)$ est égal à ± 1. Pour cela, il suffit de montrer que pour tout nombre premier l, l ne divise pas $\mathrm{Res}(V_p, V_q)$, c'est-à-dire que V_p et V_q n'ont pas de racine commune dans une extension finie K de $\mathbb{F}_l$.
Soit $x \in K$ une racine commune de V_p et V_q dans K. Comme précédemment, on peut écrire $x = \zeta + \frac{1}{\zeta}$ avec ζ appartenant à une extension L de K. $V_p(x) = 0$ donc $\zeta^p = 1$ et $V_q(x) = 0$ donc $\zeta^q = 1$. Or p et q sont premiers entre eux donc $\zeta = 1$. Quitte à échanger les rôles de p et q, on peut supposer que $p \neq l$, on a alors

$$V_p(x) = \sum_{i=-\frac{p-1}{2}}^{\frac{p-1}{2}} \zeta^i = p \neq 0$$

dans $\mathbb{F}_l$. □

Par la formule $\mathrm{Res}(V_q, V_p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\mathrm{Res}(V_p, V_q)$, on en déduit la loi de réciprocité quadratique.

2.14 Méthode de Newton

Référence :
– [Rou09].

Soit $f : [c, d] \to \mathbb{R}$, $c < d$, une fonction de classe $\mathcal{C}^2$ telle que $f(c) < 0 < f(d)$ et $f'(x) > 0$ pour tout $x \in [c, d]$.

Ces hypothèses entraînent qu'il existe un unique $a \in]c, d[$ tel que $f(a) = 0$. Le but est d'approcher a. On définit

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

et, pour $x_0 \in [c, d]$, on pose $x_{n+1} := F(x_n)$.

Proposition.
Il existe $\alpha > 0$ tel que si $x_0 \in [a - \alpha, a + \alpha]$, la suite $(x_n)_{n\in\mathbb{N}}$ converge de façon quadratique vers a, i.e. *il existe $C > 0$ tel que*

$$\forall n \in \mathbb{N}, \quad |x_{n+1} - a| \leq C|x_n - a|^2.$$

Démonstration. On a

$$F(a) = a \quad \text{et} \quad F'(a) = 1 - \frac{f'(a)^2 - f(a)f''(a)}{f'(a)^2} = 0.$$

Pour $x \in [c, d]$, on a

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

En appliquant la formule de Taylor-Lagrange à l'ordre 2, il existe z_x entre a et x tel que

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

En posant

$$C := \frac{\max_{[c,d]} |f''|}{2 \min_{[c,d]} |f'|},$$

on a alors

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

Soit désormais $\alpha > 0$ tel que $C\alpha < 1$ et $I := [a - \alpha, a + \alpha] \subset [c, d]$. Alors pour $x \in I$,

$$|F(x) - a| \leq C\alpha^2 < \alpha,$$

d'où $F(I) \subset I$.

Si $x_0 \in I$, on en déduit que $x_n \in I$ pour tout n et

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

d'où

$$C|x_n - a| \leq (C|x_0 - a|)^{2^n} \leq (C\alpha)^{2^n}$$

et donc le résultat voulu, puisque $C\alpha < 1$. □

Proposition.
On suppose de plus que $f'' > 0$. Alors

- *$I := [a, d]$ est stable par F,*
- *pour $x_0 \in I$, la suite $(x_n)_{n\in\mathbb{N}}$ est strictement décroissante ou constante, converge vers a, et*

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

Démonstration. Remarquons d'abord que si $x_0 = a$, alors $(x_n)_n$ est constante. On suppose dorénavant $x_0 > a$.

Montrons d'abord que I est stable par F.

Pour $x \in]a, d]$, $f'(x) > 0$ et $f(x) > 0$ donc $F(x) < x$.
De plus, $f'' > 0$ donc

$$F(x) - a = \frac{1}{2}\frac{f''(z_x)}{f'(x)}(x-a)^2 > 0.$$

On obtient donc que I est stable par F et que pour tout n, $a < x_n \leq d$ et $(x_n)_n$ est strictement décroissante. $(x_n)_n$ admet donc une limite $l \in I$ et, par continuité, $F(l) = l$ donc $l = a$. Alors on montre de même que ci-dessus que

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

d'où la convergence quadratique de (x_n) vers a.

Finalement, en posant $z_n := z_{x_n}$, on a

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

car $a \leq z_n \leq x_n$ donc $\lim_{n\to+\infty} z_n = a$. □

2.15 Méthode du gradient à pas optimal

Références :
– [RWM10] page 412 ;
– [FGN08] page 139.
Pour $A \in \mathcal{S}_n^{++}(\mathbb{R})$ et $b \in \mathbb{R}^n$ on définit

$$\begin{aligned} f : \mathbb{R}^n &\longrightarrow \mathbb{R} \\ x &\longmapsto \frac{1}{2}\langle Ax, x\rangle - \langle b, x\rangle. \end{aligned}$$

On a

$$f(x+h) - f(x) = \langle Ax - b, h\rangle + \langle Ah, h\rangle$$

car A est symétrique, d'où $\nabla f(x) = Ax - b$. Résoudre $Ax = b$ revient donc à trouver l'unique point critique $\bar{x}$ de f, qui est alors un minimum global strict de f car $\langle Ah, h\rangle > 0$ pour tout $h \neq 0$.

On définit alors l'algorithme du gradient à pas optimal :
– on prend $x_0 \in \mathbb{R}^n$,
– pour $k \in \mathbb{N}$, on pose $x_{k+1} = x_k + t_k d_k$ avec $d_k := -\nabla f(x_k) = b - Ax_k$ et t_k l'unique réel positif minimisant $t \mapsto f(x_k + td_k)$.

Théorème.
La suite $(x_k)_{k\in\mathbb{N}}$ ainsi définie converge vers $\bar{x}$.

Démonstration. Dans toute la preuve on notera $\|\cdot\|_A$ la norme issue du produit scalaire $(x, y) \mapsto \langle Ax, y\rangle$. On supposera aussi $d_k \neq 0$ pour tout k (sinon la suite $(x_k)_{k\in\mathbb{N}}$ est stationnaire en $\bar{x}$).

On commence par donner l'expression de t_k :

$$f(x_k + td_k) = f(x_k) + \frac{t^2}{2}\langle Ad_k, d_k\rangle + t\langle Ax_k - b, d_k\rangle$$

qui est un polynôme du second degré en t, donc

$$t_k = \frac{\|d_k\|^2}{\|d_k\|_A^2}.$$

On a

$$\|x_{k+1} - \bar{x}\|_A^2 = \|x_k + t_k d_k - \bar{x}\|_A^2 = \|x_k - \bar{x}\|_A^2 + t_k^2\|d_k\|_A^2 + 2t_k\langle A(x_k - \bar{x}), d_k\rangle.$$

Or $A(x_k - \bar{x}) = Ax_k - b = -d_k$, donc

$$\begin{aligned}\|x_{k+1} - \bar{x}\|_A^2 &= \|x_k - \bar{x}\|_A^2 + \frac{\|d_k\|^4}{\|d_k\|_A^2} - 2\frac{\|d_k\|^4}{\|d_k\|_A^2} \\ &= \|x_k - \bar{x}\|_A^2 - \frac{\|d_k\|^4}{\|d_k\|_A^2}.\end{aligned}$$

On en déduit

$$\begin{aligned}\frac{\|x_{k+1} - \bar{x}\|_A^2}{\|x_k - \bar{x}\|_A^2} &= 1 - \frac{\|d_k\|^4}{\|d_k\|_A^2\|x_k - \bar{x}\|_A^2} \\ &= 1 - \frac{\|d_k\|^4}{\|d_k\|_A^2\|A^{-1}d_k\|_A^2} \\ &= 1 - \frac{\|d_k\|^4}{\|d_k\|_A^2\|d_k\|_{A^{-1}}^2}.\end{aligned}$$

On dispose alors du lemme suivant :

Lemme (Inégalité de Kantorovitch)**.**
Soit $A \in \mathcal{S}_n^{++}(\mathbb{R})$ de valeurs propres $\lambda_1 \leq \cdots \leq \lambda_n$. Alors

$$\forall x \in \mathbb{R}^n \setminus \{0\}, \quad \frac{\|x\|^4}{\|x\|_A^2\|x\|_{A^{-1}}^2} \geq 4\frac{\lambda_1\lambda_n}{(\lambda_1 + \lambda_n)^2}.$$

On en déduit

$$\begin{aligned}\|x_{k+1} - \bar{x}\|_A^2 &\leq \left(1 - 4\frac{\lambda_1\lambda_n}{(\lambda_1 + \lambda_n)^2}\right)\|x_k - \bar{x}\|_A^2 \\ &= \left(\frac{\lambda_1 - \lambda_n}{\lambda_1 + \lambda_n}\right)^2\|x_k - \bar{x}\|_A^2 \\ &= \left(\frac{1 - \mathrm{Cond}(A)}{1 + \mathrm{Cond}(A)}\right)^2\|x_k - \bar{x}\|_A^2\end{aligned}$$

avec $\mathrm{Cond}(A) = \frac{\lambda_n}{\lambda_1} \geq 1$. Or pour tout $x, \lambda_1\|x\|^2 \leq \langle Ax, x\rangle = \|x\|_A^2 \leq \lambda_n\|x\|^2$, d'où

$$\|x_k - \bar{x}\| \leq \left(\frac{1 - \mathrm{Cond}(A)}{1 + \mathrm{Cond}(A)}\right)^k \sqrt{\mathrm{Cond}(A)}\|x_0 - \bar{x}\|.$$

□

Démonstration de l'inégalité de Kantorovitch. Il suffit de montrer l'inégalité pour $\|x\| = 1$, ce que l'on suppose désormais.

A est symétrique donc il existe une base $(e_1, \ldots, e_n)$ orthonormale de vecteurs propres de A. Pour $x = \sum x_i e_i$, on a alors

$$\begin{aligned}
\langle Ax, x\rangle\langle A^{-1}x, x\rangle &= \sum_{i=1}^n \lambda_i x_i^2 \sum_{i=1}^n \frac{1}{\lambda_i} x_i^2 \\
&= \frac{\lambda_1}{\lambda_n} \sum_{i=1}^n \frac{\lambda_i}{\lambda_1} x_i^2 \sum_{i=1}^n \frac{\lambda_n}{\lambda_i} x_i^2 \\
&\leq \frac{\lambda_1}{4\lambda_n} \left(\sum_{i=1}^n \left(\frac{\lambda_i}{\lambda_1} + \frac{\lambda_n}{\lambda_i}\right) x_i^2\right)^2
\end{aligned}$$

car $ab \leq \frac{1}{4}(a+b)^2$. L'étude de la fonction $f : x \mapsto \frac{x}{\lambda_1} + \frac{\lambda_n}{x}$ montre qu'elle admet un maximum en λ_1 et en λ_n sur $[\lambda_1, \lambda_n]$, et on a $f(\lambda_1) = f(\lambda_n) = 1 + \frac{\lambda_n}{\lambda_1}$, on a donc

$$\begin{aligned}
\|x\|_A^2\|x\|_{A^{-1}}^2 &\leq \frac{\lambda_1}{4\lambda_n} \left(\sum_{i=1}^n \left(1 + \frac{\lambda_n}{\lambda_1}\right) x_i^2\right)^2 \\
&= \frac{\lambda_1}{4\lambda_n} \left(1 + \frac{\lambda_n}{\lambda_1}\right)^2 \\
&= \frac{(\lambda_1 + \lambda_n)^2}{4\lambda_1\lambda_n}.
\end{aligned}$$

□

2.16 Partition d'un entier en parts fixées

Référence :
– [FGN09b] page 194.

Théorème.
Soit $a_1, \ldots, a_k \in \mathbb{N}^*$ premiers entre eux dans leur ensemble.
Pour $n \in \mathbb{N}$, on pose

$$u_n = \mathrm{Card}\left\{(x_1, \ldots, x_k) \in \mathbb{N}^k \mid a_1x_1 + \cdots + a_kx_k = n\right\}.$$

Alors

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

Démonstration. On pose, lorsque cela a un sens,

$$f(z) = \sum_{n=0}^{+\infty} u_n z^n.$$

Pour tout $i \in \{1, \ldots, k\}$, la série entière $\sum_{x_i \in \mathbb{N}} z^{x_i a_i}$ a un rayon de convergence 1, donc le produit de Cauchy de ces k séries entières a un rayon de convergence ≥ 1. Or, pour tout $|z| < 1$,

$$\prod_{i=1}^{k} \left(\sum_{x_i=0}^{+\infty} z^{x_i a_i} \right) = \sum_{n=0}^{+\infty} \sum_{\substack{(x_1,\ldots,x_k) \in \mathbb{N}^k \\ a_1 x_1 + \cdots + a_k x_k = n}} z^n = f(z).$$

D'où, pour tout $|z| < 1$,

$$f(z) = \prod_{i=1}^{k} \frac{1}{1 - z^{a_i}}.$$

f est donc une fraction rationnelle de pôles les racines a_i-ièmes de l'unité. Le pôle 1 est de multiplicité k et tous les autres sont de multiplicité strictement inférieure à k. En effet, d'une part les polynômes $1 - z^{a_i}$ sont à racines simples et d'autre part, d'après le théorème de Bezout, il existe $u_1, \ldots, u_k$ tels que $\sum_{i=1}^{k} a_i u_i = 1$. Alors si ω est tel que $\omega^{a_1} = \ldots = \omega^{a_k} = 1$, on a

$$\omega = \omega^{\sum_{i=1}^{k} a_i u_i} = \prod_{i=1}^{k} (\omega^{a_i})^{u_i} = 1.$$

On note $\omega_1, \ldots, \omega_p$ les pôles de f avec $\omega_1 = 1$. Alors par décomposition de f en éléments simples, il existe, pour $1 \leq i \leq p$ et $1 \leq j \leq k-1$, $c_{ij} \in \mathbb{C}$ et $\alpha \in \mathbb{C}$ tels que pour tout $|z| < 1$,

$$f(z) = \frac{\alpha}{(1-z)^k} + \sum_{\substack{1 \leq i \leq p \\ 1 \leq j \leq k-1}} \frac{c_{ij}}{(\omega_i - z)^j}.$$

Or les coefficients de décomposition en série entière de $\frac{1}{(\omega - z)^j}$ s'obtiennent en dérivant $j-1$ fois la décomposition en série entière de $\frac{1}{\omega - z}$. On a

$$\frac{1}{\omega - z} = \frac{1}{\omega} \frac{1}{1 - \frac{z}{\omega}} = \sum_{n=0}^{+\infty} \frac{z^n}{\omega^{n+1}},$$

d'où

$$\frac{(j-1)!}{(\omega - z)^j} = \sum_{n=j-1}^{+\infty} \frac{n!}{(n-j+1)!} \frac{z^{n-j+1}}{\omega^{n+1}},$$

i.e.

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

On en déduit

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

Le premier terme est équivalent à $\frac{n^{k-1}}{(k-1)!}$ et les autres termes sont négligeables devant n^{k-1}, d'où

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

Il ne reste plus qu'à calculer α. Pour cela, on multiplie $f(z)$ par $(1-z)^k$ et on fait tendre z vers 1 :

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

d'où

$$\alpha = \frac{1}{a_i \cdots a_k}$$

et on obtient bien le résultat voulu. □

Remarque. On peut aussi remplacer toutes les séries entières par des séries formelles, ça permet de placer ce développement dans des leçons d'algèbre.

2.17 Prolongement méromorphe de Γ

Référence :
– [QZ06] page 314.
On définit la fonction Γ sur l'ouvert $\Omega := \{z \in \mathbb{C} \mid \operatorname{Re} z > 0\}$ par

$$\Gamma(z) = \int_0^{+\infty} t^{z-1} e^{-t} \, \mathrm{d}t.$$

Théorème.
La fonction Γ se prolonge en une fonction méromorphe sur $\mathbb{C}$ dont les pôles sont simples en $-n, n \in \mathbb{N}$, et n'admettant pas de zéro.

Démonstration. On désire appliquer le théorème d'holomorphie sous l'intégrale pour montrer que Γ est holomorphe sur Ω. D'une part, $z \mapsto t^{z-1}e^{-t}$ est holomorphe sur Ω. D'autre part, on a $|t^{z-1}e^{-t}| = t^{\operatorname{Re} z - 1}e^{-t}$ pour $t > 0$, donc si $\operatorname{Re} z \in [\varepsilon, M]$ avec $M > \varepsilon > 0$, alors pour $t \in]0,1[$,

$$|t^{z-1}e^{-t}| \leq t^{\varepsilon - 1}e^{-t} \in L^1([0,1])$$

et pour $t \in [1, +\infty[$,

$$|t^{z-1}e^{-t}| \leq t^M e^{-t} \in L^1([1, +\infty[)$$

donc on peut bien appliquer le théorème d'holomorphie sous l'intégrale.

Par intégration par parties, on obtient la relation $\Gamma(z+1) = z\Gamma(z)$ pour $z \in \Omega$. En posant $\Gamma(z) = \frac{\Gamma(z+1)}{z}$, on peut prolonger de proche en proche la fonction Γ en une fonction méromorphe sur $\mathbb{C}$. Pour établir les propriétés du théorème, nous allons montrer que Γ se prolonge en une fonction F méromorphe qui s'écrit sous la forme $F(z) = \frac{1}{G(z)}$ avec G holomorphe.

Lemme.
Pour $z \in \Omega$,

$$\Gamma(z) = \lim_{n \to +\infty} \frac{n^z n!}{z(z+1)\cdots(z+n)}.$$

Démonstration. On considère la suite de fonctions

$$f_n(t) := \mathbf{1}_{]0,n[}(t) \left(1 - \frac{t}{n}\right)^n t^{z-1}.$$

(f_n) converge simplement vers la fonction $f(t) := \mathbf{1}_{]0,+\infty[}e^{-t}t^{z-1}$. Par ailleurs, $1 - \frac{t}{n} \leq e^{-\frac{t}{n}}$ donc

$$|f_n(t)| \leq \mathbf{1}_{]0,n[}(t) \left(e^{-\frac{t}{n}}\right)^n t^{\operatorname{Re} z - 1} \leq \mathbf{1}_{]0,+\infty[}(t) e^{-t} t^{\operatorname{Re} z - 1}.$$

On peut donc appliquer le théorème de convergence dominée et on en déduit

$$\Gamma(z) = \int_0^{+\infty} t^{z-1}e^{-t}\,\mathrm{d}t = \lim_{n \to +\infty} \int_0^n t^{z-1}\left(1 - \frac{t}{n}\right)^n \mathrm{d}t.$$

On effectue le changement de variables $t = ns$ dans l'intégrale :

$$\Gamma(z) = \lim_{n \to +\infty} n^z \int_0^1 s^{z-1}(1-s)^n\,\mathrm{d}s = \lim_{n \to +\infty} n^z I_n(z).$$

Montrons par récurrence que, pour $z \in \Omega$,

$$I_n(z) = \frac{n!}{z(z+1)\cdots(z+n)}.$$

C'est vrai pour $n = 0$. Par ailleurs,

$$\begin{aligned} I_{n+1}(z) &= \int_0^1 s^{z-1}(1-s)^{n+1}\,\mathrm{d}s \\ &= \left[\frac{s^z}{z}(1-s)^{n+1}\right]_0^1 + \frac{n+1}{z}\int_0^1 s^z(1-s)^n\,\mathrm{d}s \\ &= \frac{n+1}{z} I_n(z+1) \\ &= \frac{(n+1)!}{z(z+1)\cdots(z+n+1)}. \end{aligned}$$

□

Posons, pour $z \in \mathbb{C}$ et $n \in \mathbb{N}$,

$$G_n(z) := \frac{z(z+1)\cdots(z+n)}{(n+1)^z n!} \quad \text{et} \quad G(z) := \lim_{n\to+\infty} G_n(z).$$

On a, pour $z \in \Omega$ tel que $\Gamma(z) \neq 0$, $\frac{1}{\Gamma(z)} = G(z)$. Montrons que G est bien définie sur $\mathbb{C}$ et que G est analytique. Pour cela, nous allons montrer que G est limite uniforme de fonctions holomorphes sur tout disque borné.

On a

$$(n+1)^{-z} = \prod_{k=1}^{n} \left(\frac{k+1}{k}\right)^{-z} = \prod_{k=1}^{n} e^{-z\ln\frac{k+1}{k}}$$

donc

$$G_n(z) = z\prod_{k=1}^{n}\left(1+\frac{z}{k}\right)e^{-z\ln\frac{k+1}{k}} = z\prod_{k=1}^{n} g_k(z)$$

où chaque g_k est holomorphe sur $\mathbb{C}$.

Soit $R > 0$ et $|z| < R$. Pour $n > R$ on écrit

$$G_n(z) = z\prod_{1\leq k\leq R} g_k(z)\prod_{R<k\leq n} g_k(z).$$

Pour $k > R$ on a $\frac{|z|}{k} < 1$ donc on peut écrire $g_k(z) = \exp\left(\text{Log}\,\left(1+\frac{z}{k}\right) - z\ln\left(1+\frac{1}{k}\right)\right)$, d'où

$$G_n(z) = z\left(\prod_{1\leq k<R} g_k(z)\right)\exp\left(\sum_{k=\lfloor R\rfloor+1}^{n}\left(\text{Log}\,\left(1+\frac{z}{k}\right) - z\ln\left(1+\frac{1}{k}\right)\right)\right).$$

Or

$$\left|\text{Log}\,\left(1+\frac{z}{k}\right) - z\ln\left(1+\frac{1}{k}\right)\right| \leq \frac{C}{k^2}$$

pour $k > R$ par développement limité, donc la série ci-dessus converge uniformément sur $D(0,R)$ vers une fonction holomorphe, il en est donc de même de (G_n). R étant arbitraire, cela prouve que G est holomorphe sur $\mathbb{C}$. De plus, $G(z) = z\prod_{k=1}^{+\infty} g_k(z)$ et le produit convergent $\prod_{k=1}^{+\infty} g_k$ a pour zéros les zéros des g_k, c'est-à-dire les $-k$ pour $k \in \mathbb{N}^*$. On en déduit que la fonction $F(z) := \frac{1}{G(z)}$ est méromorphe sur $\mathbb{C}$, sans zéros, et dont les pôles sont simples en les $-n$ pour $n \in \mathbb{N}$.

Par ailleurs,

$$F(z) = \lim_{n\to+\infty} \frac{n^z n!}{z(z+1)\cdots(z+n)}$$

donc F coïncide avec Γ sur Ω, F est donc le prolongement méromorphe de Γ sur $\mathbb{C}$. □

2.18 Réduction de Frobenius

Référence :
– [Gou09] page 290.

Théorème.
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n.
Soit $u \in \mathcal{L}(E)$.
Alors il existe une suite $F_1, \dots, F_r$ de sous-espaces vectoriels de E non réduits à $\{0\}$ et stables par u telle que :

(i) $E = F_1 \oplus \dots \oplus F_r$

(ii) $\forall i \in \{1, \dots, r\}, u_i := u_{|F_i}$ *est un endomorphisme cyclique*

(iii) si P_i désigne le polynôme minimal de u_i, on a :

$$\forall i \in \{1, \dots, r-1\}, P_{i+1} \mid P_i$$

La suite de polynômes $P_1, \dots, P_r$ ne dépend que de u. On l'appelle suite des invariants de similitude de u.

On a alors l'existence d'une base $\mathcal{B}$ de E telle que

$$Mat_{\mathcal{B}}(u) = \begin{pmatrix} C(P_1) & & 0 \\ & \ddots & \\ 0 & & C(P_r) \end{pmatrix}$$

où $C(P_i)$ désigne la matrice compagnon de P_i.
On a $P_1 = \pi_u$ et $P_1 \dots P_r = \chi_u$.

Lemme.
Soit $u \in \mathcal{L}(E)$ un endomorphisme cyclique.
Alors il existe une base de E dans laquelle la matrice de u est égale à $C(\pi_u)$.

Démonstration. Il existe $x \in E$ tel que $(x, u(x), \dots, u^{n-1}(x))$ soit une base de E. On en déduit que π_u, le polynôme minimal de u, est de degré n (il est de degré au plus n par Cayley-Hamilton).
Si $\pi_u = X^n + a_{n-1}X^{n-1} + \dots + a_0$, on a alors $u^n(x) = -a_{n-1}u^{n-1}(x) - \dots - a_0 x$ car π_u annule u. □

Démonstration du théorème. La forme matricielle obtenue se déduit immédiatement du lemme.

– Existence : soit $k = \deg(\pi_u)$, soit $x \in E$.
On note P_x le polynôme unitaire engeandrant l'idéal :

$$\{P \in \mathbb{K}[X] \ / \ P(u)(x) = 0\}$$

et

$$E_x := \{P(u)(x) \ / \ P \in \mathbb{K}[X]\}.$$

Soit $x \in E$ tel que $P_x = \pi_u$ (une preuve de l'existence d'un tel x est donnée en fin de document).
Le sous-espace vectoriel $F := E_x$ est de dimension k et est stable par u.
On pose :

$$e_1 = x, e_2 = u(x), \ldots, e_k = u^{k-1}(x).$$

Alors $(e_1, \ldots, e_k)$ forme une base de F car $\deg(P_x) = k$ (plus de détails sont donnés en fin de document).
On complète $(e_1, \ldots, e_k)$ en une base $(e_1, \ldots, e_n)$ et on considère la base duale $(e_1^*, \ldots, e_n^*)$.

On note $G = \Gamma^\circ$ où $\Gamma = \text{vect}(\{ {}^t u^i(e_k^*), i \in \mathbb{N}\})$ (orthogonal vis-à-vis du dual).
G est un sev de E stable par u car Γ est stable par ${}^t u$.
Montrons $F \oplus G = E$:

– $F \cap G = \{0\}$:
On remarque que l'on a, pour $i + j \leq k$,

$$\begin{aligned} \langle {}^t u^i(e_k^*), e_j \rangle &= \langle e_k^*, u^i(e_j) \rangle \\ &= \langle e_k^*, e_{i+j} \rangle \\ &= \delta_{i+j,k}. \end{aligned} \tag{2.3}$$

Donc si $y \in F \cap G$, $\langle {}^t u^i(e_k^*), y \rangle = e_{k-i}^*(y) = 0$ pour $0 \leq i \leq k-1$, donc $y = 0$.

– $\dim F + \dim G = n$:
On a $\pi_{{}^t u} = \pi_u$ donc $\dim \Gamma \leq k$ (on peut aussi dire que $(\text{id}, u, \ldots, u^k)$ est liée donc $(e_k^*, {}^t u(e_k^*), \ldots, {}^t u^k(e_k^*))$ aussi), donc $\dim G = n - \dim \Gamma \geq n - k$.
D'où $\dim F + \dim G \geq n$, d'où le résultat.

On note P_1 le polynôme minimal de $u_{|F}$ ($\pi_u = P_x = P_1$) et P_2 le polynôme minimal de $u_{|G}$, on a $P_2 \mid P_1$ car $P_1 = \pi_u$.
Puis on recommence sur $u_{|G}$.

– Unicité : soient $F_1, \ldots, F_r$ et $G_1, \ldots, G_s$ vérifiant les hypothèses du théorème.
On note $P_i = \pi_{u_{|F_i}}$ et $Q_j = \pi_{u_{|G_j}}$.

Supposons $(P_1, \ldots, P_r) \neq (Q_1, \ldots, Q_s)$.
On note $p = \inf\{i, P_i \neq Q_i\}$, p existe car $\sum_i \deg(P_i) = n = \sum_j \deg(Q_j)$ et $\deg(P_i), \deg(Q_j) \neq 0$.

$$P_p(u)(E) = P_p(u)(F_1) \oplus \ldots \oplus P_p(u)(F_{p-1})$$

car $E = F_1 \oplus \ldots \oplus F_r$ et $P_p(u)(F_k) = 0$ pour $k \geq p$ et les F_i sont stables par u.

Or

$$P_p(u)(E) = P_p(u)(G_1) \oplus \ldots \oplus P_p(u)(G_s)$$

et

$$\dim P_p(u)(F_i) = \dim P_p(u)(G_i) \text{ pour } 1 \leq i \leq p-1$$

car d'après le lemme, il existe $\mathcal{B}_i$ et $\mathcal{B}'_i$ telles que $\mathrm{Mat}_{\mathcal{B}_i}(u_{|F_i}) = \mathrm{Mat}_{\mathcal{B}'_i}(u_{|G_i})$. D'où :

$$0 = \dim P_p(u)(G_p) = \ldots = \dim P_p(u)(G_s)$$

D'où $Q_p \mid P_p$, donc $Q_p = P_p$ par symétrie.

□

Détails supplémentaires

Proposition.
Si $k = \deg(\pi_u)$, $\mathcal{L}_u := \{P(u) \mid P \in \mathbb{K}[X]\}$ est un sev de $\mathcal{L}(E)$ de dimension k, dont une base est $(Id_E, u, \ldots, u^{k-1})$.

Si $l = \deg(P_x)$, E_x est un sev de E de dimension l, dont une base est $(x, \ldots, u^{l-1}(x))$.

Démonstration.

$$\begin{aligned} \varphi : \mathbb{K}[X] &\longrightarrow \mathcal{L}(E) \\ P &\longmapsto P(u) \end{aligned}$$

est linéaire, $\mathrm{Im}\,\varphi = \mathcal{L}_u$.

$$\ker \varphi = \{P \in \mathbb{K}[X] \ / \ P(u) = 0\} = (\pi_u)$$

Donc

$$\mathcal{L}_u \cong \mathbb{K}[X]/(\pi_u)$$

dont une base est $(1, X, \ldots, X^{k-1})$

Idem avec

$$\begin{aligned} \varphi : \mathbb{K}[X] &\longrightarrow E \\ P &\longmapsto P(u)(x) \end{aligned}$$

□

Proposition.
Il existe $x \in E$ tel que $P_x = \pi_u$.

Démonstration. Soit $\pi_u = Q_1^{\alpha_1} \ldots Q_l^{\alpha_l}$ avec Q_i irréductible unitaire, $\alpha_i > 0$.

– soit $i \in \{1, \ldots, l\}$, soit R tel que $\pi_u = Q_i^{\alpha_i} R$.

$$0 = \pi_u(u) = Q_i^{\alpha_i}(u) \circ R(u)$$

Donc

$$\operatorname{Im} R(u) \subseteq \ker Q_i^{\alpha_i}(u)$$

Si

$$\operatorname{Im} R(u) \subseteq \ker Q_i^{\alpha_i - 1}(u)$$

alors

$$Q_i^{\alpha_i - 1}(u) \circ R(u) = 0$$

donc $\pi_u \mid Q_i^{\alpha_i - 1} R$, or $\deg Q_i^{\alpha_i - 1} R < \deg \pi_u$, donc il existe $a_i \in \operatorname{Im} R(u)$ tel que $Q_i^{\alpha_i - 1}(u)(a_i) \neq 0$.
Mais $Q_i^{\alpha_i}(u)(a_i) = 0$ donc $P_{a_i} \mid Q_i^{\alpha_i}$, donc $P_{a_i} = Q_i^{\alpha_i}$ car $P_{a_i} \nmid Q_i^{\alpha_i - 1}$ et Q_i est irréductible.
En résumé, pour $1 \leq i \leq l$, il existe $a_i \in E$ tel que $P_{a_i} = Q_i^{\alpha_i}$.

– Montrons que :

$$P_x \wedge P_y = 1 \Longrightarrow P_{x+y} = P_x P_y$$

On a

$$P_x P_y(u)(x + y) = P_x P_y(u)(x) + P_x P_y(u)(y) = 0$$

Donc $P_{x+y} \mid P_x P_y$.
D'autre part,

$$P_{x+y}(u)(y) = -P_{x+y}(u)(x)$$

Donc

$$P_x P_{x+y}(u)(y) = -P_x P_{x+y}(u)(x) = 0$$

Donc $P_y \mid P_x P_{x+y}$ et $P_x \wedge P_y = 1$ donc $P_y \mid P_{x+y}$.
De même, $P_x \mid P_{x+y}$ donc $P_x P_y \mid P_{x+y}$ car $P_x \wedge P_y = 1$.
D'où $P_x P_y = P_{x+y}$.

– Alors pour $1 \leq i \leq l$, il existe a_i tel que $P_{a_i} = Q_i^{\alpha_i}$ et $Q_i^{\alpha_i} \wedge Q_j^{\alpha_j} = 1$ pour $i \neq j$, donc :

$$P_{\sum_{i=1}^{l} a_i} = \prod_{i=1}^{l} P_{a_i} = \pi_u$$

□

2.19 Sous-espaces de $\mathcal{C}(\mathbb{R},\mathbb{C})$ de dimension finie stables par translations

Référence :
– [Lei99b] page 92.

Théorème.
Soit F un sous-espace vectoriel de $\mathcal{C}(\mathbb{R},\mathbb{C})$ de dimension finie. Pour $a\in\mathbb{R}$, on définit $\tau_a : f\mapsto f(\cdot - a)$ endomorphisme de $\mathcal{C}(\mathbb{R},\mathbb{C})$.

Alors F est stable par tous les endomorphismes $\tau_a, a\in\mathbb{R}$ et de dimension n si et seulement si F est l'espace des solutions d'une équation différentielle linéaire homogène d'ordre n à coefficients constants.

Démonstration. Si F est l'espace des solutions d'une équation différentielle linéaire homogène d'ordre n à coefficients constants, alors F est un sous-espace vectoriel de $\mathcal{C}(\mathbb{R},\mathbb{C})$ de dimension n d'après le théorème de Cauchy-Lipschitz linéaire. De plus, un tel espace est bien stable par translations.

Supposons désormais que F est stable par translations. On commence par montrer que $F\subset\mathcal{C}^\infty(\mathbb{R},\mathbb{C})$.

Soit $(f_1,\dots,f_n)$ une base de F. Pour $a\in\mathbb{R}$ et $i\in\{1,\dots,n\}$, on a $\tau_{-a}f_i\in F$ donc il existe des scalaires $\lambda_{i,1}(a),\dots,\lambda_{i,n}(a)$ tels que

$$\forall x\in\mathbb{R},\quad f_i(x+a)=\sum_{k=1}^{n}\lambda_{i,k}(a)f_k(x). \tag{2.4}$$

Pour $x\in\mathbb{R}$, on note $F_k(x)=\int_0^x f_k(t)\,\mathrm{d}t$. En intégrant 2.4, on a

$$\int_0^x f_i(t+a)\,\mathrm{d}t=\sum_{k=1}^{n}\lambda_{i,k}(a)F_k(x),$$

d'où

$$F_i(x+a)-F_i(a)=\sum_{k=1}^{n}\lambda_{i,k}(a)F_k(x).$$

Les f_i sont linéairement indépendants donc les F_i aussi. On dispose alors du lemme suivant :

Lemme.
Soit $h_1,\dots,h_n$ des fonctions de $\mathbb{R}$ dans $\mathbb{C}$ linéairement indépendantes. Alors il existe des réels $x_1,\dots,x_n$ tels que la matrice $(h_i(x_j))_{1\leq i,j\leq n}$ soit inversible.

Soit donc $x_1,\dots,x_n\in\mathbb{R}$ tels que $A:=(F_i(x_j))_{1\leq i,j\leq n}$ soit inversible. Par la relation $F_i(x_j+a)-F_i(a)=\sum_{k=1}^n\lambda_{i,k}(a)F_k(x_j)$, on obtient $B(a)=\Lambda(a)A$ avec $B(a):=(F_i(x_j+a)-F_i(a))_{1\leq i,j\leq n}$ et $\Lambda(a):=(\lambda_{i,j}(a))_{1\leq i,j\leq n}$.

On a donc $\Lambda(a)=B(a)A^{-1}$ pour tout $a\in\mathbb{R}$. Les f_i sont continues donc les F_i sont de classe $\mathcal{C}^1$ et donc l'application $a\mapsto B(a)$ aussi. On en déduit que

$a \mapsto \Lambda(a)$ est de classe $\mathcal{C}^1$ et donc que les $\lambda_{i,j}$ sont de classe $\mathcal{C}^1$. En prenant $x = 0$ dans 2.4, on a

$$f_i(a) = \sum_{k=1}^{n} \lambda_{i,k}(a) f_k(0)$$

donc les f_i sont de classe $\mathcal{C}^1$. Par récurrence, on en déduit que les f_i sont de classe $\mathcal{C}^\infty$, donc $F \subset \mathcal{C}^\infty(\mathbb{R}, \mathbb{C})$.

En dérivant 2.4 par rapport à a en 0, on a, pour tout $x \in \mathbb{R}$,

$$f_i'(x) = \sum_{k=1}^{n} \lambda_{i,k}'(0) f_k(x).$$

On en déduit $f_i' \in F$ pour tout i, *i.e.* F est stable par l'endomorphisme D de dérivation.
Soit μ le polynôme minimal de $D_{|F}$, on note $d := \deg \mu$ ($d \leq n$). On a $F \subset \ker \mu(D)$, or d'après le théorème de Cauchy-Lipschitz linéaire, $\ker \mu(D)$ est un sous-espace de $\mathcal{C}(\mathbb{R}, \mathbb{C})$ de dimension d, on doit donc avoir $d = n$ et donc $F = \ker \mu(D)$. □

Démonstration du lemme. On note $K := \text{vect}(h_1, \ldots, h_n)$ et, pour $x \in \mathbb{R}$, δ_x la forme linéaire $f \mapsto f(x)$ sur K. Soit $\Gamma := \{\delta_x \mid x \in \mathbb{R}\}$ et $G := \text{vect}(\Gamma) \subset K^*$. On a $G^\circ = \Gamma^\circ = \{0\}$, donc $G = K^*$.

On en déduit que Γ engendre K^*, et donc qu'il existe $x_1, \ldots, x_n \in \mathbb{R}$ tels que $(\delta_{x_1}, \ldots, \delta_{x_n})$ soit une base de K^*. La matrice de passage de la base duale des h_i à la base des δ_{x_i} est $(h_i^{**}(\delta_{x_j}))_{1 \leq i,j \leq n}$, or $h_i^{**}(\delta_{x_j}) = \delta_{x_j}(h_i) = h_i(x_j)$, d'où le résultat. □

2.20 Sous-groupes compacts de $GL_n(\mathbb{R})$

Référence :
– [Ale99] pages 141 et 160.

Théorème.
Tout sous-groupe compact de $GL_n(\mathbb{R})$ est conjugué à sous-groupe de $O_n(\mathbb{R})$.

Lemme.
Soit E un $\mathbb{R}$-espace vectoriel de dimension finie, K un convexe compact de E et H un sous-groupe compact de $GL(E)$.
Si K est stable par H, alors il existe $a \in K$ fixé par tous les éléments de H.

Démonstration. Soit $\|\cdot\|$ une norme euclidienne sur E. Pour $x \in E$, on définit

$$N(x) := \sup_{u \in H} \|u(x)\| = \max_{u \in H} \|u(x)\|,$$

l'existence du maximum étant garantie par compacité de H.

Alors N est une norme sur E :

– Si $N(x) = 0$, on a $\|\mathrm{id}_E(x)\| = 0$, d'où $x = 0$.
– $N(\lambda x) = |\lambda| N(x)$.
– Finalement,

$$\begin{aligned} N(x+y) &= \max_{u\in H} \|u(x+y)\| \\ &\leq \max_{u\in H} (\|u(x)\| + \|u(y)\|) \\ &\leq \max_{u\in H} \|u(x)\| + \max_{u\in H} \|u(y)\| \\ &= N(x) + N(y). \end{aligned}$$

De plus, N est invariante par H : $N(v(x)) = N(x)$ pour tout $v \in H$ car $u \mapsto u \circ v$ est une bijection de H.
Enfin, montrons que N est une norme strictement convexe.
Soit $x, y \in E$ tels que $N(x+y) = N(x) + N(y)$. Soit $u_0 \in H$ tel que $N(x+y) = \|u_0(x+y)\|$. On a alors

$$N(x+y) = \|u_0(x) + u_0(y)\| \leq \|u_0(x)\| + \|u_0(y)\| \leq N(x) + N(y) = N(x+y),$$

d'où $\|u_0(x) + u_0(y)\| = \|u_0(x)\| + \|u_0(y)\|$ et donc $u_0(x)$ et $u_0(y)$ sont positivement liés car $\|\cdot\|$ est une norme euclidienne, il en est donc de même de x et y par linéarité et inversibilité de u_0.

K étant compact, il existe $a \in K$ de norme minimale pour N. De plus, a est unique. En effet, si a' est de norme minimale pour N, alors $\frac{a+a'}{2} \in K$ car K est convexe et

$$N(a) \leq N\left(\frac{a+a'}{2}\right) \leq \frac{N(a) + N(a')}{2} = N(a)$$

donc a et a' sont positivement liés donc égaux car de même norme.

Pour $v \in H$ on a $v(a) \in K$ car K est stable par H et $N(v(a)) = N(a)$ donc $v(a) = a$, ce qui montre que a est fixe par tous les éléments de H. □

Démonstration du théorème. Soit G un sous-groupe compact de $GL_n(\mathbb{R})$. Alors G agit sur l'espace E des matrices symétriques par congruence, ce qui définit l'antimorphisme suivant :

$$\begin{aligned} \rho : G &\longrightarrow GL(E) \\ A &\longmapsto (\rho_A : S \mapsto {}^tASA) \end{aligned}$$

Cet antimorphisme est de plus continu, donc le groupe $H := \rho(G)$ est un sous-groupe compact de $GL(E)$.

Par ailleurs, l'orbite de I_n, qui est l'ensemble $\mathcal{E} := \{ {}^tMM \mid M \in G\}$, est un compact de E donc son enveloppe convexe K est compacte d'après le théorème de Carathéodory. De plus $\mathcal{E} \subset \mathcal{S}_n^{++}(\mathbb{R})$ et $\mathcal{S}_n^{++}(\mathbb{R})$ est convexe donc $K \subset \mathcal{S}_n^{++}(\mathbb{R})$. Enfin, K est stable par H :

$$\rho_A({}^tMM) = {}^t(MA)(MA) \in \mathcal{E}$$

et les éléments de K sont combinaisons linéaires d'éléments de $\mathcal{E}$.

On peut donc appliquer le lemme : il existe $S \in \mathcal{S}_n^{++}(\mathbb{R})$ fixé par tous les éléments de H, *i.e.* ${}^tASA = S$ pour tout $A \in G$. G est donc contenu dans le groupe orthogonal de la forme quadratique associée à S, et donc G est conjugué à un sous-groupe de $O_n(\mathbb{R})$. □

Détails supplémentaires

Proposition.
Soit q une forme quadratique associée à $S \in \mathcal{S}_n^{++}(\mathbb{R})$.
Si $G \subset O(q)$, alors G est conjugué à un sous-groupe de $O_n(\mathbb{R})$.

Démonstration. $S \in \mathcal{S}_n^{++}(\mathbb{R})$ donc il existe $T \in \mathcal{S}_n^{++}(\mathbb{R})$ tel que $S = T^2$.
Alors, pour $A \in G$,

$$\begin{aligned} S &= {}^tASA \\ T^2 &= {}^tAT^2A \\ I_n &= (T^{-1}\,{}^tAT)(TAT^{-1}) \\ I_n &= {}^t(TAT^{-1})(TAT^{-1}) \end{aligned}$$

D'où $TAT^{-1} \in O_n(\mathbb{R})$. □

2.21 Sous-groupes finis de $SO(3, \mathbb{R})$

Références :
– [Ulm12] page 138 ;
– [RWM10].

Théorème.
Tout sous-groupe fini de $SO(3)$ est isomorphe à l'un des groupes suivants : $\mathbb{Z}/n\mathbb{Z}, D_n, \mathfrak{A}_4, \mathfrak{S}_4, \mathfrak{A}_5$.

Démonstration. Soit G un tel groupe d'ordre $n \geq 2$, G agit sur $\mathbb{S}^2$. Un élément de $G \setminus \{\mathrm{id}\}$ est une rotation axiale donc possède 2 points fixes pour cette action, appelés pôles. On note X l'ensemble des pôles d'éléments de $G \setminus \{\mathrm{id}\}$, on a $2 \leq |X| \leq 2(n-1)$.
X est stable par G car si x est un pôle de g, alors $h(x)$ est un pôle de hgh^{-1}. Par ailleurs, si $x \in X$, le stabilisateur G_x de x est, par restriction à $\mathrm{vect}(x)^\perp$, un sous-groupe fini de $SO(2)$ donc est cyclique.

On considère l'action de G sur X, alors si r désigne le nombre d'orbites, la formule de Burnside donne

$$r = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix(g)}| = \frac{1}{n}(|X| + 2(n-1))$$

et puisque $2 \leq |X| \leq 2(n-1)$, on obtient $r = 2$ ou 3.

Supposons qu'il y ait deux orbites. Alors la formule de Burnside donne

$$2 = \frac{1}{n}(|X_1| + |X_2| + 2(n-1)),$$

d'où $|X_1| + |X_2| = 2$, *i.e.* $|X_1| = |X_2| = 1$. Il y a donc un pôle dans chaque orbite et donc tous les éléments de $G \setminus \{\mathrm{id}\}$ admettent le même axe de rotation, donc G est cyclique.

Supposons désormais qu'il y ait trois orbites. En notant n_i le cardinal du stabilisateur d'un élément d'une orbite X_i, avec $n_1 \leq n_2 \leq n_3$, on a d'une part $n_i \geq 2$ et d'autre part la formule de Burnside donne

$$3 = \frac{1}{n}\left(\frac{n}{n_1} + \frac{n}{n_2} + \frac{n}{n_3} + 2(n-1)\right),$$

d'où

$$\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} = 1 + \frac{2}{n}.$$

On en déduit $\frac{3}{n_1} > 1$, d'où $n_1 = 2$. D'où

$$\frac{1}{n_2} + \frac{1}{n_3} = \frac{1}{2} + \frac{2}{n}. \tag{2.5}$$

Par conséquent, $\frac{2}{n_2} > \frac{1}{2}$ et donc $n_2 = 2$ ou 3.
Si $n_2 = 2$, alors $\frac{1}{n_3} = \frac{2}{n}$ et donc $n_3 = \frac{n}{2}$ et n est pair. Si $n_2 = 3$, alors $\frac{1}{n_3} = \frac{1}{6} + \frac{2}{n}$, d'où $\frac{1}{n_3} > \frac{1}{6}$, donc $n_3 \in \{3, 4, 5\}$.

En résumé, la relation (2.5) donne les cas suivants :

1. $n_1 = n_2 = 2, n_3 = \frac{n}{2}$.
2. $n_1 = 2, n_2 = n_3 = 3$, alors $n = 12$.
3. $n_1 = 2, n_2 = 3, n_3 = 4$, alors $n = 24$.
4. $n_1 = 2, n_2 = 3, n_3 = 5$, alors $n = 60$.

Identifions la structure de G dans chacun des cas :

1. Si $n = 4$, alors $G \simeq \mathbb{Z}/4\mathbb{Z}$ ou $G \simeq D_2$.
   Supposons $n \neq 4$. Soit $z \in X_3$ et $x \in X_1$, alors $G_z = G_{-z}$ donc $|\mathrm{Orb}(-z)| = |\mathrm{Orb}(z)| = 2$ et donc $X_3 = \{z, -z\}$ puisque c'est la seule orbite de cardinal 2 ($n \neq 4$). Les rotations de G qui ne fixent pas z sont donc des rotations d'angle π dont les pôles sont dans le plan $\{z\}^\perp$, qui s'identifient à des symétries axiales dans ce plan. G s'identifie ainsi, par restriction à $\{z\}^\perp$, à un sous-groupe fini de $O(2)$.
   G_z est cyclique d'ordre $\frac{n}{2}$, soit g un générateur de G_z. Considérons

   $$P := (g^i(x))_{0 \leq i \leq \frac{n}{2}-1},$$

   alors x n'est pas fixé par une rotation de G_z donc P forme un polygône régulier à $\frac{n}{2}$ côtés dans le plan $\{z\}^\perp$ et $|X_1| = \frac{n}{2}$ donc $P = X_1$.
   G agit sur P donc par égalité des cardinaux, $G \simeq D_{n/2}$.

2. L'action de G sur X_2 est fidèle car $|X_2| = 4$ et seule l'identité a un plan de points fixes dans $SO(3)$. D'où un morphisme injectif $G \to \mathfrak{S}_4$ et par cardinalité, $G \simeq \mathfrak{A}_4$.

3. On a $|X_2| = 8$ et si $z \in X_2$, alors $-z \in X_2$ car $|G_z| = |G_{-z}|$ et les orbites sont de cardinaux distincts. G permute donc les paires de points opposés de X_2, ce qui induit un morphisme $\varphi : G \to \mathfrak{S}_4$.

   Supposons que φ ne soit pas injectif et soit $g \in \ker\varphi$ non trivial. Alors g laisse stable les paires donc g^2 admet tout X_2 comme points fixes et donc $g^2 = \mathrm{id}$. Par ailleurs, les deux points fixes c et $-c$ de g ne sont pas dans X_2 car les stabilisateurs d'éléments de X_2 sont d'ordre divisant 3, donc si $z \in X_2$, $g(z) = -z$.

   Soit $h \in G$, alors $hgh^{-1} \in \ker\varphi$ est non trivial et donc g et hgh^{-1} ont même restriction à X_2 et donc $hgh^{-1}g^{-1}$ a 8 points fixes, donc $g = hgh^{-1}$. Or les points fixes de hgh^{-1} sont $h(c)$ et $h(-c)$ donc $\{c, -c\}$ est stable par G. Ceci n'est pas possible car il n'y a pas d'orbite de cardinal 2. Par conséquent, φ est injectif et par cardinalité, $G \simeq \mathfrak{S}_4$.

4. On a $|X_1| = 30$ et $n_1 = 2$, $|X_2| = 20$ et $n_2 = 3$, $|X_3| = 12$ et $n_3 = 5$. Les pôles opposés appartenant à la même orbite, les 30 pôles de X_1 fournissent 15 axes de rotation distincts et donc 15 sous-groupes d'ordre 2 qui sont conjugués entre eux comme stabilisateurs d'éléments d'une même orbite. On obtient de même 10 sous-groupes d'ordre 3 conjugués et 6 sous-groupes d'ordre 5 conjugués et on vérifie que ces sous-groupes sont les seuls sous-groupes de G par cardinalité.

   Montrons alors que G est simple. Soit H un sous-groupe distingué de G non trivial et distinct de G.

   Si $5 \mid |H|$, H contient les 24 éléments d'ordre 5 car il est distingué, donc $|H| = 30$ et donc H contient aussi les 15 éléments d'ordre 2, ce qui n'est pas possible.

   Si $2 \mid |H|$, alors H contient les 15 éléments d'ordre 2 donc $|H| \geq 16$, donc $|H| \in \{20, 30\}$, donc $5 \mid |H|$ ce qui n'est pas possible.

   Finalement $|H| = 3$, or H doit contenir les 20 éléments d'ordre 3, ce qui n'est pas possible.

   Donc G est simple et $|G| = 60$ donc $G \simeq \mathfrak{A}_5$.

□

2.22 Surjectivité de l'exponentielle matricielle

Référence :
– [Zav13]

Théorème.
La fonction $\exp : \mathcal{M}_n(\mathbb{C}) \longrightarrow GL_n(\mathbb{C})$ *est surjective.*

Lemme.
Soit G un groupe topologique et H un sous-groupe de G contenant un voisinage de e. Alors H est ouvert et fermé, en particulier H contient la composante connexe de e.

Démonstration. Soit V un voisinage de e dans H, alors pour $h \in H$, hV est un voisinage de h dans H et donc H est ouvert. On a d'autre part

$$H^c = \bigcup_{g \notin H} gH$$

donc H^c est ouvert en tant qu'union d'ouverts, donc H est fermé. □

Démonstration du théorème. Soit $M \in \mathcal{M}_n(\mathbb{C})$. Alors $\mathbb{C}[M]$ est un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{C})$ de dimension finie donc est fermé. Or pour tout $N \in \mathbb{N}$ et pour tout $X \in \mathbb{C}[M]$,$\sum_{n=0}^{N} \frac{1}{n!} X^n \in \mathbb{C}[M]$, donc $\exp(X) \in \mathbb{C}[M]$.
Par ailleurs, $\exp(X) \in GL_n(\mathbb{C})$ car d'inverse $\exp(-X)$, donc l'application

$$\begin{aligned} \varphi : \mathbb{C}[M] &\longrightarrow \mathbb{C}[M]^\times \\ X &\longmapsto \exp(X) \end{aligned}$$

est bien définie et est un morphisme de groupes car les éléments de $\mathbb{C}[M]$ commutent. En notant $H := \mathrm{Im}(\varphi)$, H est donc un sous-groupe du groupe topologique $\mathbb{C}[M]^\times$. Pour montrer que $H = \mathbb{C}[M]^\times$, il suffit donc par le lemme de montrer que H contient un voisinage de I_n et que $\mathbb{C}[M]^\times$ est connexe.

Pour montrer que H contient un voisinage de I_n, nous allons appliquer le théorème d'inversion locale. L'application φ est de classe $\mathcal{C}^1$ et on a

$$\begin{aligned} \varphi(H) &= \exp(H) \\ &= I_n + H + o(\|H\|) \\ &= \varphi(0) + H + o(\|H\|). \end{aligned}$$

La différentielle en 0 de φ est donc l'identité. De plus, $\mathbb{C}[M]^\times$ est ouvert dans $\mathbb{C}[M]$ car $\mathbb{C}[M]^\times = \mathbb{C}[M] \cap GL_n(\mathbb{C})$ donc, d'après le théorème d'inversion locale, φ réalise un $\mathcal{C}^1$-difféomorphisme entre un voisinage de 0 dans $\mathbb{C}[M]$ et un voisinage de I_n dans $\mathbb{C}[M]^\times$. H contient donc un voisinage de I_n.

Il suffit maintenant de montrer que $\mathbb{C}[M]^\times$ est connexe. Soit $A, B \in \mathbb{C}[M]^\times$, alors $P(z) := \det(zA + (1-z)B)$ est un polynôme non nul donc l'ensemble Z de ses racines est fini. $\mathbb{C} \setminus Z$ est connexe par arcs et contient 0 et 1 donc il existe un chemin γ reliant 0 à 1 dans $\mathbb{C} \setminus Z$. Le chemin $\gamma(t)A + (1-\gamma(t))B$ relie alors B à A dans $\mathbb{C}[M]^\times$.

Pour montrer que l'exponentielle est surjective, on prend $M \in GL_n(\mathbb{C})$, on a alors $M \in \mathbb{C}[M]^\times$ donc, par ce qui a été fait précédemment, il existe $A \in \mathbb{C}[M]$ tel que $\exp(A) = M$. □

Proposition.
Soit $A \in GL_n(\mathbb{R})$, alors il existe $M \in \mathcal{M}_n(\mathbb{R})$ telle que $\exp(M) = A$ si et seulement s'il existe $B \in \mathcal{M}_n(\mathbb{R})$ telle que $A = B^2$.

Démonstration. Si $\exp(M) = A$, alors $\left(\exp\left(\frac{M}{2}\right)\right)^2 = A$.

Soit $B \in \mathcal{M}_n(\mathbb{R})$ telle que $B^2 = A \in GL_n(\mathbb{R})$. Alors $B \in GL_n(\mathbb{R})$ car de déterminant non nul, donc il existe $Q \in \mathbb{C}[X]$ telle que $\exp(Q(B)) = B$. Or $B = \overline{B} = \exp(\overline{Q}(B))$, donc $A = B \times \overline{B} = \exp(Q(B) + \overline{Q}(B))$ car $Q(B)$ et $\overline{Q}(B)$ commutent. Or $Q + \overline{Q} \in \mathbb{R}[X]$, d'où le résultat. □

Exemple. $A := \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$ n'a pas d'antécédent dans $\mathcal{M}_2(\mathbb{R})$ par exp. Supposons qu'il existe $B \in \mathcal{M}_2(\mathbb{R})$ telle que $\exp(B) = A$, alors si λ est valeur propre de B, $\exp\lambda$ est valeur propre de A donc $\lambda = i\pi + 2ik\pi$ pour $k \in \mathbb{Z}$. Donc $\lambda \neq \bar{\lambda}$, or B est réelle donc $\bar{\lambda}$ est aussi valeur propre de B, donc B est diagonalisable. On en déduit que A est diagonalisable, ce qui est absurde.

On pouvait aussi donner une matrice de déterminant négatif, car $\det\exp(B) = \exp(\mathrm{tr}(B)) > 0$ pour $B \in \mathcal{M}_n(\mathbb{R})$.

2.23 Table de caractères de $\mathfrak{S}_4$

Référence :
– [RWM10].

On commence par déterminer les classes de conjugaison de $\mathfrak{S}_4$, qui sont caractérisées par le profil des permutations. On obtient alors :
– l'identité, seule dans sa classe,
– les transpositions, au nombre de $\binom{4}{2} = 6$,
– les 3-cycles, au nombre de $2 \times \binom{3}{4} = 8$,
– les 4-cycles, au nombre de $3! = 6$,
– les double-transpositions, au nombre de 3.

Nous savons alors que $\mathfrak{S}_4$ admet à isomorphisme près 5 représentations irréductibles.

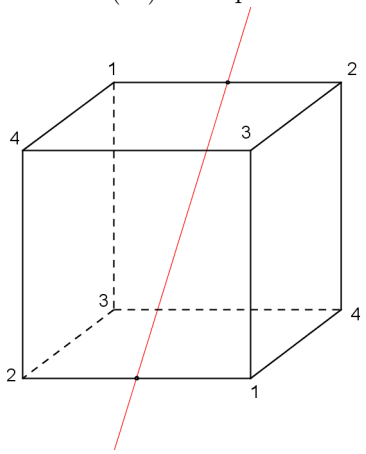
La représentation triviale et la représentation signature donnent deux représentations irréductibles de degré 1, de caractères respectifs $\chi_1 = (1, 1, 1, 1, 1)$ et $\chi_\varepsilon = (1, -1, 1, -1, 1)$, où l'ordre des classes de conjugaison dans les colonnes est celui donné précédemment.

On considère la représentation ρ_p par permutation de $\mathfrak{S}_4$. Elle n'est pas irréductible car la droite $\mathcal{D} := \mathrm{vect}(1, 1, 1, 1)$ et son orthogonal $\mathcal{H} := \{(x_1, x_2, x_3, x_4) \in \mathbb{C}^4 \mid \sum_{i=1}^4 x_i = 0\}$ sont stables.
ρ_p induit sur $\mathcal{D}$ la représentation triviale et sur $\mathcal{H}$ une représentation ρ_s de degré 3. On a alors $\chi_p = \chi_1 + \chi_s$, or la valeur de $\chi_p(\sigma)$ pour $\sigma \in \mathfrak{S}_4$ correspond au nombre de points fixes de σ, d'où $\chi_p = (4, 2, 1, 0, 0)$, et donc $\chi_s = (3, 1, 0, -1, -1)$.
Vérifions que χ_s est irréductible :

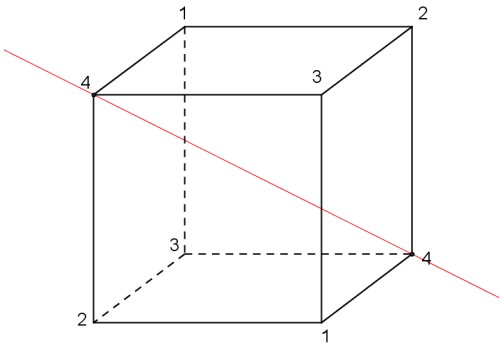
$$\langle \chi_s, \chi_s \rangle = \frac{1}{24}(1 \times 3^2 + 6 \times 1^2 + 8 \times 0^2 + 6 \times (-1)^2 + 3 \times (-1)^2) = 1.$$

Le groupe des isométries positives conservant le cube est isomorphe à $\mathfrak{S}_4$ et cet isomorphisme se réalise via les permutations des grandes diagonales, cela

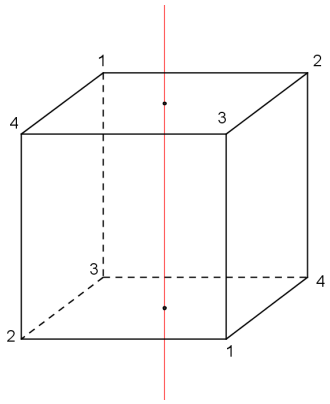
nous donne donc une représentation de degré 3 de $\mathfrak{S}_4$ de caractère χ_c.
La permutation (12) correspond à une rotation d'angle π :



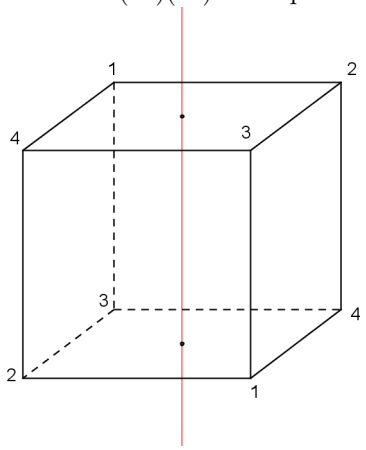
d'où $\chi_c((12)) = 1 + 2\cos\pi = -1$.
La permutation (123) correspond à une rotation d'angle $\frac{2\pi}{3}$:



d'où $\chi_c((123)) = 1 + 2\cos(\frac{2\pi}{3}) = 0$.
La permutation (1234) correspond à une rotation d'angle $\frac{\pi}{2}$:



d'où $\chi_c((1234)) = 1 + 2\cos(\frac{\pi}{2}) = 1$.
La permutation $(13)(24)$ correspond à une rotation d'angle π :



d'où $\chi_c((13)(24)) = 1 + 2\cos(\pi) = -1$.
Finalement, $\chi_c = (3, -1, 0, 1, -1)$ et on a comme précédemment que $\langle \chi_c, \chi_c \rangle = 1$, donc χ_c est irréductible.

On a pour l'instant :

	1 Id	6 (12)	8 (123)	6 (1234)	3 (12)(34)
χ_1	1	1	1	1	1
χ_ε	1	-1	1	-1	1
χ_s	3	1	0	-1	-1
χ_c	3	-1	0	1	-1

Pour déterminer la dernière représentation irréductible, on utilise, en notant n_i les degrés des représentations, la relation $\sum_{i=1}^{5} n_i = 24$ qui nous donne $n_5 = 2$ et la relation $\sum_{i=1}^{5} n_i \chi_i(\sigma) = 0$ pour $\sigma \neq \mathrm{Id}$ qui nous permet de compléter la

table. On obtient alors :

	1	6	8	6	3
	Id	(12)	(123)	(1234)	(12)(34)
χ_1	1	1	1	1	1
χ_ε	1	-1	1	-1	1
χ_s	3	1	0	-1	-1
χ_c	3	-1	0	1	-1
χ_5	2	0	-1	0	2

2.24 Table de caractères du groupe diédral D_n

Référence :

– [Pey04] page 227.

On commence par rappeler la définition et les propriétés du groupe diédral D_n.

D_n est le sous-groupe de $O(2,\mathbb{R})$ engendré par la rotation r d'angle $\frac{2\pi}{n}$ et par la symétrie axiale s d'axe vect$\begin{pmatrix}1\\0\end{pmatrix}$. Puisque r et s engendrent D_n, une représentation ρ est déterminée par la donnée de $\rho(r)$ et $\rho(s)$. De plus, les éléments r et s vérifient les relations suivantes :

$$r^n = s^2 = (rs)^2 = \mathrm{id}$$

et les éléments de D_n sont de la forme r^k ou $r^k s$ avec $k \in \{0,\dots,n-1\}$.

On suppose d'abord n pair.

On s'intéresse en premier lieu aux représentations de degré 1. Le caractère d'une représentation de degré 1 doit vérifier $\chi(s)^2 = 1, \chi(rs)^2 = 1$ et $\chi(r)^n = 1$. La dernière condition est redondante car n est pair, on doit donc avoir $\chi(s) = \pm 1$ et $\chi(r) = \pm 1$. On obtient alors les 4 caractères suivants :

	r^k	$r^k s$
χ_1	1	1
χ_2	1	-1
χ_3	$(-1)^k$	$(-1)^k$
χ_4	$(-1)^k$	$(-1)^{k+1}$

Pour étudier les représentations de degré 2, on définit, pour $h \in \mathbb{N}$, la représentation ρ_h par

$$\rho_h(r) = \begin{pmatrix} \cos\left(\frac{2\pi h}{n}\right) & -\sin\left(\frac{2\pi h}{n}\right) \\ \sin\left(\frac{2\pi h}{n}\right) & \cos\left(\frac{2\pi h}{n}\right) \end{pmatrix} \quad \text{et} \quad \rho_h(s) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

On vérifie que ces applications définissent bien des représentations de D_n. On a alors

$$\rho_h(r^k) = \begin{pmatrix} \cos\left(\frac{2\pi hk}{n}\right) & -\sin\left(\frac{2\pi hk}{n}\right) \\ \sin\left(\frac{2\pi hk}{n}\right) & \cos\left(\frac{2\pi hk}{n}\right) \end{pmatrix} \quad \text{et} \quad \rho_h(r^k s) = \begin{pmatrix} \cos\left(\frac{2\pi hk}{n}\right) & \sin\left(\frac{2\pi hk}{n}\right) \\ \sin\left(\frac{2\pi hk}{n}\right) & -\cos\left(\frac{2\pi hk}{n}\right) \end{pmatrix}.$$

De plus, on peut prendre $h \in \{0, \dots, n-1\}$ et les représentations ρ_h et ρ_{n-h} sont isomorphes car :

$$\forall g \in D_n, \quad \rho_h(g) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \rho_{n-h}(g) \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^{-1}.$$

On considère donc les représentations ρ_h pour $h \in \{0, \dots, \frac{n}{2}\}$.

Par ailleurs, ρ_0 est réductible car $\text{vect}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ est stable. De même, $\rho_{n/2}$ est réductible par stabilité de la même droite. Montrons que les autres représentations ρ_h sont bien irréductibles. Si ce n'était pas le cas, il existerait une droite stable par tous les $\rho_h(g)$, donc en particulier par $\rho_h(s)$. Il s'agirait donc de $\text{vect}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ou de $\text{vect}\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, or ces droites ne sont pas stables par $\rho_h(r)$:

$$\begin{pmatrix} \cos\left(\frac{2\pi h}{n}\right) & -\sin\left(\frac{2\pi h}{n}\right) \\ \sin\left(\frac{2\pi h}{n}\right) & \cos\left(\frac{2\pi h}{n}\right) \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\left(\frac{2\pi h}{n}\right) \\ \sin\left(\frac{2\pi h}{n}\right) \end{pmatrix}$$

et $\sin\left(\frac{2\pi h}{n}\right) \neq 0$ pour $h \in \{1, \dots, \frac{n}{2} - 1\}$, de même pour $\text{vect}\begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

On obtient ainsi les $\frac{n}{2} - 1$ caractères irréductibles :

	r^k	$r^k s$
χ_h	$2\cos\left(\frac{2\pi hk}{n}\right)$	0

Les caractères étant distincts, les représentations ne sont pas isomorphes.

On vérifie maintenant qu'on a obtenu toutes les représentations en calculant la somme des carrés des degrés des représentations : $4 \times 1^2 + (\frac{n}{2} - 1) \times 2^2 = 2n = |D_n|$.

On regarde désormais le cas où n est impair.

On ne peut ici avoir que deux représentations de degré 1 :

	r^k	$r^k s$
χ_1	1	1
χ_2	1	-1

On définit ensuite les représentations ρ_h de degré 2 comme dans le cas pair, elles sont irréductibles et non isomorphes deux à deux pour $h \in \{1, \dots, \frac{n-1}{2}\}$. On calcule alors la somme des carrés des degrés et on obtient $2 \times 1 + \frac{n-1}{2} \times 2^2 = 2n = |D_n|$.

Exemple

Étudions le cas de D_4. On a ici 4 caractères irréductibles de degré 1 et $\frac{4}{2} - 1 = 1$ caractère irréductible de degré 2.

	id	r	r^2	r^3	s	rs	r^2s	r^3s
χ_1	1	1	1	1	1	1	1	1
χ_2	1	1	1	1	-1	-1	-1	-1
χ_3	1	-1	1	-1	1	-1	1	-1
χ_4	1	-1	1	-1	-1	1	-1	1
χ_5	2	0	-2	0	0	0	0	0

On trouve alors les classes de conjugaison $\{\mathrm{id}\}, \{r, r^3\}, \{r^2\}, \{s, r^2s\}$ et $\{rs, r^3s\}$ ainsi que les sous-groupes distingués de D_4 : D_4, $\{\mathrm{id}\}$, $\{\mathrm{id}, r^2\}$, $\{\mathrm{id}, r, r^2, r^3\}$, $\{\mathrm{id}, r^2, s, r^2s\}$ et $\{\mathrm{id}, r^2, rs, r^3s\}$.

2.25 Théorème d'Abel angulaire et théorème taubérien faible

Référence :
– [Gou94] page 249.

Théorème (Abel angulaire)**.**
Soit $\sum a_n z^n$ une série entière de rayon de convergence ≥ 1 et de somme f telle que $\sum a_n$ converge. Pour $\theta_0 \in [0, \frac{\pi}{2}[$, on pose

$$\Delta_{\theta_0} := \{z \in D \mid \exists \rho > 0, \exists \theta \in [-\theta_0, \theta_0], \quad z = 1 - \rho e^{i\theta}\},$$

où D désigne le disque unité ouvert de $\mathbb{C}$. Alors

$$\lim_{\substack{z \to 1 \\ z \in \Delta_{\theta_0}}} f(z) = \sum_{n=0}^{+\infty} a_n.$$

Démonstration. On pose

$$S_n := \sum_{k=0}^{n} a_k, \quad S := \sum_{n=0}^{+\infty} a_n, \quad R_n := S - S_n.$$

Pour $z \in D$, on effectue une transformation d'Abel en écrivant $a_n = R_{n-1} - R_n$:

$$\begin{aligned}
\sum_{n=0}^{N} a_n z^n - S_N &= \sum_{n=1}^{N} (R_{n-1} - R_n)(z^n - 1) \\
&= \sum_{n=0}^{N-1} R_n(z^{n+1} - 1) - \sum_{n=0}^{N} R_n(z^n - 1) \\
&= \sum_{n=0}^{N-1} R_n(z^{n+1} - z^n) - R_N(z^N - 1)
\end{aligned}$$

$$\sum_{n=0}^{N} a_n z^n - S_N = (z-1)\sum_{n=0}^{N-1} R_n z^n - R_N(z^N - 1).$$

$\lim_{N\to+\infty} R_N = 0$ car $\sum a_n$ converge donc, en passant à la limite,

$$f(z) - S = (z-1)\sum_{n=0}^{+\infty} R_n z^n.$$

Soit désormais $\varepsilon > 0$ et $N \in \mathbb{N}$ tel que pour tout $n \geq N$, $|R_n| < \varepsilon$. Alors, pour tout $z \in D$,

$$\begin{aligned} |f(z) - S| &\leq |z-1| \left| \sum_{n=0}^{N} R_n z^n \right| + \varepsilon |z-1| \sum_{n=N+1}^{+\infty} |z|^n \\ &\leq |z-1| \sum_{n=0}^{N} |R_n| + \varepsilon \frac{|z-1|}{1-|z|}. \end{aligned}$$

Pour z suffisamment proche de 1, on aura $|z-1|\sum_{n=0}^{N} |R_n| < \varepsilon$, donc il suffit de borner $\frac{|z-1|}{1-|z|}$ au voisinage de 1 dans Δ_{θ_0} pour obtenir le résultat.

Pour $z \in \Delta_{\theta_0}$, on peut écrire $z = 1 - \rho e^{i\theta}$ avec $\rho > 0$ et $|\theta| \leq \theta_0$. On a alors $|z|^2 = 1 - 2\rho\cos\theta + \rho^2$, d'où

$$\begin{aligned} \frac{|z-1|}{1-|z|} &= \frac{|z-1|}{1-|z|^2}(1+|z|) \\ &= \frac{\rho}{2\rho\cos\theta - \rho^2}(1+|z|) \\ &\leq \frac{2}{2\cos\theta - \rho}. \end{aligned}$$

On a donc, pour $\rho \leq \cos\theta_0$,

$$\frac{|z-1|}{1-|z|} \leq \frac{2}{2\cos\theta_0 - \cos\theta_0} = \frac{2}{\cos\theta_0}.$$

Pour z suffisamment proche de 1, on a donc

$$|f(z) - S| \leq \varepsilon \left(1 + \frac{2}{\cos\theta_0}\right),$$

d'où le résultat. □

Théorème (Taubérien faible)**.**
Soit $\sum a_n z^n$ une série entière de rayon de convergence 1 et de somme f. On suppose

$$\exists S \in \mathbb{C}, \quad \lim_{\substack{x\to 1 \\ x<1}} f(x) = S.$$

Si $a_n = o\left(\frac{1}{n}\right)$, alors $\sum a_n$ converge et $\sum_{n=0}^{+\infty} a_n = S$.

Démonstration. Pour $n \in \mathbb{N}$, on note $S_n := \sum_{k=0}^{n} a_k$. Pour $x \in]0,1[$, on a

$$S_n - f(x) = \sum_{k=0}^{n} a_k(1-x^k) - \sum_{k=n+1}^{+\infty} a_k x^k.$$

Or

$$1 - x^k = (1-x)\sum_{i=0}^{k-1} x^i \leq k(1-x) \quad \text{car } 0 < x < 1,$$

donc

$$\begin{aligned} |S_n - f(x)| &\leq (1-x)\sum_{k=0}^{n} k|a_k| + \sum_{k=n+1}^{+\infty} \frac{k|a_k|}{n} x^k \\ &\leq (1-x)Mn + \frac{1}{n(1-x)} \sup_{k>n} k|a_k|, \end{aligned}$$

où M désigne un majorant de la suite $(k|a_k|)$, qui existe car $a_k = o\left(\frac{1}{k}\right)$. Pour $0 < \varepsilon < 1$, on a alors

$$\left|S_n - f\left(1 - \frac{\varepsilon}{n}\right)\right| \leq M\varepsilon + \frac{1}{\varepsilon} \sup_{k>n} k|a_k|.$$

Donc il existe $N_0 \in \mathbb{N}$ tel que pour tout $n \geq N_0$,

$$\left|S_n - f\left(1 - \frac{\varepsilon}{n}\right)\right| \leq M\varepsilon + \varepsilon = (M+1)\varepsilon.$$

Par ailleurs, $\lim_{x \to 1^-} f(x) = S$ donc il existe $N_1 \geq N_0$ tel que pour tout $n \geq N_1$,

$$\left|f\left(1 - \frac{\varepsilon}{n}\right) - S\right| < \varepsilon.$$

On en déduit que pour tout $n \geq N_1$,

$$|S_n - S| \leq \left|S_n - f\left(1 - \frac{\varepsilon}{n}\right)\right| + \left|f\left(1 - \frac{\varepsilon}{n}\right) - S\right| \leq (M+1)\varepsilon + \varepsilon = (M+2)\varepsilon,$$

d'où le résultat. □

2.26 Théorème de Banach – Steinhaus

Références :
- [Bre05] page 16.
- [Gou08] page 404.

Théorème.
Soit E un espace de Banach et F un espace vectoriel normé. Soit $(T_i)_{i \in I}$ une famille d'opérateurs linéaires et continus de E dans F. On suppose que

$$\forall x \in E, \quad \sup_{i \in I} \|T_i x\| < \infty.$$

Alors

$$\sup_{i\in I} \|T_i\| < \infty.$$

Démonstration. Pour $n \geq 1$, on pose

$$X_n := \{x \in E \mid \forall i \in I, \|T_i x\| \leq n\}.$$

Alors X_n est fermé car les T_i sont continus, et par hypothèse on a $\bigcup_{n\in\mathbb{N}^*} X_n = E$.

D'après le lemme de Baire, il existe n_0 tel que $\overset{\circ}{X_{n_0}} \neq \varnothing$. Soit $x_0 \in E$ et $r > 0$ tel que $B(x_0, r) \subset X_{n_0}$, on a alors

$$\forall i \in I, \forall z \in B(0,1), \quad \|T_i(x_0 + rz)\| \leq n_0.$$

On en déduit

$$r\|T_i\| \leq n_0 + \|T_i x_0\|,$$

ce qui permet de conclure. □

Corollaire.
On note $\mathcal{C}_{2\pi}$ le $\mathbb{C}$-ev des fonctions continues 2π-périodiques à valeurs complexes muni de la norme $\|\cdot\|_\infty$. Pour $f \in \mathcal{C}_{2\pi}$, on définit

$$\forall n \in \mathbb{Z}, c_n(f) := \frac{1}{2\pi}\int_{-\pi}^{\pi} f(t)e^{-int}\,\mathrm{d}t \quad \textit{et} \quad \forall n \geq 0, S_n(f) : x \mapsto \sum_{k=-n}^{n} c_k(f)e^{ikx}.$$

Alors il existe une fonction $f \in \mathcal{C}_{2\pi}$ telle que $(S_n(f)(0))_{n\in\mathbb{N}}$ diverge.

Démonstration. Soit

$$\begin{aligned} \ell_n : \mathcal{C}_{2\pi} &\longrightarrow \mathbb{C} \\ f &\longmapsto S_n(f)(0) = \sum_{k=-n}^{n} c_k(f). \end{aligned}$$

Alors ℓ_n est une forme linéaire continue sur $\mathcal{C}_{2\pi}$. En effet, si $f \in \mathcal{C}_{2\pi}$, on a

$$\begin{aligned} \ell_n(f) &= \sum_{k=-n}^{n} \frac{1}{2\pi}\int_{-\pi}^{\pi} f(t)e^{-ikt}\,\mathrm{d}t \\ &= \frac{1}{2\pi}\int_{-\pi}^{\pi} f(t)\sum_{k=-n}^{n} e^{-ikt}\,\mathrm{d}t \\ &= \frac{1}{2\pi}\int_{-\pi}^{\pi} f(t)D_n(t)\,\mathrm{d}t \end{aligned}$$

où $D_n(t) = \sum_{k=-n}^{n} e^{-ikt} = \frac{\sin((2n+1)t/2)}{\sin(t/2)}$. D'où

$$|\ell_n(f)| \leq \frac{\|f\|_\infty}{2\pi}\int_{-\pi}^{\pi} |D_n(t)|\,\mathrm{d}t,$$

c'est-à-dire

$$\|\ell_n\| \leq \frac{1}{2\pi}\int_{-\pi}^{\pi} |D_n(t)|\,\mathrm{d}t.$$

Le but est maintenant de montrer qu'il existe $f \in \mathcal{C}_{2\pi}$ tel que $\sup_{n\in\mathbb{N}} |\ell_n(f)| = +\infty$ donc, en appliquant le théorème de Banach – Steinhaus, il suffit de montrer que $\sup_{n\in\mathbb{N}} \|\ell_n\| = +\infty$. Montrons

$$\|\ell_n\| = \frac{1}{2\pi}\int_{-\pi}^{\pi} |D_n(t)|\,\mathrm{d}t.$$

Pour $\varepsilon > 0$, on définit

$$\begin{aligned} f_\varepsilon : \mathbb{R} &\longrightarrow \mathbb{C} \\ x &\longmapsto \frac{D_n(x)}{|D_n(x)| + \varepsilon}. \end{aligned}$$

On a $\|f_\varepsilon\|_\infty \leq 1$ et, par théorème de convergence dominée,

$$|\ell_n(f_\varepsilon)| \xrightarrow[\varepsilon\to 0]{} \frac{1}{2\pi}\int_{-\pi}^{\pi} |D_n(t)|\,\mathrm{d}t.$$

On a donc

$$\|\ell_n\| = \frac{1}{2\pi}\int_{-\pi}^{\pi} |D_n(t)|\,\mathrm{d}t.$$

On a alors

$$\begin{aligned} \|\ell_n\| &\geq \frac{1}{\pi}\int_0^{\pi} \left|\frac{\sin((2n+1)t/2)}{t/2}\right| \mathrm{d}t \\ &= \frac{2}{\pi}\int_0^{(2n+1)\pi/2} \left|\frac{\sin(t)}{t}\right| \mathrm{d}t \\ &\xrightarrow[n\to+\infty]{} +\infty \text{ car } t \mapsto \frac{\sin(t)}{t} \text{ n'est pas intégrable.} \end{aligned}$$

$(\mathcal{C}_{2\pi}, \|\cdot\|_\infty)$ est un espace de Banach, donc par le théorème de Banach – Steinhaus, il existe $f \in \mathcal{C}_{2\pi}$ tel que $\sup_{n\in\mathbb{N}} |\ell_n(f)| = +\infty$, c'est-à-dire

$$\sup_{n\in\mathbb{N}} S_n(f)(0) = +\infty.$$

Donc $(S_n(f)(0))_{n\in\mathbb{N}}$ diverge. □

2.27 Théorème de Bernstein

Référence :
– [QZ06] page 518.

Théorème.
Soit $f : [0,1] \to \mathbb{C}$ une fonction continue. On pose

$$\omega(h) := \sup\{|f(u) - f(v)|, |u - v| \leq h\}$$

son module de continuité.
On considère

$$B_n(f,x) = B_n(x) := \sum_{k=0}^{n} \binom{n}{k} x^k (1-x)^{n-k} f\left(\frac{k}{n}\right)$$

le $n^{ième}$ polynôme de Bernstein de f.
Alors

(i) *(B_n) converge uniformément vers f sur $[0,1]$.*

(ii) *$\|f - B_n\|_\infty \leq C\omega\left(\frac{1}{\sqrt{n}}\right)$ où C est une constante.*

(iii) *L'estimation (ii) est optimale : il existe f lipschitzienne telle que $\|f - B_n\|_\infty \geq \frac{\delta}{\sqrt{n}}$ pour une constante $\delta > 0$.*

Démonstration. (i) Soit $x \in [0,1]$ et $(X_i)_{i\geq 1}$ une suite de variables de Bernoulli i.i.d de paramètre x. On note $S_n := X_1 + \cdots + X_n$.
On a alors

$$\mathbb{E}\left(f\left(\frac{S_n}{n}\right)\right) = B_n(x) \text{ et } \mathbb{E}(f(x)) = f(x)$$

par théorème de transfert, d'où

$$\begin{aligned} |f(x) - B_n(x)| &= \left|\mathbb{E}\left(f(x) - f\left(\frac{S_n}{n}\right)\right)\right| \\ &\leq \mathbb{E}\left(\left|f(x) - f\left(\frac{S_n}{n}\right)\right|\right). \end{aligned}$$

f est continue sur $[0,1]$ compact donc uniformément continue par le théorème de Heine, donc $\omega(\delta)$ est défini pour tout $\delta > 0$ et $\lim_{\delta\to 0} \omega(\delta) = 0$. Par ailleurs, $|f(x) - f\left(\frac{S_n}{n}\right)| \leq 2\|f\|_\infty$ donc, pour $\delta > 0$,

$$\mathbb{E}\left|f(x) - f\left(\frac{S_n}{n}\right)\right| \leq \omega(\delta)\mathbb{P}\left(\left|x - \frac{S_n}{n}\right| \leq \delta\right) + 2\|f\|_\infty \mathbb{P}\left(\left|x - \frac{S_n}{n}\right| > \delta\right).$$

Par l'inégalité de Tchebychev, on a alors

$$\begin{aligned} \mathbb{P}\left(\left|x - \frac{S_n}{n}\right| > \delta\right) &\leq \frac{\mathrm{Var}\left(\frac{S_n}{n}\right)}{\delta^2} \\ &= \frac{\mathrm{Var}(S_n)}{n^2\delta^2} \\ &= \frac{x(1-x)}{n\delta^2} \\ &\leq \frac{1}{4n\delta^2}. \end{aligned}$$

On en déduit que, pour tout $x \in [0,1]$,

$$|f(x) - B_n(x)| \leq \omega(\delta) + \frac{\|f\|_\infty}{2n\delta^2},$$

d'où

$$\limsup_{n\to+\infty} \|f - B_n\|_\infty \leq \omega(\delta).$$

Le résultat vient de $\lim_{\delta\to 0} \omega(\delta) = 0$.

(ii) Affinons le résultat de convergence uniforme prouvé ci-dessus. On a d'abord

$$\mathbb{E}\left|f(x) - f\left(\frac{S_n}{n}\right)\right| \leq \mathbb{E}\omega\left(\left|x - \frac{S_n}{n}\right|\right).$$

Montrons que $\omega(\lambda h) \leq (\lambda+1)\omega(h)$:
ω est croissante et $\omega(h+k) \leq \omega(h)+\omega(k)$ donc, par récurrence, $\omega(nh) \leq n\omega(h)$ pour $n \in \mathbb{N}$. On a alors, pour $\lambda \in \mathbb{R}, \omega(\lambda h) \leq \omega(\lceil\lambda\rceil h) \leq \lceil\lambda\rceil\omega(h) \leq (\lambda+1)\omega(h)$.
On en déduit

$$\begin{aligned}
|f(x) - B_n(x)| &\leq \omega\left(\frac{1}{\sqrt{n}}\right)\mathbb{E}\left(\sqrt{n}\left|x - \frac{S_n}{n}\right| + 1\right) \\
&= \omega\left(\frac{1}{\sqrt{n}}\right)\left(1 + \sqrt{n}\left\|x - \frac{S_n}{n}\right\|_1\right) \\
&\leq \omega\left(\frac{1}{\sqrt{n}}\right)\left(1 + \sqrt{n}\left\|x - \frac{S_n}{n}\right\|_2\right)
\end{aligned}$$

par l'inégalité de Hölder. Or

$$\begin{aligned}
\left\|x - \frac{S_n}{n}\right\|_2^2 &= \mathbb{E}\left(\left|x - \frac{S_n}{n}\right|^2\right) \\
&= \mathrm{Var}\left(x - \frac{S_n}{n}\right) + \left(\mathbb{E}\left(x - \frac{S_n}{n}\right)\right)^2 \\
&= \frac{1}{n^2}nx(1-x) + \left(x - \frac{1}{n}nx\right)^2 \\
&= \frac{x(1-x)}{n}.
\end{aligned}$$

D'où

$$\begin{aligned}
|f(x) - B_n(x)| &\leq \omega\left(\frac{1}{\sqrt{n}}\right)\left(1 + \sqrt{n}\sqrt{\frac{x(1-x)}{n}}\right) \\
&\leq \frac{3}{2}\omega\left(\frac{1}{\sqrt{n}}\right).
\end{aligned}$$

D'où $\|f - B_n\|_\infty \leq \frac{3}{2}\omega\left(\frac{1}{\sqrt{n}}\right)$.

(iii) On pose $f : x \mapsto \left|x - \frac{1}{2}\right|$, on a $\omega(h) \leq h$. Par ailleurs,

$$\begin{aligned}\|f - B_n\|_\infty &\geq \left|f\left(\frac{1}{2}\right) - B_n\left(\frac{1}{2}\right)\right| \\ &= \left|B_n\left(\frac{1}{2}\right)\right| \\ &= \mathbb{E}\left|\frac{S_n}{n} - \frac{1}{2}\right| \\ &= \frac{1}{2n}\mathbb{E}|2S_n - n|.\end{aligned}$$

D'où $\|f - B_n\|_\infty \geq \frac{1}{2n}\mathbb{E}|\varepsilon_1 + \cdots + \varepsilon_n|$ avec $\varepsilon_j := 2X_j - 1$ variables de Rademacher i.i.d. D'où

$$\begin{aligned}\|f - B_n\|_\infty &\geq \frac{1}{2n}\|\varepsilon_1 + \cdots + \varepsilon_n\|_1 \\ &\geq \frac{1}{2n\sqrt{e}}\|\varepsilon_1 + \cdots + \varepsilon_n\|_2\end{aligned}$$

par inégalité de Khintchine.
Or $\|\varepsilon_1 + \cdots + \varepsilon_n\|_2^2 = \mathrm{Var}(\varepsilon_1 + \cdots + \varepsilon_n) + (\mathbb{E}(\varepsilon_1 + \cdots + \varepsilon_n))^2 = n$. D'où

$$\|f - B_n\|_\infty \geq \frac{1}{2\sqrt{ne}} \geq \frac{1}{2\sqrt{e}}\omega\left(\frac{1}{\sqrt{n}}\right).$$

□

Détails supplémentaires

Proposition (Inégalité de Khintchine)**.**
*Soit $\varepsilon_1, \ldots, \varepsilon_n$ des variables de Rademacher (*i.e. *valant ± 1 avec probabilité $\frac{1}{2}$) i.i.d. Soit $f \in vect_{\mathbb{R}}(\varepsilon_1, \ldots, \varepsilon_n)$.*
Alors $\|f\|_2 \leq \sqrt{e}\mathbb{E}(|f|)$.

Démonstration. On a $f = \sum_j a_j\varepsilon_j$ et on peut supposer $\|f\|_2^2 = 1 = \sum_j a_j^2$.
Posons $g := \prod_{j=1}^n (1 + ia_j\varepsilon_j)$. Alors pour presque tout x,

$$\begin{aligned}|g(x)| &= \prod_{j=1}^n \sqrt{1 + a_j^2\varepsilon_j^2(x)} \\ &= \prod_{j=1}^n \sqrt{1 + a_j^2} \\ &\leq \prod_{j=1}^n \sqrt{\exp(a_j^2)} \\ &= \sqrt{\exp\left(\sum a_j^2\right)} \\ &= \sqrt{e}.\end{aligned}$$

D'où $\|g\|_\infty \leq \sqrt{e}$.

De plus, si $j \in \{1, \ldots, n\}$,

$$\begin{aligned}\mathbb{E}(\varepsilon_j g) &= \mathbb{E}\left(\varepsilon_j(1+ia_j\varepsilon_j)\prod_{k\neq j}(1+ia_k\varepsilon_k)\right)\\ &= \mathbb{E}(\varepsilon_j(1+ia_j\varepsilon_j))\mathbb{E}\left(\prod_{k\neq j}(1+ia_k\varepsilon_k)\right) \text{ par indépendance des } \varepsilon_j\end{aligned}$$

$$\begin{aligned}\mathbb{E}(\varepsilon_j g) &= \mathbb{E}(\varepsilon_j(1+ia_j\varepsilon_j))\prod_{k\neq j}\mathbb{E}(1+ia_k\varepsilon_k)\\ &= ia_j \text{ car } \mathbb{E}(\varepsilon_j) = 0.\end{aligned}$$

Or $\mathbb{E}(fg) = \sum_{j=1}^n a_j\mathbb{E}(\varepsilon_j g)$, d'où $|\mathbb{E}(fg)| = \left|i\sum_{j=1}^n a_j^2\right| = 1$.
Or

$$\|f\|_1 \geq \frac{|\mathbb{E}(fg)|}{\|g\|_\infty} \geq \frac{1}{\sqrt{e}}.$$

□

2.28 Théorème de Cartan – Von Neumann

Référence :
– [GT98] page 83.

Théorème.
Tout sous-groupe fermé de $GL_n(\mathbb{R})$ est une sous-variété de $GL_n(\mathbb{R})$.

Démonstration. Soit G un sous-groupe fermé de $GL_n(\mathbb{R})$, il s'agit de montrer que tout point de G admet un voisinage difféomorphe à un ouvert d'un espace vectoriel. Or G est un groupe et la translation $h \mapsto gh$ est un $\mathcal{C}^\infty$-difféomorphisme, donc il suffit de montrer cette propriété au voisinage de I_n.
Plus précisément, nous allons montrer qu'il existe un sous-espace vectoriel F de $\mathcal{M}_n(\mathbb{R})$, deux voisinages ouverts U et V de 0 et I_n respectivement dans $\mathcal{M}_n(\mathbb{R})$ et un $\mathcal{C}^\infty$-difféomorphisme $\varphi : U \to V$ tel que $\varphi(U \cap F) = V \cap G$.

Étape 1 : Définition de F.

On pose

$$\mathcal{L}_G := \{m \in \mathcal{M}_n(\mathbb{R}) \mid \forall t \in \mathbb{R}, e^{tm} \in G\}.$$

Montrons que $\mathcal{L}_G$ est un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{R})$.

Puisque $0 \in \mathcal{L}_G$ et $(m \in \mathcal{L}_G, \lambda \in \mathbb{R}) \Rightarrow \lambda m \in G$, il reste à montrer que $\mathcal{L}_G$ est stable par addition. Soit donc $a, b \in \mathcal{L}_G$, montrons que

$$\lim_{k \to +\infty} \underbrace{\left(e^{a/k} e^{b/k}\right)^k}_{\in G} = e^{a+b},$$

ce qui permettra de conclure car G est fermé.

Par le développement limité de l'exponentielle, on a

$$e^{a/k} e^{b/k} = I_n + \frac{a+b}{k} + o\left(\frac{1}{k}\right).$$

Par ailleurs, $D\exp(0) = \mathrm{id}$ donc, d'après le théorème d'inversion locale, exp réalise un $\mathcal{C}^1$-difféomorphisme d'un voisinage de 0 sur un voisinage de I_n dans $\mathcal{M}_n(\mathbb{R})$. En notant L sa réciproque, on a $DL(I_n) = D\exp(0)^{-1} = \mathrm{id}$ donc $L(I_n + m) = m + o(\|m\|)$ pour m au voisinage de 0.

Il vient alors, pour k suffisamment grand,

$$\left(e^{a/k} e^{b/k}\right)^k = \exp\left(kL\left(I_n + \frac{a+b}{k} + o\left(\frac{1}{k}\right)\right)\right) = \exp(a + b + o(1)).$$

On a donc bien la convergence souhaitée.

Étape 2 : Définition de φ.

Soit M un supplémentaire de $\mathcal{L}_G$ dans $\mathcal{M}_n(\mathbb{R})$. On définit

$$\begin{aligned} \varphi : \mathcal{L}_G \oplus M &\longrightarrow GL_n(\mathbb{R}) \\ l + m &\longmapsto e^l e^m. \end{aligned}$$

φ est de classe $\mathcal{C}^\infty$, $\varphi(0) = I_n$ et $D\varphi(0) = \mathrm{id}$ donc, d'après le théorème d'inversion locale, φ induit un $\mathcal{C}^\infty$-difféomorphisme d'un voisinage U de 0 sur un voisinage V de I_n dans $\mathcal{M}_n(\mathbb{R})$. De plus, on a $\varphi(U \cap \mathcal{L}_G) \subset V \cap G$.

Il reste à montrer que, quitte à restreindre U, $V \cap G \subset \varphi(U \cap \mathcal{L}_G)$, *i.e.* pour tout $l + m \in U$ tel que $\varphi(l + m) \in G$, alors $m = 0$.
On dispose alors du lemme suivant :

Lemme.
Il existe un voisinage ouvert $W \subset U$ de 0 dans $\mathcal{M}_n(\mathbb{R})$ tel que

$$\forall l + m \in W, \quad e^m \in G \Rightarrow m = 0.$$

Ainsi, avec ce lemme, si $l + m \in W$ est tel que $\varphi(l + m) \in G$, alors $e^m = e^{-l}\varphi(l + m) \in G$ et donc $m = 0$. □

Démonstration du lemme. Raisonnons par l'absurde en supposant que pour tout voisinage ouvert $W \subset U$ de 0 dans $\mathcal{M}_n(\mathbb{R})$, il existe $l + m \in W$ tel que $e^m \in G$

et $m \neq 0$. On a alors l'existence d'une suite $(l_k + m_k)_{k\in\mathbb{N}}$ tendant vers 0, et donc d'une suite $(m_k)_{k\in\mathbb{N}}$ d'éléments de $M \setminus \{0\}$ tendant vers 0 par continuité de la projection sur M parallèlement à $\mathcal{L}_G$, telle que $e^{m_k} \in G$ pour tout k.

On pose alors $\varepsilon_k := \frac{m_k}{\|m_k\|}$, qui est une suite à valeurs dans la sphère compacte de M donc, quitte à extraire, on peut supposer que (ε_k) converge vers $\varepsilon \in M$ de norme 1. Montrons alors que $\varepsilon \in \mathcal{L}_G$, ce qui constituera une contradiction car $\mathcal{L}_G \cap M = \{0\}$.

Pour $t \in \mathbb{R}$, on pose

$$\frac{t}{\|m_k\|} = \lambda_k + \mu_k \quad \text{avec } \lambda_k \in \mathbb{Z} \text{ et } |\mu_k| \leq \frac{1}{2}.$$

On a alors d'une part

$$e^{\lambda_k m_k} = (e^{m_k})^{\lambda_k} \in G,$$

et d'autre part

$$e^{\lambda_k m_k} = e^{t\varepsilon_k} e^{-\mu_k m_k} \xrightarrow[k\to+\infty]{} e^{t\varepsilon}.$$

On en déduit que $e^{t\varepsilon} \in G$ car G est fermé et donc que $\varepsilon \in \mathcal{L}_G$. □

On peut remarquer que $\mathcal{L}_G$ est le plan tangent à G en I_n. En effet, si $A \in \mathcal{L}_G$, alors $t \mapsto e^{tA}$ est une courbe de G donc A est le vecteur tangent au point I_n. Ceci prouve que $\mathcal{L}_g \subset T_{I_n}G$, et on a égalité pour des raisons de dimension.

2.29 Théorème de Cauchy – Lipschitz

Référence :
– [Dem06].
On s'intéresse au problème de Cauchy

$$\begin{cases} X' = f(t, X) \\ X(t_0) = x_0 \end{cases} \tag{2.6}$$

où $f : U \to \mathbb{R}^n$ avec U un ouvert de $\mathbb{R} \times \mathbb{R}^n$ et $(t_0, x_0) \in U$.

Définition. On dit que f est localement lipschitzienne en X si pour tout $(t_1, x_1) \in U$, il existe un voisinage V de x_1, un voisinage W de t_1 et $k > 0$ tels que pour tous $x, y \in V$ et tout $t \in W$, $\|f(t, x) - f(t, y)\| \leq k\|x - y\|$.

Théorème.
Si f est continue sur U et localement lipschitzienne en X, alors 2.6 admet une unique solution maximale.

Démonstration. f est continue sur U donc 2.6 est équivalent à

$$X(t) = x_0 + \int_{t_0}^{t} f(u, X(u))\,\mathrm{d}u. \tag{2.7}$$

Soit $V \in \mathcal{V}(x_0), W \in \mathcal{V}(t_0)$ et $k > 0$ comme dans la définition du caractère localement lipschitzien de f, on peut supposer $W \times V$ borné. On note $M := \sup_{W\times V} \|f\|$.

On se place sur un cylindre de sécurité : soit $r > 0$ tel que $\overline{B}(x_0, r) \subset V$ et soit $T > 0$ tel que $[t_0 - T, t_0 + T] \subset W$. On note $\mathcal{F}$ l'espace des fonctions continues de $[t_0 - T, t_0 + T]$ dans $\overline{B}(x_0, r)$ muni de la norme infinie, il s'agit alors d'un espace complet.

On définit l'application Φ de $\mathcal{F}$ dans $\mathcal{F}$ par

$$\Phi(Y)(t) := x_0 + \int_{t_0}^{t} f(u, Y(u))\,\mathrm{d}u.$$

Il faut d'abord que $\mathcal{F}$ soit stable par Φ.

$$\|\Phi(Y)(t) - x_0\| \leq |t - t_0|M \leq TM$$

donc en choisissant $T \leq \frac{r}{M}$, $\Phi(Y)$ est bien à valeurs dans $\overline{B}(x_0, r)$ (ce choix garantit aussi que le cylindre considéré est bien un cylindre de sécurité).

Le but est maintenant de montrer que Φ admet un point fixe en utilisant le théorème de Picard. En effet, l'équation 2.7 implique qu'une fonction X de classe $\mathcal{C}^1$ est solution de 2.6 si et seulement si elle est point fixe de Φ.

On va montrer que Φ admet une itérée contractante. Soit $Y, Z \in \mathcal{F}$, montrons par récurrence sur $p \in \mathbb{N}$ que

$$\forall t \in [t_0 - T, t_0 + T], \quad \|\Phi^p(Y)(t) - \Phi^p(Z)(t)\| \leq \frac{k^p|t - t_0|^p}{p!}\|Y - Z\|_\infty.$$

Cette inégalité est vraie pour $p = 0$ et

$$\begin{aligned}
\|\Phi^{p+1}(Y)(t) - \Phi^{p+1}(Z)(t)\| &\leq \left| \int_{t_0}^{t} \|f(u, \Phi^p(Y)(u)) - f(u, \Phi^p(Z)(u))\|\,\mathrm{d}u \right| \\
&\leq \left| \int_{t_0}^{t} k\|\Phi^p(Y)(u) - \Phi^p(Z)(u)\|\,\mathrm{d}u \right| \\
&\leq \left| \int_{t_0}^{t} k\frac{k^p|u - t_0|^p}{p!}\|Y - Z\|_\infty\,\mathrm{d}u \right| \\
&= \frac{k^{p+1}|t - t_0|^{p+1}}{(p+1)!}\|Y - Z\|_\infty,
\end{aligned}$$

d'où le résultat. On a donc, pour tout $p \in \mathbb{N}$ et tous $Y, Z \in \mathcal{F}$,

$$\|\Phi(Y) - \Phi(Z)\|_\infty \leq \frac{k^p T^p}{p!}\|Y - Z\|_\infty.$$

Or $\frac{k^p T^p}{p!} \xrightarrow[p\to+\infty]{} 0$ donc il existe $p \in \mathbb{N}$ tel que $\frac{k^p T^p}{p!} < 1$. D'après le théorème de point fixe de Picard, Φ admet un unique point fixe X sur $\mathcal{F}$, qui est donc l'unique solution de 2.6 sur $[t_0 - T, t_0 + T]$.

Cette solution se prolonge en une solution maximale. Supposons qu'il existe deux tels prolongements X_1 et X_2 sur deux intervalles I_1 et I_2. L'intervalle $I_1 \cap I_2$ est non vide car il contient $[t_0 - T, t_0 + T]$. Soit J le plus grand intervalle inclus dans $I_1 \cap I_2$ et contenant $[t_0 - T, t_0 + T]$ tel que $X_1 = X_2$ sur J. Alors J est fermé dans $I_1 \cap I_2$ car $X_1 - X_2$ est continue. Si $J \neq I_1 \cap I_2$, alors on peut appliquer l'unicité locale précédemment démontrée en l'une des bornes de J et contredire la maximalité de J. Donc $J = I_1 \cap I_2$, d'où on déduit $X_1 = X_2$ sur $I_1 \cap I_2$ et, par définition de solution maximale, $I_1 = I_2$. Finalement, X se prolonge en une unique solution maximale. □

2.30 Théorème de Frobenius – Zolotarev

Référence :
– [BMP05] page 251.

Théorème.
Soit p un nombre premier ≥ 3 et $n \in \mathbb{N}^*$. Alors pour tout $u \in GL_n(\mathbb{F}_p)$, on a :

$$\varepsilon(u) = \left(\frac{\det(u)}{p}\right)$$

où $\left(\frac{a}{p}\right)$ est le symbole de Legendre :

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ si } a \equiv 0 \text{ mod } p, \\ 1 \text{ si } a \text{ est un carré modulo } p \text{ (un résidu quadratique)}, \\ -1 \text{ sinon} \end{cases}$$

et où $\varepsilon(u)$ est la signature de u en tant que permutation sur l'ensemble fini $\mathbb{F}_p^n$.

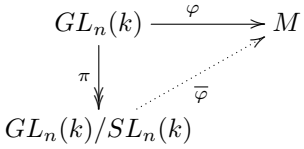
Démonstration. Il s'agit de montrer que la signature se factorise de la façon suivante : $\varepsilon = \left(\frac{\cdot}{p}\right) \circ \det$. On commence par énoncer un premier lemme.

Lemme.
Soit k un corps, M un groupe abélien et $n \in \mathbb{N}^*$. On suppose $k \neq \mathbb{F}_2$ ou $n \neq 2$. Alors tout morphisme de groupe $\varphi : GL_n(k) \to M$ se factorise par le déterminant,
i.e. il existe un unique morphisme de groupe $\delta : k^\times \to M$ tel que $\varphi = \delta \circ \det$.

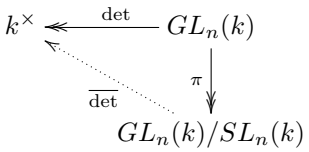
Démonstration. D'une part, puisque $k \neq \mathbb{F}_2$ ou $n \neq 2$, on a $D(GL_n(k)) = SL_n(k)$ (voir détails en fin de document).

D'autre part, pour $x, y \in GL_n(k), \varphi([x, y]) = [\varphi(x), \varphi(y)] = e$ car M est abélien.
$D(GL_n(k))$ est engendré par les commutateurs donc $D(GL_n(k)) \subseteq \ker \varphi$.

Donc $\varphi : GL_n(k) \to M$ se factorise en un unique morphisme $\overline{\varphi} : GL_n(k)/SL_n(k) \to M$:

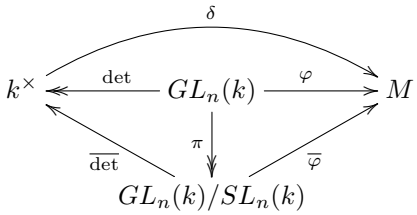


Comme det est un morphisme surjectif de $GL_n(k)$ dans $k^\times$ dont le noyau est $SL_n(k)$, on obtient le diagramme commutatif suivant :



avec $\overline{\det}$ un isomorphisme. Alors :

$$\varphi = \overline{\varphi} \circ (\overline{\det})^{-1} \circ \overline{\det} \circ \pi = \delta \circ \det \text{ avec } \delta = \overline{\varphi} \circ (\overline{\det})^{-1}$$



La surjectivité de det assure alors l'unicité du morphisme δ vérifiant $\delta \circ \det = \varphi$.

□

On a, dans le cadre du théorème, $\varepsilon : GL_n(\mathbb{F}_p) \to \{-1, 1\}$ avec $\{-1, 1\}$ abélien donc, par le lemme, il existe un unique morphisme $\delta : \mathbb{F}_p^\times \to \{-1, 1\}$ tel que $\varepsilon = \delta \circ \det$. Il s'agit de montrer que δ est le symbole de Legendre. Pour cela, nous allons montrer que le symbole de Legendre est l'unique morphisme non trivial de $\mathbb{F}_p^\times$ dans $\{-1, 1\}$, puis que $\varepsilon : GL_n(\mathbb{F}_p) \to \{-1, 1\}$ n'est pas trivial.

Le symbole de Legendre est bien non trivial car $x^2 = (-x)^2$ donc :

$$\begin{aligned} \mathbb{F}_p^\times &\to \mathbb{F}_p^\times \\ x &\mapsto x^2 \end{aligned}$$

n'est pas injective ($p \geq 3$) donc n'est pas surjective.

Si $\alpha : \mathbb{F}_p^\times \to \{-1, 1\}$ est un morphisme non trivial, $\ker \alpha$ est un sous-groupe d'indice 2 de $\mathbb{F}_p^\times$. Or $\mathbb{F}_p^\times$ est un groupe cyclique de cardinal pair donc ne possède qu'un seul sous-groupe H d'indice 2.

On a ainsi la partition $\mathbb{F}_p^\times = H \sqcup xH$ où $x \notin H$ avec :

$$\alpha(y) = \begin{cases} 1 \text{ si } y \in H \\ -1 \text{ si } y \in xH \end{cases}$$

Ainsi, α est entièrement déterminé donc est unique, c'est le morphisme de Legendre.

Montrons maintenant que ε n'est pas trivial.

Il existe une extension $\mathbb{F}_q/\mathbb{F}_p$ de degré n (à savoir $\mathbb{F}_{p^n}$). Vus comme $\mathbb{F}_p$-espaces vectoriels, $\mathbb{F}_p^n$ et $\mathbb{F}_q$ sont isomorphes. Il suffit donc de trouver une bijection $\mathbb{F}_p$-linéaire de $\mathbb{F}_q$ de signature -1. Or $\mathbb{F}_q^\times$ est cyclique d'ordre $q-1$. Soit g un générateur de ce groupe. La bijection $\mathbb{F}_p$-linéaire $x \mapsto gx$ de $\mathbb{F}_q$ agit comme le cycle $(g, g^2, \ldots, g^{q-1})$ de longueur $q-1$. Sa signature est donc $(-1)^q = -1$ car $q = p^n$ est impair.

Finalement, ε n'est pas trivial donc $\delta \circ \det$ non plus, donc δ n'est pas trivial et il s'agit donc du symbole de Legendre. □

Détails supplémentaires

Théorème.
$D(GL_n(k)) = SL_n(k)$ pour $n \neq 2$ ou $k \neq \mathbb{F}_2$.

Démonstration. Pour $u, v \in GL_n(k)$, $[u, v] \in SL_n(k)$, donc :

$$D(GL_n(k)) \subseteq SL_n(k)$$

Pour montrer l'inclusion inverse, il suffit de montrer que toute transvection est un commutateur ($n \geq 2$). Comme toutes les transvections sont conjuguées, il suffit de le montrer pour l'une d'elles.

– Si $n \geq 3$, alors :

$$I_n + E_{1,2} = [I_n + E_{1,3}, I_n + E_{3,2}]$$

– Si la caractéristique de k est différente de 2, alors :

$$I_n + E_{1,2} = [I_n + E_{1,2}, \mathrm{Diag}(2^{-1}, 1, \ldots, 1)]$$

– Si $\mathrm{card}(k) > 3$, alors, pour $a \in k$, a différent de $-1, 0$ et 1, on a :

$$I_n + E_{1,2} = [I_n + a^2(1-a^2)E_{1,2}, \mathrm{Diag}(a, a^{-1}, 1, \ldots, 1)]$$

□

Proposition.
Le symbole de Legendre est un morphisme.

Démonstration. Pour p premier impair,

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \text{ dans } \mathbb{F}_p$$

D'où :

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

□

2.31 Théorème de Gauss – Wantzel

Référence :
– [Car89] pages 48 et 214.

Lemme.
Soit m et n deux entiers premiers entre eux. Alors :

$$\textit{l'angle } \widehat{\frac{2\pi}{mn}} \textit{ est constructible } \iff \textit{ les angles } \widehat{\frac{2\pi}{m}} \textit{ et } \widehat{\frac{2\pi}{n}} \textit{ sont constructibles.}$$

Démonstration.

$\Rightarrow$: Chaque angle est un multiple de $\widehat{\frac{2\pi}{mn}}$.

$\Leftarrow$: $n \wedge m = 1$ donc par Bezout, il existe $a, b \in \mathbb{Z}$ tels que $an + bm = 1$. D'où :

$$\widehat{\frac{2\pi}{mn}} = a\widehat{\frac{2\pi}{m}} + b\widehat{\frac{2\pi}{n}}$$

donc $\widehat{\frac{2\pi}{mn}}$ est constructible. □

Corollaire.
Soit $n \geq 3$ et

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

sa décomposition en produit de facteurs premiers.
Alors :

$$\textit{le polygone régulier à } n \textit{ côtés est constructible } \iff \textit{ les angles } \widehat{\frac{2\pi}{p_i^{\alpha_i}}} \textit{ le sont.}$$

Théorème (Gauss – Wantzel)**.**
Soit $\alpha \in \mathbb{N}^*$.
Alors :

(i) Les angles $\widehat{\frac{2\pi}{2^\alpha}}$ sont constructibles.

(ii) Soit p un nombre premier impair, alors :

$$\textit{l'angle } \widehat{\frac{2\pi}{p^\alpha}} \textit{ est constructible } \iff \alpha = 1 \textit{ et } p = 1 + 2^{2^\beta} \textit{ où } \beta \in \mathbb{N}.$$

Démonstration.

(i) Cela revient à construire des bissectrices.

(ii) $\Rightarrow$: On pose $q := p^\alpha$ et $\omega := e^{2i\pi/q}$. On a donc supposé ω constructible. Par le théorème de Wantzel, on a alors :

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = 2^m \text{ où } m \in \mathbb{N}.$$

Or ω est une racine primitive q-ième de l'unité, donc son polynôme minimal sur $\mathbb{Q}$ est le polynôme cyclotomique Φ_q, de degré $\varphi(q) = p^{\alpha-1}(p-1)$. D'où :

$$2^m = [\mathbb{Q}(\omega) : \mathbb{Q}] = p^{\alpha-1}(p-1)$$

Or p est premier impair donc $\alpha = 1$ et on obtient $p = 2^m + 1$.
On écrit maintenant $m = \lambda 2^\beta$ avec $\beta \in \mathbb{N}$ et $\lambda \in \mathbb{N}^*$ impair.
Puisque -1 est racine de $1 + X^\lambda$, on a $1 + X \mid 1 + X^\lambda$, donc :

$$1 + 2^{2^\beta} \mid 1 + (2^{2^\beta})^\lambda = p$$

et p étant premier, on a :

$$p = 1 + 2^{2^\beta}.$$

$\Leftarrow$: On pose $n := 2^\beta$, $p = 1 + 2^n$ et $\omega := e^{2i\pi/p}$.
Alors puisque le polynôme minimal de ω est Φ_p, on a :

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1 = 2^n$$

Soit G le groupe d'automorphismes sur $\mathbb{Q}$ de $\mathbb{Q}(\omega)$ (*i.e.* le groupe des automorphismes de corps de $\mathbb{Q}(\omega)$ fixant $\mathbb{Q}$). Alors tout $g \in G$ est entièrement déterminé par $g(\omega)$. De plus,

$$\Phi_p(g(\omega)) = g(\Phi_p(\omega)) = g(0) = 0$$

Ainsi $g(\omega)$ est une racine de Φ_p donc est une puissance de ω.
Réciproquement, le morphisme qui est l'identité sur $\mathbb{Q}$ et qui envoie ω sur ω^k appartient à G.
Donc

$$G = \{\omega \mapsto \omega^k \mid k \in \{1, \ldots, p-1\}\}$$

et donc G est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$. G est ainsi engendré par un certain g d'ordre $p - 1 = 2^n$.
On pose, pour $0 \leq i \leq n$,

$$\mathbb{K}_i := \left\{ z \in \mathbb{Q}(\omega) \mid g^{2^i}(z) = z \right\}$$

Alors on a les inclusions :

$$\mathbb{Q} \subset \mathbb{K}_0 \subset \mathbb{K}_1 \subset \ldots \subset \mathbb{K}_n = \mathbb{Q}(\omega)$$

Montrons que $\mathbb{Q} = \mathbb{K}_0$ et que toutes les extensions sont quadratiques.

La famille $(\omega, g(\omega), \ldots, g^{p-2}(\omega))$ est une base de $\mathbb{Q}(\omega)$ (car $\{\omega, g(\omega), \ldots, g^{p-2}(\omega)\} = \{\omega, \omega^2, \ldots, \omega^{p-1}\}$) donc pour $z \in \mathbb{K}_0$, il existe $\lambda_0, \ldots, \lambda_{p-2}$ tels que :

$$z = \lambda_0\omega + \cdots + \lambda_{p-2}g^{p-2}(\omega)$$

Donc en appliquant g, on a :

$$z = g(z) = \lambda_0 g(\omega) + \cdots + \lambda_{p-2}g^{p-1}(\omega)$$

avec $g^{p-1} = \mathrm{id}$, donc par identification, on a $\lambda_0 = \cdots = \lambda_{p-2}$.
On a alors :

$$\begin{aligned} z &= \lambda_0(\omega + g(\omega) + \cdots + g^{p-2}(\omega)) \\ &= \lambda_0(\omega + \omega^2 + \cdots + \omega^{p-1}) \\ &= -\lambda_0 \end{aligned}$$

Par conséquent, $z \in \mathbb{Q}$ donc $\mathbb{K}_0 = \mathbb{Q}$.
De plus,

$$\sum_{k=0}^{2^{n-i}-1} g^{k2^i}(\omega) \in \mathbb{K}_i \setminus \mathbb{K}_{i-1}$$

donc les extensions $\mathbb{Q} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \ldots \subset \mathbb{K}_n = \mathbb{Q}(\omega)$ sont strictes et $[\mathbb{K}_n : \mathbb{Q}] = 2^n$. Toutes les extensions sont donc de degré 2 car il y en a n.
Finalement, par le théorème de Wantzel, ω est constructible à la règle et au compas.

□

En combinant le théorème et le corollaire du lemme, on obtient que le polygone régulier à n côtés est constructible si et seulement si n est le produit d'une puissance de 2 et d'un nombre fini de nombres de Fermat premiers distincts.

Détails supplémentaires

Théorème (Wantzel)**.**
Un nombre $z \in \mathbb{C}$ est constructible si et seulement s'il existe des corps $\mathbb{L}_1, \ldots, \mathbb{L}_n$ tels que

- $\mathbb{L}_0 = \mathbb{Q}$,
- $\mathbb{L}_{i+1}$ *est une extension quadratique de* $\mathbb{L}_i$,
- $z \in \mathbb{L}_n$.

Remarque. On énonce en général le théorème de Wantzel pour z réel. Le passage de réel à complexe se fait correctement, dans le cas présent il se fait plus simplement en remarquant que $\omega + \omega^{-1} = 2\Re(\omega)$.

2.32 Théorème de Hahn – Banach géométrique

Référence :
– [Bre05] page 1.

On prouve ici le théorème de Hahn – Banach géométrique à partir de la version analytique. On commence par rappeler le théorème de Hahn – Banach analytique.

Théorème (Hahn – Banach analytique)**.**
Soit E un $\mathbb{R}$-espace vectoriel.
Soit $p : E \to \mathbb{R}$ une application vérifiant

(i) $\forall x \in E, \forall \lambda > 0, \quad p(\lambda x) = \lambda p(x)$;

(ii) $\forall x, y \in E, \quad p(x+y) \leq p(x) + p(y)$.

Soit G un sous-espace vectoriel de E, soit $g : G \to \mathbb{R}$ une forme linéaire telle que pour tout $x \in G, g(x) \leq p(x)$.
Alors il existe $f : E \to \mathbb{R}$ une forme linéaire qui prolonge g et telle que pour tout $x \in E, f(x) \leq p(x)$.

Théorème (Hahn – Banach géométrique, sens large)**.**
Soit E un espace vectoriel normé sur $\mathbb{R}$.
Soit $A \subset E, B \subset E$ deux ensembles convexes, non vides et disjoints.
On suppose que A est ouvert.
Alors il existe un hyperplan affine fermé qui sépare A et B au sens large.

Lemme.
Soit $C \subset E$ un convexe ouvert avec $0 \in C$.
On pose, pour $x \in E$, $p(x) := \inf\{\alpha > 0 \mid x \in \alpha C\}$ la jauge de C.
Alors p vérifie les conditions (i) et (ii) de Hahn – Banach analytique et

(iii) *Il existe M tel que* $\forall x \in E, \quad 0 \leq p(x) \leq M\|x\|$;

(iv) $C = \{x \in E \mid p(x) < 1\}$.

Démonstration.
(iii) Soit $r > 0$ tel que $B(0,r) \subset C$, alors $p(x) \leq \frac{1}{r}\|x\|$, d'où (iii).
(i) Vérification immédiate.
(iv) – Supposons $x \in C$, C est ouvert donc il existe $\varepsilon > 0$ tel que $(1+\varepsilon)x \in C$, donc

$$p(x) \leq \frac{1}{1+\varepsilon} < 1.$$

– Si $p(x) < 1$, il existe $0 < \alpha < 1$ tel que $\frac{x}{\alpha} \in C$, donc

$$x = \alpha \frac{x}{\alpha} + (1-\alpha) \times 0 \in C.$$

(ii) Soit $x, y \in E$, soit $\varepsilon > 0$, alors d'après (i) et (iv),

$$\frac{x}{p(x)+\varepsilon} \text{ et } \frac{y}{p(y)+\varepsilon} \in C.$$

Donc

$$\forall t \in [0,1], \quad \frac{tx}{p(x)+\varepsilon} + \frac{(1-t)y}{p(y)+\varepsilon} \in C.$$

Alors

$$\text{pour } t = \frac{p(x)+\varepsilon}{p(x)+p(y)+2\varepsilon}, \text{ on a } \frac{x+y}{p(x)+p(y)+2\varepsilon} \in C.$$

D'où $\forall \varepsilon > 0, p(x+y) < p(x)+p(y)+2\varepsilon$, d'où (ii).

□

Lemme.
Soit $C \subset E$ un convexe ouvert non vide. Soit $x_0 \in E \setminus C$.
Alors il existe $f \in E'$ tel que pour tout $x \in C, f(x) < f(x_0)$.
En particulier, l'hyperplan affine d'équation $\{f = f(x_0)\}$ sépare $\{x_0\}$ et C au sens large.

Démonstration. Par translation, on peut toujours supposer $0 \in C$ et introduire p la jauge de C.

On considère $G := \mathbb{R}x_0$ et on pose $g : G \to \mathbb{R}$ la forme linéaire définie par $g(tx_0) = t$ pour $t \in \mathbb{R}$.
Alors pour tout $x \in G, g(x) \leq p(x)$:

- si $t > 0$, alors $\frac{x}{g(x)} = \frac{tx_0}{t} = x_0 \notin C$ donc $g(x) \leq p(x)$;
- si $t \leq 0, g(x) \leq 0 \leq p(x)$.

Donc par Hahn – Banach analytique, il existe f une forme linéaire sur E prolongeant g telle que pour tout $x \in E, f(x) \leq p(x)$. On a $f(x_0) = 1$ et f est continue par (iii). D'autre part, $(iv) \Rightarrow f(x) < 1, \forall x \in C$. □

Démonstration du théorème. On pose $C := A - B$. Alors C est convexe, ouvert (car $C = \bigcup_{y \in B}(A - y)$) et $0 \notin C$ car $A \cap B = \varnothing$.

D'après le dernier lemme, il existe $f \in E'$ tel que pour tout $z \in C, f(z) < 0$, *i.e.* pour tous $x \in A$ et $y \in B$, $f(x) < f(y)$.
Soit $\alpha \in \mathbb{R}$ tel que $\sup_{x \in A} f(x) \leq \alpha \leq \inf_{y \in B} f(y)$. Alors l'hyperplan affine d'équation $\{f = \alpha\}$ sépare A et B au sens large. □

Théorème (Hahn – Banach géométrique, sens strict)**.**
Soit $A \subset E$ et $B \subset E$ deux ensembles convexes, non vides, disjoints. On suppose que A est fermé et que B est compact. Alors il existe un hyperplan fermé qui sépare A et B au sens strict.

Démonstration. Pour $\varepsilon > 0$, on pose $A_\varepsilon := A + B(0,\varepsilon)$ et $B_\varepsilon := B + B(0,\varepsilon)$ de sorte que A_ε et B_ε sont convexes, ouverts et non vides. De plus, pour $\varepsilon > 0$ assez petit, A_ε et B_ε sont disjoints (sinon on pourrait trouver des suites $\varepsilon_n \to 0, x_n \in A$ et $y_n \in B$ telles que $\|x_n - y_n\| < 2\varepsilon_n$ et on pourrait extraire une sous-suite $y_n \to y \in B$ par compacité de B et $y \in A$ car A fermé).

D'après le théorème de Hahn – Banach géométrique sens large, il existe un hyperplan fermé d'équation $\{f = \alpha\}$ qui sépare A_ε et B_ε au sens large. On a

donc

$$\forall x \in A, \forall y \in B, \forall z, z' \in B(0,1), \quad f(x+\varepsilon z) \leq \alpha \leq f(y+\varepsilon z').$$

Il en résulte que

$$\forall x \in A, \forall y \in B, \quad f(x)+\varepsilon\|f\| \leq \alpha \leq f(y)-\varepsilon\|f\|.$$

On conclut que A et B sont séparés au sens strict par l'hyperplan $\{f = \alpha\}$ puisque $\|f\| \neq 0$. □

Compléments

Démonstration du théorème de Hahn – Banach analytique.

Lemme (Zorn)**.**
Tout ensemble ordonné, inductif et non vide admet un élément maximal.

On considère

$$P := \{h \mid h : D(h) \subset E \to \mathbb{R} \text{ avec } D(h) \text{ sev de } E, h \text{ linéaire}, G \subset D(h), \\ h \text{ prolonge } g \text{ et } \forall x \in D(h), h(x) \leq p(x)\}.$$

On munit P de la relation d'ordre

$$h_1 \leq h_2 \iff D(h_1) \subset D(h_2) \text{ et } h_2 \text{ prolonge } h_1.$$

$P \neq \varnothing$ car $g \in P$.

P est inductif : soit $Q \subset P$ un sous-ensemble totalement ordonné, on note $Q = (h_i)_{i\in I}$, on définit $D(h) := \bigcup_{i\in I} D(h_i)$ et $h(x) := h_i(x)$ si $x \in D(h_i)$.
Alors h est un majorant de Q.

D'après le lemme de Zorn, P possède un élément maximal f. Prouvons que $D(f) = E$.

Supposons que $D(f) \neq E$ et soit $x_0 \notin D(f)$, on pose $D(h) := D(f) + \mathbb{R}x_0$ et

$$h(x+tx_0) = f(x) + t\alpha \qquad \forall x \in D(f), \forall t \in \mathbb{R}$$

pour un certain α, le but étant que $h \in P$.
On doit donc avoir

$$f(x) + t\alpha \leq p(x+tx_0) \qquad \forall x \in D(f), \forall t \in \mathbb{R}.$$

i.e.

$$\begin{cases} f(x) + \alpha \leq p(x+x_0) & \forall x \in D(f) \\ f(x) - \alpha \leq p(x-x_0) \end{cases}$$

par (i).
Il suffit donc de choisir α tel que

$$\sup_{y\in D(f)} (f(y) - p(y-x_0)) \leq \alpha \leq \inf_{x\in D(f)} (p(x+x_0) - f(x)).$$

Ceci est possible car

$$\begin{aligned} f(x)+f(y) &\leq p(x+y) \\ &\leq p(x+x_0)+p(y-x_0). \end{aligned}$$

Donc $f(y)-p(y-x_0) \leq p(x+x_0)-f(x) \qquad \forall x,y \in D(f)$.

Ainsi, $h \in P$ et $f \leq h, f \neq h$, on obtient une contradiction. □

Corollaire.
Soit E un espace vectoriel normé, G un sous-espace vectoriel de E.
Soit $g : G \to \mathbb{R}$ linéaire et continue.
Alors il existe $f \in E'$ prolongeant g et telle que $\|f\| = \|g\|$.

Démonstration. On pose $p(x) := \|g\|\|x\|$, les hypothèses du théorème sont bien vérifiées et on a $|f(x)| \leq \|g\|\|x\|$, d'où $\|f\| \leq \|g\|$, d'où $\|f\| = \|g\|$ car f prolonge g. □

Corollaire.
Pour tout $x \in E$, il existe $f_0 \in E'$ tel que $\|f_0\| = \|x_0\|$ et $\langle f_0, x_0\rangle = \|x_0\|^2$.

Démonstration. Appliquer le corollaire avec $G := \mathbb{R}x_0$ et $g(tx_0) := t\|x_0\|^2$, de sorte que $\|g\| = \|x_0\|$. □

Corollaire.
Pour tout $x \in E$,

$$\|x\| = \sup_{\substack{f \in E' \\ \|f\| \leq 1}} |\langle f, x\rangle| = \max_{\substack{f \in E' \\ \|f\| \leq 1}} |\langle f, x\rangle|$$

Démonstration. Soit $x \neq 0$, alors :

$$\sup_{\substack{f \in E' \\ \|f\| \leq 1}} |\langle f, x\rangle| \leq \|x\|$$

et, par le corollaire précédent, il existe $f_0 \in E'$ tel que $\|f_0\| = \|x\|$ et $\langle f_0, x\rangle = \|x\|^2$.

On pose $f_1 := \frac{f_0}{\|x\|}$, on a $\|f_1\| = 1$ et $\langle f_1, x\rangle = \|x\|$. □

2.33 Théorème de Jordan

Référence :
– [GT98].

Théorème.
Soit $\Gamma = \mathrm{Im}(\gamma)$ avec $\gamma : \mathbb{R} \to \mathbb{C}$ de classe $\mathcal{C}^1$, 1-périodique, telle que $\gamma_{|[0,1[}$ soit injective et $\gamma'(t) \neq 0$. Alors $\mathbb{C} \setminus \Gamma$ a deux composantes connexes.

Démonstration. On commence par supposer pour plus de commodités que $|\gamma'(t)| = 1$ pour tout t (une justification est donnée en fin de document), que $\gamma(0) = 0$ et que $\gamma'(0) = 1$.

Lemme.
Si pour $\varepsilon > 0$ on note Γ_ε^+ (resp. Γ_ε^-) la courbe paramétrée par

$$\gamma_\varepsilon^+(t) = \gamma(t) + i\varepsilon\gamma'(t) \text{ (resp. } \gamma_\varepsilon^-(t) = \gamma(t) - i\varepsilon\gamma'(t))$$

alors il existe $\alpha > 0$ tel que pour tout $0 < \varepsilon < \alpha$, $\Gamma \cap \Gamma_\varepsilon^+ = \Gamma \cap \Gamma_\varepsilon^- = \varnothing$.

Démonstration. Supposons qu'il existe s, t tels que $\gamma(t) = \gamma_\varepsilon^+(s)$ (on peut supposer $|t-s| \leq \frac{1}{2}$), alors

$$\begin{aligned} |\gamma(t) - (\gamma(s) + (t-s)\gamma'(s))| &= |\gamma'(s)||i\varepsilon - (t-s)| \\ &> |t-s|. \end{aligned}$$

Par ailleurs, γ' est continue sur $\mathbb{R}$ et périodique donc uniformément continue, donc il existe $\eta > 0$ tel que

$$|t_1 - t_2| \leq \eta \Longrightarrow |\gamma'(t_1) - \gamma'(t_2)| \leq 1.$$

Si $|t-s| \leq \eta$, alors en appliquant le théorème des accroissements finis à $t \mapsto \gamma(t) - (\gamma(s) + (t-s)\gamma'(s))$ on a

$$|\gamma(t) - (\gamma(s) + (t-s)\gamma'(s))| \leq \sup_{t_1 \in [s,t]} |\gamma'(t_1) - \gamma'(s)||t-s| \leq |t-s|.$$

Ceci est impossible donc $|t-s| > \eta$. Posons alors

$$\alpha := \inf_{\frac{1}{2} \geq |t_1 - t_2| \geq \eta} |\gamma(t_1) - \gamma(t_2)|.$$

Alors α est atteint par compacité de $\{\frac{1}{2} \geq |t_1 - t_2| \geq \eta\}$ et continuité de $(t_1, t_2) \mapsto |\gamma(t_1) - \gamma(t_2)|$, on en déduit que $\alpha > 0$ par injectivité de γ.

Soit $\varepsilon < \alpha$ et supposons qu'il existe s, t tels que $\gamma(t) = \gamma_\varepsilon^+(s)$. Alors $|t-s| > \eta$ et on a

$$\begin{aligned} |\gamma(t) - \gamma_\varepsilon^+(s)| &= |\gamma(t) - (\gamma(s) + i\varepsilon\gamma'(s))| \\ &\geq |\gamma(t) - \gamma(s)| - |i\varepsilon\gamma'(s)| \\ &\geq \alpha - \varepsilon > 0. \end{aligned}$$

On aboutit donc sur une contradiction, d'où $\Gamma \cap \Gamma_\varepsilon^+ = \varnothing$. De même, $\Gamma \cap \Gamma_\varepsilon^- = \varnothing$. □

Montrons que $\mathbb{C} \setminus \Gamma$ possède au plus deux composantes connexes. Pour cela, posons $\varepsilon < \alpha$ et montrons que tout point de $\mathbb{C} \setminus \Gamma$ peut être relié par un chemin à Γ_ε^+ ou à Γ_ε^- sans couper Γ.

Soit donc $z \in \mathbb{C} \setminus \Gamma$.
Par compacité de Γ, la distance de z à Γ est atteinte en un point $\gamma(t_0)$ et on a $z - \gamma(t_0) \perp \gamma'(t_0)$ (en dérivant $t \mapsto |z - \gamma(t)|^2$).
Alors la demi-droite $[\gamma(t_0), z)$ rencontre Γ_ε^+ au point $\gamma_\varepsilon^+(t_0)$ ou Γ_ε^- au point $\gamma_\varepsilon^-(t_0)$. Supposons par exemple que nous soyons dans le premier cas et montrons que $[\gamma_\varepsilon^+(t_0), z]$ ne rencontre par Γ. Deux cas sont possibles :

– $\gamma(t_0), \gamma_\varepsilon^+(t_0)$ et z sont alignés dans cet ordre. Alors si $[\gamma_\varepsilon^+(t_0), z]$ rencontrait Γ, cela contredirait la minimalité de $|z - \gamma(t_0)|$.
– $\gamma(t_0), z$ et $\gamma_\varepsilon^+(t_0)$ sont alignés dans cet ordre. Alors si $[\gamma_\varepsilon^+(t_0), z]$ rencontrait Γ, ce point serait également sur un $\Gamma_{\varepsilon'}^+$ avec $\varepsilon' \leq \varepsilon$, ce qui contredirait le lemme.

Montrons maintenant que $\mathbb{C} \setminus \Gamma$ a au moins deux composantes connexes. Pour cela, il suffit de trouver deux points de $\mathbb{C} \setminus \Gamma$ qui n'ont pas le même indice par rapport à γ. Choisissons $i\varepsilon$ et $-i\varepsilon$.

$$\mathrm{Ind}_\gamma(i\varepsilon) - \mathrm{Ind}_\gamma(-i\varepsilon) = \frac{1}{2i\pi} \int_{-1/2}^{1/2} \left(\frac{\gamma'(t)}{\gamma(t) - i\varepsilon} - \frac{\gamma'(t)}{\gamma(t) + i\varepsilon} \right) \mathrm{d}t = \frac{\varepsilon}{\pi} \int_{-1/2}^{1/2} \frac{\gamma'(t)}{\gamma^2(t) + \varepsilon^2} \, \mathrm{d}t.$$

Le dénominateur ne peut s'annuler que si $t = 0$ et $\varepsilon = 0$ car $\pm i\varepsilon \notin \Gamma$.

Par ailleurs, $\lim_{t\to 0} \frac{\gamma(t)}{t} = \gamma'(0) = 1$ donc il existe $\delta > 0$ tel que si $|t| < \delta$, alors $\Re\left(\frac{\gamma^2(t)}{t^2}\right) > \frac{1}{2}$.
On a alors, par changement de variable $t = \varepsilon s$,

$$\begin{aligned} \frac{\varepsilon}{\pi} \int_{-\delta}^{\delta} \frac{\gamma'(t)}{\gamma^2(t) + \varepsilon^2} \, \mathrm{d}t &= \frac{\varepsilon^2}{\pi} \int_{-\delta/\varepsilon}^{\delta/\varepsilon} \frac{\gamma'(\varepsilon s)}{\gamma^2(\varepsilon s) + \varepsilon^2} \, \mathrm{d}s \\ &= \frac{1}{\pi} \int_{\mathbb{R}} \frac{\gamma'(\varepsilon s)}{1 + \frac{\gamma^2(\varepsilon s)}{(\varepsilon s)^2} s^2} \mathbf{1}_{[-\delta/\varepsilon, \delta/\varepsilon]}(s) \, \mathrm{d}s. \end{aligned}$$

Or δ a été choisi pour que l'intégrande soit inférieure à $1/(1 + \frac{s^2}{2})$. D'où, par théorème de convergence dominée,

$$\frac{1}{\pi} \int_{\mathbb{R}} \frac{\gamma'(\varepsilon s)}{1 + \frac{\gamma^2(\varepsilon s)}{(\varepsilon s)^2} s^2} \mathbf{1}_{[-\delta/\varepsilon, \delta/\varepsilon]}(s) \, \mathrm{d}s \xrightarrow[\varepsilon \to 0]{} \frac{1}{\pi} \int_{\mathbb{R}} \frac{\mathrm{d}s}{1 + s^2} = 1.$$

D'autre part, la fonction $(\varepsilon, t) \mapsto \frac{\gamma'(t)}{\gamma^2(t) + \varepsilon^2}$ est continue sur le compact $[0, \frac{\alpha}{2}] \times \{\frac{1}{2} \geq |t| \geq \delta\}$, elle est donc majorée indépendamment de t et ε par une constante, d'où

$$\frac{\varepsilon}{\pi} \int_{\delta \leq |t| \leq \frac{1}{2}} \frac{\gamma'(t)}{\gamma^2(t) + \varepsilon^2} \, \mathrm{d}t \xrightarrow[\varepsilon \to 0]{} 0.$$

Finalement, on a

$$\lim_{\varepsilon \to 0} (\mathrm{Ind}_\gamma(i\varepsilon) - \mathrm{Ind}_\gamma(-i\varepsilon)) = 1.$$

Donc pour ε suffisamment petit, les indices sont distincts. □

Détails supplémentaires

Montrons que l'on peut se ramener au cas où $|\gamma'(t)| = 1$ pour tout t, quitte à modifier la période de γ.
Soit

$$s(t) := \int_0^t |\gamma'(u)| \, \mathrm{d}u$$

l'abscisse curviligne de γ, qui est continue car γ est $\mathcal{C}^1$. γ' est continue et non nulle donc s est strictement croissante sur $\mathbb{R}$. Il s'agit donc d'une bijection et on peut considérer $\tilde{\gamma} := \gamma \circ s^{-1}$. On a alors

$$\begin{aligned}\tilde{\gamma}'(t) &= (s^{-1})'(t)\gamma'(s^{-1}(t)) \\ &= \frac{1}{s'(s^{-1}(t))}\gamma'(s^{-1}(t)) \\ &= \frac{\gamma'(s^{-1}(t))}{|\gamma'(s^{-1}(t))|}.\end{aligned}$$

On a donc $|\tilde{\gamma}'(t)| = 1$ pour tout t.

Soit $T := s(1)$, montrons que $\tilde{\gamma}$ est T-périodique. Pour $t \in \mathbb{R}$, on a

$$t + T = \int_0^{s^{-1}(t)} |\gamma'(u)| \,\mathrm{d}u + \int_0^1 |\gamma'(u)| \,\mathrm{d}u = \int_0^{s^{-1}(t)+1} |\gamma'(u)| \,\mathrm{d}u = s(s^{-1}(t) + 1)$$

car γ est périodique. D'où

$$\tilde{\gamma}(t + T) = \gamma \circ s^{-1}(s(s^{-1}(t) + 1)) = \gamma(s^{-1}(t) + 1) = \gamma(s^{-1}(t)) = \tilde{\gamma}(t).$$

2.34 Théorème de Kronecker

Référence :
– [FGN07] page 213.

Théorème.
On définit

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

où $Z(P)$ désigne les racines complexes de P.

Si $P \in \Omega_n$, alors les racines de P sont des racines de l'unité.

Démonstration. Montrons dans un premier temps que Ω_n est fini.
On note $z_1, \ldots, z_n$ les racines de P et $\sigma_1, \ldots, \sigma_n$ les fonctions symétriques élémentaires de P évaluées en $(z_1, \ldots, z_n)$.
Alors

$$P = X^n - \sigma_1 X^{n-1} + \ldots + (-1)^n \sigma_n$$

et $\sigma_i \in \mathbb{Z}$.
Or $|z_i| \leq 1$ donc, pour $1 \leq p \leq n$,

$$|\sigma_p| = \left| \sum_{1 \leq i_1 < \ldots < i_p \leq n} z_{i_1} \cdots z_{i_n} \right| \leq \sum_{1 \leq i_1 < \ldots < i_p \leq n} 1 = \binom{n}{p}.$$

On en déduit que Ω_n est fini.

On considère désormais

$$P_k := \prod_{i=1}^{n} (X - z_i^k)$$

et montrons que $P_k \in \Omega_n$.
Le coefficient de X^{n-r} dans P_k est $(-1)^r \sigma_r(z_1^k, \dots, z_n^k)$. Or $\sigma_r(X_1^k, \dots, X_n^k)$ est un polynôme symétrique à coefficients dans $\mathbb{Z}$, donc par le théorème de structure des polynômes symétriques il existe $Q_r \in \mathbb{Z}[X_1, \dots, X_n]$ tel que

$$\sigma_r(X_1^k, \dots, X_n^k) = Q_r(\sigma_1(X_1, \dots, X_n), \dots, \sigma_n(X_1, \dots, X_n)).$$

On en déduit, étant donné que $\sigma_i(z_1, \dots, z_n) \in \mathbb{Z}$,

$$\sigma_r(z_1^k, \dots, z_n^k) = Q_r(\sigma_1(z_1, \dots, z_n), \dots, \sigma_n(z_1, \dots, z_n)) \in \mathbb{Z}.$$

On a donc $P_k \in \mathbb{Z}[X]$. De plus, P_k est unitaire et ses racines sont les z_i^k qui vérifient $0 < |z_i^k| \leq 1$. Par conséquent, $P_k \in \Omega_n$.

Or Ω_n est fini donc l'ensemble des racines des éléments de Ω_n est fini donc, pour $i \in \{1, \dots, n\}$, l'application

$$\begin{aligned} \mathbb{N}^* &\longrightarrow \mathbb{C} \\ k &\longmapsto z_i^k \end{aligned}$$

n'est pas injective. On en déduit qu'il existe $k \neq l$ tels que $z_i^k = z_i^l$ et $z_i \neq 0$ donc $z_i^{k-l} = 1$ et z_i est une racine de l'unité. □

Corollaire.
Soit $P \in \mathbb{Z}[X]$ unitaire et irréductible tel que $Z(P) \subset D(0,1)$, où $Z(P)$ désigne les racines de P.
Alors $P = X$ ou P est un polynôme cyclotomique.

Démonstration. Supposons $P \neq X$. Alors P est irréductible donc 0 n'est pas racine de P et, d'après le théorème de Kronecker, ses racines sont des racines de l'unité. De plus, les racines de P sont simples car P est irréductible (sinon il serait divisible par $P \wedge P'$ non trivial) et donc $P \mid X^N - 1$ pour un certain N. Or

$$X^N - 1 = \prod_{d \mid N} \Phi_d$$

avec Φ_d irréductible sur $\mathbb{Z}$.
$P \neq 1$ donc $P = \Phi_k$ pour un certain k. □

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

Détails supplémentaires

Autre rédaction possible pour montrer que $P_k \in \mathbb{Z}[X]$:

Introduisons le polynôme $Q_k := X - Y^k \in \mathbb{Z}[X,Y]$ et considérons $R_k(X) := \mathrm{Res}_Y(P(Y), Q_k(X,Y))$. $P \in \mathbb{Z}[X]$ et $Q_k \in \mathbb{Z}[X,Y]$ donc $R_k \in \mathbb{Z}[X]$. Par ailleurs,

$$R_k(X) = \prod_{i=1}^{n} Q_k(X, z_i) = \prod_{i=1}^{n} (X - z_i^k) = P_k(X)$$

donc $P_k \in \mathbb{Z}[X]$.

2.35 Théorème de l'élément primitif

Références :
- [Per96] page 87 ;
- [Esc04] page 89.

Théorème.
Toute extension finie d'un corps fini ou d'un corps de caractéristique nulle est monogène.

Démonstration. Soit L/K une extension finie.

Si L est fini, alors le groupe multiplicatif de L est cyclique et si α en est un générateur alors $K(\alpha) = L$.

Soit maintenant K de caractéristique nulle. On commence par supposer que $L = K[x,y]$.
Pour trouver $z \in L$ tel que $L = K[z]$, on va chercher z sous la forme $z = x + ty$ avec $t \in K$. On pose $K' = K[z]$, il s'agit de montrer que $y \in K'$. Pour cela, nous allons exhiber un polynôme de $K'[X]$ dont un des coefficients est y.

Si π_x et π_y désignent les polynômes minimaux respectifs de x et y sur K, on a $\pi_y(y) = 0$ et $\pi_y \in K[X] \subset K'[X]$. D'autre part, en posant $F(X) := \pi_x(z - tX)$, on a aussi $F(y) = \pi_x(z - ty) = \pi_x(x) = 0$ et $F \in K'[X]$. On en déduit

$$X - y \mid \mathrm{pgcd}(F, \pi_y) \quad \text{dans } L[X],$$

avec $\mathrm{pgcd}(F, \pi_y) \in K'[X]$. Montrons alors qu'il existe $t \in K$ tel que $\mathrm{pgcd}(F, \pi_y) = X - y$. Soit M un corps de décomposition de $\pi_x \pi_y$, il s'agit de montrer qu'il existe $t \in K$ tel que y soit la seule racine commune de F et π_y dans M.

Dans $M[X]$, on a

$$\pi_x = (X - x) \prod_{i=2}^{n} (X - x_i) \quad \text{et} \quad \pi_y = (X - y) \prod_{j=2}^{m} (X - y_j),$$

d'où

$$\begin{aligned} F(X) &= (z - tX - x)\prod_{i=2}^{n}(z - tX - x_i) \\ &= t(y - X)\prod_{i=2}^{n}(x - x_i + t(y - X)). \end{aligned}$$

On choisit donc $t \neq 0$ tel que, pour tout $i, j, x - x_i + t(y - y_j) \neq 0$. Montrons qu'un tel t existe.

On a d'abord que π_y est scindé à racines simples. En effet, il est irréductible dans $K[X]$ et $\pi_y' \neq 0$ car $\mathrm{car}(K) = 0$ donc $\mathrm{pgcd}(\pi_y, \pi_y') = 1$ car sinon ce polynôme de $K[X]$ serait un diviseur strict de π_y. On en déduit que, pour tout $j, y \neq y_j$ et donc qu'on peut poser l'ensemble

$$\mathcal{E} := \left\{ \frac{x_i - x}{y - y_j} \right\}.$$

On prend alors $t \in K \setminus \mathcal{E}$ non nul, ce qui est possible car $\mathcal{E}$ est fini et K infini. Pour le choix d'un tel t, on a bien

$$\mathrm{pgcd}(F, \pi_y) = X - y \in K'[X]$$

et donc $y \in K'$.
On a alors $x = z - ty \in K'$, d'où $L = K'$ et L est monogène.

On procède maintenant par récurrence pour montrer le théorème.
Soit $L = K(x_1, \ldots, x_n)$, alors par hypothèse de récurrence il existe $\alpha \in L$ tel que $K(x_1, \ldots, x_{n-1}) = K(\alpha)$. On a alors $L = K(\alpha, x_n)$ qui est monogène par ce qui a été fait précédemment. □

Exemple. Soit $L := \mathbb{F}_p(X, Y)$, on considère le sous-corps de L défini par $K := \mathbb{F}_p(X^p, Y^p)$. Alors L/K n'est pas monogène.

En effet, $[L : K] = p^2$ car $(X^i Y^j)_{0 \leq i,j \leq p-1}$ est une base de L/K mais si $x \in L$, alors $x^p \in K$ donc le polynôme minimal de x sur K divise $X^p - x^p$ qui est de degré p, donc L/K ne peut être monogène.

Proposition.
Soit L/K une extension finie. Alors L/K admet un nombre fini d'extensions intermédiaires si et seulement si L/K est monogène.

Démonstration. $\Rightarrow$: Si K est fini, alors L est une extension monogène. On suppose donc K infini.
Soit $a, b \in L$, montrons que $K(a, b)/K$ est monogène.
Pour tout $c \in K$, les extensions $K(a + cb)$ forment des extensions intermédiaires entre K et $K(a, b)$. Puisque K est infini, il existe $c \neq c'$ tels que $K(a + cb) = K(a + c'b)$.
On a alors $a + c'b \in K(a + cb)$, d'où $b(c' - c) \in K(a + cb)$, donc $b \in K(a + cb)$.
On en déduit $a \in K(a + cb)$ et $K(a + cb) = K(a, b)$.

En procèdant par récurrence comme dans la preuve du théorème on prouve que L est monogène.

$\Leftarrow$: Soit M un corps intermédiaire de $L = K(\alpha)$ et soit P, Q les polynômes minimaux de α respectivement sur K et M. Alors $Q \mid P$.
Soit $M' \subset M$ le sur-corps de K engendré par les coefficients de Q. Alors le polynôme minimal de α sur M' est Q donc $[L : M] = [L : M'] = \deg Q$, d'où $M = M'$.
Les corps intermédiaires sont donc engendrés par les différents facteurs unitaires de P dans $L[X]$. Ceux-ci sont en nombre fini, ce qui conclut la démonstration.

□

2.36 Théorème de Lie – Kolchin

Référence :
– [CL05] page 90.

Théorème.
Tout sous-groupe connexe et résoluble de $GL_n(\mathbb{C})$ est conjugué à un sous-groupe du groupe des matrices triangulaires supérieures inversibles T.

On dit que $V \subset \mathbb{C}^n$ est stable par G s'il est stable par tout élément de G. On dit que G est irréductible si les seuls sous-espaces de $\mathbb{C}^n$ stables par G sont $\{0\}$ et $\mathbb{C}^n$.

Lemme.
Un sous-groupe connexe, résoluble et irréductible de $GL_n(\mathbb{C})$ est commutatif.

Démonstration. G est résoluble, on pose $m := \inf\{k \geq 1 \mid D^k(G) = \{I_n\}\}$.

Supposons que $m \geq 2$.
On pose $H := D^{m-1}(G)$, alors $D(H) = \{I_n\}$ donc H est abélien. H est donc cotrigonalisable, *i.e.* il existe $P \in GL_n(\mathbb{C})$ telle que $PHP^{-1} \subset T$. Quitte à remplacer G par PGP^{-1}, on peut supposer $H \subset T$.

Montrons que H est codiagonalisable. Soit $V \subset \mathbb{C}^n$ le sev engendré par les vecteurs propres communs à tous les éléments de H, montrons que $V = \mathbb{C}^n$.
$H \subset T$ donc $e_1 \in V$, donc $V \neq \{0\}$. Il reste à prouver que V est G-stable :
Soit v vecteur propre de tout élément de H, soit $g \in G$.
Alors $\forall h \in H, h(g(v)) = gg^{-1}hg(v)$ et $g^{-1}hg \in H$ car $H \lhd G$ ($H = D^{m-1}(G)$) donc $g^{-1}hg(v) = \lambda v$ pour un certain λ. D'où $h(g(v)) = \lambda g(v)$ et $g(v) \in V$.
G étant irréductible, $V = \mathbb{C}^n$ donc H est conjugué à un sous-groupe du groupe D des matrices diagonales inversibles, donc on peut supposer $H \subset D$.

Montrons que H est inclus dans le centre de G.
Pour $h \in H$, on définit

$$\begin{aligned} \varphi_h : G &\longrightarrow H \\ g &\longmapsto ghg^{-1} \end{aligned}$$

φ_h est continue et G est connexe donc $\varphi_h(G)$ est connexe.
Par ailleurs, $ghg^{-1} \in H$ est diagonale de même valeurs propres que h donc $\varphi_h(G)$ est fini, donc $\varphi_h(G) = \{h\}$, *i.e.*

$$\forall h \in H, \forall g \in G, hg = gh$$

i.e. $H \subset Z(G)$.

Montrons que H est réduit à $\{I_n\}$.
Soit $h \in H, W \neq \{0\}$ un espace propre de h.
$h \in Z(G)$ donc W est G-stable donc $W = \mathbb{C}^n$ car G est irréductible, donc $h = \lambda I_n$.
Or $H \subset D(G) \subset SL_n(\mathbb{C})$ donc $\lambda^n = 1$. On en déduit que H est fini, or G connexe $\Rightarrow D(G)$ connexe donc H est connexe est donc $H = \{I_n\}$.

Ce qui précède est absurde donc $m = 1$ et G est abélien. □

Démonstration du théorème. Procédons par récurrence sur n.

Si $n = 1$, $GL_n(\mathbb{C}) = \mathbb{C}^* = T$.

Supposons le théorème démontré pour tout $k \leq n - 1$.
Si G est irréductible, d'après le lemme il est commutatif donc cotrigonalisable.
Sinon, il existe $V \subset \mathbb{C}^n$ G-stable de dimension $p \in \{1, \ldots, n-1\}$.

Soit W un supplémentaire de V.
Quitte à changer de base, on peut supposer que les matrices de G sont de la forme

$$\begin{pmatrix} g_1 & * \\ 0 & g_2 \end{pmatrix}.$$

Alors

$$\begin{array}{ccc} G \longrightarrow GL_p(\mathbb{C}) & & G \longrightarrow GL_{n-p}(\mathbb{C}) \\ g \longmapsto g_1 & \text{et} & g \longmapsto g_2 \end{array}$$

sont deux morphismes continus donc ont pour image des sous-groupes connexes et résolubles de $GL_p(\mathbb{C})$ et de $GL_{n-p}(\mathbb{C})$ respectivement.

Par hypothèse de récurrence, ils sont cotrigonalisables donc G aussi en concaténant les bases obtenues. □

Détails supplémentaires

Lemme.
G connexe $\Longrightarrow$ $D(G)$ connexe.

Démonstration. On pose

$$S := \{[g_1, g_2] \mid g_1, g_2 \in G\},$$

alors S est connexe comme image de $(g_1, g_2) \mapsto g_1 g_2 g_1^{-1} g_2^{-1}$ continue.
De plus, si $S_m = \{s_1 \cdots s_m \mid s_i \in S\}$, S_m est connexe comme image de S^m par $(g_1, \ldots, g_m) \mapsto g_1 \cdots g_m$ continue.

Or $D(G) = \bigcup_{m \geq 1} S_m$ et $I_n \in S_m$ pour tout m donc $D(G)$ est connexe. □

2.37 Théorème de Molien

Référence :
– [Lei99a] page 95.

Théorème.
Soit G un sous-groupe fini de $GL_n(\mathbb{C})$.
On note $A = \mathbb{C}[X_1, \ldots, X_n]$ et on pose

$$\begin{array}{rccl} \sigma & : & G & \longrightarrow & \mathfrak{S}(A) \\ & & g & \longmapsto & (P \mapsto P(g^{-1}.(X_1, \ldots, X_n))) \end{array}$$

où $(X_1, \ldots, X_n)$ est identifié avec la colonne ayant pour coordonnées $X_1, \ldots, X_n$ et $.$ est le produit matriciel.
i.e., *si $g^{-1} = (u_{i,j})_{1 \leq i,j \leq n}$,*

$$\sigma(g)(P)(X_1, \ldots, X_n) = P\left(\sum_{j=1}^{n} u_{1,j} X_j, \ldots, \sum_{j=1}^{n} u_{n,j} X_j\right)$$

Alors :
- *σ définit une action de G sur A et est à valeurs dans $GL(A)$, on notera $\sigma(g)(P) = g \cdot P$.*
- *Pour $k \in \mathbb{N}$, on note A_k l'espace des polynômes homogènes de A de degré k. L'action de G sur A induit alors une action de G sur A_k.*
- *Finalement, on note A_k^G l'ensemble des points fixes sous cette action,* i.e.

$$A_k^G = \{P \in A_k \mid \forall g \in G, g \cdot P = P\}$$

et $a_k(G) = \dim A_k^G$.
On a alors

$$\sum_{k=0}^{+\infty} a_k(G) X^k = \frac{1}{\operatorname{Card} G} \sum_{g \in G} \frac{1}{\det(\mathrm{Id} - Xg)}$$

Lemme.
Soit V un $\mathbb{C}$-espace vectoriel de dimension finie n et G un groupe fini.
Soit $\varphi : G \to GL(V)$ un morphisme de groupes.
On note

$$V^G = \bigcap_{g \in G} \ker(\varphi(g) - \mathrm{Id})$$

Alors

$$\dim V^G = \frac{1}{\operatorname{Card} G} \sum_{g \in G} \operatorname{Trace} \varphi(g)$$

Démonstration. On considère :

$$p_G = \frac{1}{\operatorname{Card} G} \sum_{g \in G} \varphi(g)$$

Montrons que $p_G(V) = V^G$:

– Soit $v \in V, h \in G$, alors

$$\begin{aligned}\varphi(h)(p_G(v)) &= \frac{1}{\operatorname{Card} G} \sum_{g \in G} \varphi(h)\varphi(g)(v) \\ &= \frac{1}{\operatorname{Card} G} \sum_{g \in G} \varphi(hg)(v) \\ &= p_G(v)\end{aligned}$$

car $g \mapsto hg$ est une bijection de G, donc $p_G(V) \subseteq V^G$.

– Réciproquement, on a $p_G(v) = v$ pour tout $v \in V^G$, donc $V^G \subseteq p_G(V)$. L'égalité $\varphi(h)p_G = p_G$ pour tout $h \in G$ montre que ${p_G}^2 = p_G$, donc p_G est un projecteur d'image V^G.

D'où

$$\operatorname{rang} p_G = \dim V^G = \operatorname{Trace} p_G$$

D'où le résultat par linéarité de la trace. □

Démonstration du théorème.

– Montrons d'abord que σ définit bien une action de G sur A. On a :

$$\begin{aligned}(g \cdot (g' \cdot P)) &= g \cdot (P({g'}^{-1}.(X_1, \ldots, X_n))) \\ &= P({g'}^{-1} g^{-1}(X_1, \ldots, X_n)) \\ &= P((gg')^{-1}.(X_1, \ldots, X_n)) \\ &= (gg') \cdot P\end{aligned}$$

et $\mathrm{Id} \cdot P = P$.
De plus, $\sigma(g)$ est clairement linéaire, donc $\sigma(g) \in GL(A)$.

– Pour $k \in \mathbb{N}$, $g \cdot A_k \subseteq A_k$, donc l'action de G sur A induit une action de G sur A_k. Notons $\sigma_k : G \to GL(A_k)$ le morphisme induit par σ.

– Soit $g \in G$. Observons d'abord que g est diagonalisable. En effet, le polynôme $X^{\operatorname{Card} G} - 1$ annule g et est scindé à racines simples.
Soit alors $u \in GL_n(\mathbb{C})$ tel que la matrice de ugu^{-1} dans la base $(e_1, \ldots, e_n)$ soit diagonale et soit $\lambda_1, \ldots, \lambda_n$ les valeurs propres de g.
Alors

$$\begin{aligned}\frac{1}{\det(\mathrm{Id} - Xg)} &= \prod_{i=1}^{n} \frac{1}{1 - \lambda_i X} \\ &= \prod_{i=1}^{n} \left(\sum_{k=0}^{+\infty} \lambda_i^k X^k \right) \\ &= \sum_{k=0}^{+\infty} \left(\sum_{k_1 + \cdots + k_n = k} \lambda_1^{k_1} \cdots \lambda_n^{k_n} \right) X^k\end{aligned}$$

D'autre part, si $k_1 + \cdots + k_n = k$, alors

$$\sigma_k(ug^{-1}u^{-1})(X_1^{k_1} \cdots X_n^{k_n}) = \lambda_1^{k_1} \cdots \lambda_n^{k_n} X_1^{k_1} \cdots X_n^{k_n}$$

Il faut noter ici que $ug^{-1}u^{-1}$ n'appartient pas forcément à G, et donc pour que $\sigma_k(ug^{-1}u^{-1})$ ait un sens il faudrait prolonger l'action σ_k en une action de $GL_n(\mathbb{C})$ sur A.
Donc $\lambda_1^{k_1} \cdots \lambda_n^{k_n}$ est valeur propre de $\sigma_k(ug^{-1}u^{-1})$. Or les $X_1^{k_1} \cdots X_n^{k_n}$ forment une base de A_k, donc

$$\mathrm{Trace}(\sigma_k(g^{-1})) = \mathrm{Trace}(\sigma_k(ug^{-1}u^{-1})) = \sum_{k_1+\cdots+k_n=k} \lambda_1^{k_1} \cdots \lambda_n^{k_n}$$

D'où

$$\frac{1}{\det(\mathrm{Id} - Xg)} = \sum_{k=0}^{+\infty} \mathrm{Trace}(\sigma_k(g^{-1}))X^k$$

En appliquant le lemme avec $V = A_k$ et $\varphi = \sigma_k$, on obtient

$$\dim A_k^G = a_k(G) = \frac{1}{\mathrm{Card}\, G} \sum_{g\in G} \mathrm{Trace}(\sigma_k(g^{-1}))$$

D'où

$$\begin{aligned}
\sum_{k=0}^{+\infty} a_k(G)X^k &= \frac{1}{\mathrm{Card}\, G} \sum_{k=0}^{+\infty} \sum_{g\in G} \mathrm{Trace}(\sigma_k(g^{-1}))X^k \\
&= \frac{1}{\mathrm{Card}\, G} \sum_{g\in G} \sum_{k=0}^{+\infty} \mathrm{Trace}(\sigma_k(g^{-1}))X^k \\
&= \frac{1}{\mathrm{Card}\, G} \sum_{g\in G} \frac{1}{\det(\mathrm{Id} - Xg)}
\end{aligned}$$

□

2.38 Théorème de Riesz – Fischer

Référence :
– [Bre05] page 57.
$(X, \mathcal{A}, \mu)$ désigne un espace mesuré.

Théorème.
Soit $1 \leq p \leq \infty$.

(i) $L^p(\mu)$ *est un espace de Banach.*

(ii) Soit $(f_n)_{n\in\mathbb{N}}$ *une suite d'éléments de* $L^p(\mu)$ *et* $f \in L^p(\mu)$ *tels que* $f_n \xrightarrow{\|\cdot\|_p} f$. *Alors il existe une sous-suite* $(f_{n_k})_{k\in\mathbb{N}}$ *et* $g \in L^p(\mu)$ *tels que* $|f_{n_k}| \leq g$ μ*-p.p. pour tout* k *et* $f_{n_k} \xrightarrow{\mu-p.p.} f$.

Démonstration. – On suppose d'abord $p = \infty$.

Soit $(f_n)_{n\in\mathbb{N}}$ une suite de Cauchy dans $L^\infty(\mu)$. Alors pour $k \geq 1$, il existe N_k tel que pour $m, n \geq N_k$, $\|f_m - f_n\|_{L^\infty} \leq \frac{1}{k}$. Il existe donc E_k négligeable tel que

$$\forall x \in X \setminus E_k, \forall m, n \geq N_k, \quad |f_m(x) - f_n(x)| \leq \frac{1}{k}.$$

En posant $E := \bigcup_k E_k$, on a $\mu(E) = 0$ et pour tout $x \in X \setminus E$, $(f_n(x))_{n\in\mathbb{N}}$ est de Cauchy donc converge vers un $f(x)$. En faisant $m \to +\infty$ dans l'inégalité précédente, on obtient

$$\forall x \in X \setminus E, \forall n \geq N_k, \quad |f(x) - f_n(x)| \leq \frac{1}{k}.$$

On en déduit $f \in L^\infty(\mu)$ et $\|f - f_n\|_{L^\infty} \leq \frac{1}{k}$ pour tout $n \geq N_k$, d'où $\|f - f_n\|_{L^\infty} \to 0$.

– On suppose maintenant $p \in [1, +\infty[$.

Soit $(f_n)_{n\in\mathbb{N}}$ une suite de Cauchy dans $L^p(\mu)$. Puisque toute suite de Cauchy admettant une valeur d'adhérence converge, quitte à extraire, on peut supposer

$$\forall n \in \mathbb{N}, \quad \|f_{n+1} - f_n\|_p \leq \frac{1}{2^n}$$

car $(f_n)_{n\in\mathbb{N}}$ est de Cauchy. On pose alors

$$g_n : x \mapsto \sum_{k=0}^{n} |f_{k+1}(x) - f_k(x)|.$$

On a $g_n \in L^p(\mu)$ et, par inégalité de Minkowski,

$$\|g_n\|_p \leq \sum_{k=0}^{n} \|f_{k+1} - f_k\|_p \leq \sum_{k=0}^{n} \frac{1}{2^k} \leq \sum_{k=0}^{+\infty} \frac{1}{2^k} = 2.$$

La suite de fonctions $(g_n)_{n\in\mathbb{N}}$ est croissante, positive et bornée en norme p donc par théorème de convergence monotone, il existe $g \in L^p(\mu)$ tel que (g_n) converge vers g presque partout. On a alors, pour $m \geq n \geq 0$,

$$\begin{aligned} |f_m(x) - f_n(x)| &\leq |f_m(x) - f_{m-1}(x)| + \cdots + |f_{n+1}(x) - f_n(x)| \\ &\leq g(x) - g_{n-1}(x). \end{aligned}$$

On a donc que pour presque tout x, $(f_n(x))_{n\in\mathbb{N}}$ est une suite de Cauchy dans $\mathbb{C}$ donc converge vers un certain $f(x)$. Or, en faisant $m \to +\infty$, on a

$$|f(x) - f_n(x)| \leq g(x)$$

donc $f \in L^p(\mu)$. Finalement, $|f(x) - f_n(x)|^p \to 0$ p.p. et $|f(x) - f_n(x)|^p \leq g(x)^p \in L^1(\mu)$, donc par le théorème de convergence dominée, $\|f - f_n\|_p \to 0$.

□

2.39 Théorème de stabilité de Lyapunov

Référence :
– [Rou09] page 138.

Théorème.
Soit $f \in \mathcal{C}^1(\mathbb{R}^n, \mathbb{R}^n)$ telle que $f(0) = 0$. On note $A := Df(0)$ de valeurs propres distinctes $\lambda_1, \dots, \lambda_k$ et on suppose que les λ_i sont de partie réelle strictement négative. Pour $x \in \mathbb{R}^n$, on considère le problème de Cauchy

$$\begin{cases} y' = f(y) \\ y(0) = x. \end{cases} \tag{2.8}$$

Alors 0 est un point d'équilibre asymptotiquement stable de 2.8, c'est-à-dire qu'il existe $V \in \mathcal{V}_{\mathbb{R}^n}(0)$ tel que pour tout $x \in V$, $y(t)$ tend exponentiellement vers 0 lorsque $t \to +\infty$.

Démonstration. On introduit le système linéarisé

$$\begin{cases} z' = Az \\ z(0) = x, \end{cases} \tag{2.9}$$

on a $z(t) = e^{tA}x$.

D'après le lemme des noyaux, $x = x_1 + \cdots + x_k$ avec $x_i \in \ker(A - \lambda_i I)^{m_i}$. On a alors

$$\begin{aligned} e^{tA}x_j &= e^{t\lambda_j} \exp(t(A - \lambda_j I))x_j \\ &= e^{t\lambda_j} \left(\sum_{p=0}^{m_j - 1} \frac{t^p}{p!} (A - \lambda_j I)^p \right) x_j. \end{aligned}$$

Si $\| \cdot \|$ désigne la norme euclidienne canonique sur $\mathbb{C}^n$, on a

$$\begin{aligned} \|e^{tA}x_j\| &\leq e^{t\Re(\lambda_j)} C_j (1 + |t|)^{m_j - 1} \|x_j\| \\ &\leq C_0 e^{t\Re(\lambda_j)} (1 + |t|)^{n-1} \|x_j\|. \end{aligned}$$

On en déduit

$$\begin{aligned} \|e^{tA}x\| &\leq \sum_{j=1}^{k} \|e^{tA}x_j\| \\ &\leq C_0 (1 + |t|)^{n-1} \left(\sum_{j=1}^{k} e^{t\Re(\lambda_j)} \right) \max_j \|x_j\|. \end{aligned}$$

Par équivalence des normes, il existe donc un polynôme P tel que

$$\|e^{tA}x\| \leq P(|t|) \left(\sum_{j=1}^{k} e^{t\Re(\lambda_j)} \right) \|x\|.$$

Or pour tout $j, \Re(\lambda_j) < 0$ donc il existe $a > 0$ tel que la fonction $t \mapsto P(|t|)\left(\sum_{j=1}^{k} e^{t\Re(\lambda_j)}\right)e^{at}$ soit bornée sur $\mathbb{R}_+$ par une constante $C > 0$. On a donc, pour z solution de 2.9,

$$\forall t \geq 0, \quad \|z(t)\| \leq Ce^{-at}\|x\|.$$

0 est donc un point d'équilibre asymptotiquement stable de 2.9.

On considère l'application

$$\begin{aligned} b : \mathbb{R}^n \times \mathbb{R}^n &\longrightarrow \mathbb{R} \\ (x, y) &\longmapsto \int_0^{+\infty} \langle e^{tA}x, e^{tA}y\rangle \, \mathrm{d}t. \end{aligned}$$

Alors b est bien définie car

$$\begin{aligned} |\langle e^{tA}x, e^{tA}y\rangle| &\leq \|e^{tA}x\|\|e^{tA}y\| \quad \text{par Cauchy-Schwarz} \\ &\leq C^2e^{-2at}\|x\|\|y\|. \end{aligned}$$

b est une forme bilinéaire symétrique, on note q sa forme quadratique associée. Alors

$$\forall x \in \mathbb{R}^n, \quad q(x) = \int_0^{+\infty} \|e^{tA}x\|^2 \, \mathrm{d}t \geq 0$$

et $e^{tA} \in GL_n(\mathbb{R})$ donc q est définie positive. On en déduit que $\sqrt{q}$ définit une norme sur $\mathbb{R}^n$.

Pour y solution de 2.8, on va montrer que $(q \circ y)'(t) \leq -\beta q(y(t))$ pour tout $t \geq 0$ et pour x au voisinage de 0. En effet, en montrant ceci on aura $\frac{d}{dt}(e^{\beta t}q(y(t))) \leq 0$ donc, puisque $q(y(0)) = q(x)$,

$$q(y(t)) \leq e^{-\beta t}q(x),$$

ce qui permettra de conclure par équivalence des normes.

On a

$$\begin{aligned} (q \circ y)'(t) &= Dq(y(t)).y'(t) \\ &= 2b(y, y') \\ &= 2b(y, r(y)) + 2b(y, Ay) \end{aligned}$$

avec $r(y) := f(y) - Ay$ le reste de Taylor à l'ordre 1 de f (car $f(0) = 0$). On a alors

$$\begin{aligned} 2b(y, Ay) &= \int_0^{+\infty} 2\langle e^{tA}y, e^{tA}Ay\rangle \, \mathrm{d}t \\ &= \left[\|e^{tA}y\|^2\right]_0^{+\infty} \\ &= -\|y\|^2. \end{aligned}$$

Par ailleurs, par Cauchy-Schwarz, on a $|b(y, r(y))| \leq \sqrt{q(y)}\sqrt{q(r(y))}$ et, $r(y)$ étant le reste de Taylor à l'ordre 1 de f,

$$\forall \varepsilon > 0, \exists \alpha > 0, \quad q(y) \leq \alpha \Rightarrow \sqrt{q(r(y))} \leq \varepsilon \sqrt{q(y)}.$$

Pour $q(y) < \alpha$, on a donc $2b(y, r(y)) \leq 2\varepsilon q(y)$. On en déduit par équivalence des normes que pour $q(y(t)) < \alpha$,

$$(q \circ y)'(t) \leq -\beta q(y(t)).$$

Il reste à montrer que si $q(x) < \alpha$, alors $q(y(t)) < \alpha$ pour tout $t \geq 0$. En effet, si ce n'est pas le cas on pose $t_0 := \inf\{t > 0 \mid q(y(t)) = \alpha\}$, on a donc

$$(q \circ y)'(t_0) \leq -\beta\alpha < 0,$$

et donc $q(y(t)) > \alpha$ pour un $t < t_0$, ce qui est absurde. On en déduit que pour $q(x) < \alpha$, alors $q(y(t)) < \alpha$ pour tout $t \geq 0$ et donc

$$(q \circ y)'(t) \leq e^{-\beta t} q(y(t)),$$

ce qui permet de conclure. □

2.40 Théorème des deux carrés

Référence :
– [Per96] page 56.

On pose $\Sigma := \{a^2 + b^2 \mid a, b \in \mathbb{N}\}$ et on considère $\mathbb{Z}[i]$ muni de $N : z \mapsto z\bar{z}$, *i.e.* $N(a + ib) = a^2 + b^2$.
N est multiplicative. De plus, $n \in \Sigma \iff \exists z \in \mathbb{Z}[i], n = N(z)$, donc Σ est stable par multiplication et on retrouve $(a^2+b^2)(c^2+d^2) = (ac-bd)^2+(ad+bc)^2$.

Théorème.
Soit p premier, alors

$$p \in \Sigma \iff p = 2 \text{ ou } p \equiv 1[4].$$

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

Démonstration. On commence par remarquer que pour $z \in \mathbb{Z}[i], z$ est inversible si et seulement si $N(z) = 1$. En effet, si $N(z) = 1$, alors $z\bar{z} = 1$ donc z est inversible. Réciproquement, si $zz' = 1$, alors $N(z)N(z') = N(1) = 1$ donc $N(z) = 1$.

- $\Rightarrow$: Si $p = a^2 + b^2$, on a $p = N(z) = z\bar{z}$ avec $z = a + ib$ et $N(z) = N(\bar{z}) \neq 1$ (car p est premier) donc z et $\bar{z}$ ne sont pas inversibles et p n'est pas irréductible dans $\mathbb{Z}[i]$.
- $\Leftarrow$: Si $p = zz'$ avec $z, z' \notin \mathbb{Z}[i]^\times$, on a $N(p) = N(z)N(z') = p^2$ et $N(z), N(z') \neq 1$, donc $p = N(z)$ (car p est premier), donc $p \in \Sigma$.

□

Démonstration du théorème. $2 = 1^2 + 1^2$ donc $2 \in \Sigma$.

On suppose p premier impair.

$\mathbb{Z}[i]$ est principal (car euclidien) donc

$$\begin{aligned} p \text{ est réductible} &\iff (p) \text{ n'est pas premier} \\ &\iff \mathbb{Z}[i]/(p) \text{ n'est pas intègre.} \end{aligned}$$

Or $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2+1)$ donc

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

D'où

$$\begin{aligned} (p) \text{ n'est pas premier} &\iff X^2+1 \text{ est réductible sur } \mathbb{F}_p \\ &\iff X^2+1 \text{ admet une racine dans } \mathbb{F}_p \\ &\iff -1 \text{ est un carré de } \mathbb{F}_p \\ &\iff (-1)^{\frac{p-1}{2}} = 1 \\ &\iff p \equiv 1[4]. \end{aligned}$$

En effet, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$:
Il y a $\frac{p-1}{2}$ carrés dans $\mathbb{F}_p^\times$ et ils sont tous contenus dans l'ensemble $\{x \in \mathbb{F}_p \mid x^{\frac{p-1}{2}} = 1\}$, de cardinal au plus $\frac{p-1}{2}$. Donc x est un carré de $\mathbb{F}_p^\times$ si et seulement si $x^{\frac{p-1}{2}} = 1$. □

Théorème.
Soit $n \geq 2$ et $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$ sa décomposition en facteurs premiers.

Alors $n \in \Sigma$ si et seulement si pour tout $p \in \mathcal{P}$ vérifiant $p \equiv 3[4]$, $v_p(n)$ est pair.

Démonstration. $\Leftarrow$: Σ est stable par multiplication et un carré est dans Σ.

$\Rightarrow$: Soit $p \equiv 3[4]$, montrons le résultat par récurrence sur $v_p(n)$.

Si $v_p(n) = 0$, c'est bon.

Sinon, p divise $n = a^2 + b^2 = (a+ib)(a-ib)$ et p est irréductible dans $\mathbb{Z}[i]$ (car $p \notin \Sigma$) donc on peut supposer sans perdre en généralité que p divise $a + ib$. Mais $p \in \mathbb{Z}$ donc $p \mid a$ et $p \mid b$, donc $p^2 \mid n$.

Si on pose $a = pa'$ et $b = pb'$, alors $\frac{n}{p^2} = a'^2 + b'^2 \in \Sigma$ et $v_p\left(\frac{n}{p^2}\right) = v_p(n) - 2 \equiv 0[2]$ par hypothèse de récurrence.

Donc $v_p(n) \equiv 0[2]$.

□

Détails supplémentaires

$\mathbb{Z}[i]$ est euclidien :

Soit $t, z \in \mathbb{Z}[i] \setminus \{0\}$, alors $\frac{z}{t} = x + iy \in \mathbb{C}$.
Soit $q = a + ib \in \mathbb{Z}[i]$ tel que $|x - a| \leq \frac{1}{2}$ et $|y - b| \leq \frac{1}{2}$.
Alors

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

Soit $r := z - qt \in \mathbb{Z}[i]$, alors

$$|r| = |t| \left|\frac{z}{t} - q\right| < |t|$$

donc $N(r) < N(t)$.
D'où $z = qt + r$ avec $N(r) < N(t)$.

2.40.1 Variante du théorème des deux carrés

Il s'agit de donner une condition nécessaire et suffisante sur $n \in \mathbb{N}$ pour que l'équation diophantienne $x^2 + 2y^2 = n$ admette une solution.

On pose $\Sigma := \{a^2+2b^2 \mid a, b \in \mathbb{Z}\}$ et on considère $\mathbb{Z}[i\sqrt{2}]$ muni de $N : z \mapsto z\bar{z}$, *i.e.* $N(a + ib\sqrt{2}) = a^2 + 2b^2$. On a alors $N(\mathbb{Z}[i\sqrt{2}]) = \Sigma$.

N est multiplicative donc Σ est stable par multiplication.

Théorème.
Soit p premier, alors

$$p \in \Sigma \iff p = 2 \text{ ou } p \equiv 1 \text{ ou } 3[8].$$

Lemme.
$p \in \Sigma \iff$ *p n'est pas irréductible dans $\mathbb{Z}[i\sqrt{2}]$.*

Démonstration. On commence par remarquer que pour $z \in \mathbb{Z}[i\sqrt{2}], z$ est inversible si et seulement si $N(z) = 1$. En effet, si $N(z) = 1$, alors $z\bar{z} = 1$ donc z est inversible. Réciproquement, si $zz' = 1$, alors $N(z)N(z') = N(1) = 1$ donc $N(z) = 1$.

- $\Rightarrow$: Si $p = a^2 + 2b^2$, on a $p = N(z) = z\bar{z}$ avec $z = a + ib\sqrt{2}$ et $N(z) = N(\bar{z}) \neq 1$ (car p est premier) donc z et $\bar{z}$ ne sont pas inversibles et p n'est pas irréductible dans $\mathbb{Z}[i\sqrt{2}]$.
- $\Leftarrow$: Si $p = zz'$ avec $z, z' \notin \mathbb{Z}[i\sqrt{2}]^\times$, on a $N(p) = N(z)N(z') = p^2$ et $N(z), N(z') \neq 1$, donc $p = N(z)$ (car p est premier), donc $p \in \Sigma$.

□

Démonstration du théorème. $2 = 0^2 + 2 \times 1^2$ donc $2 \in \Sigma$.

On suppose p premier impair.

$\mathbb{Z}[i\sqrt{2}]$ est factoriel (car euclidien) donc

$$\begin{aligned} p \text{ est réductible} &\iff (p) \text{ n'est pas premier} \\ &\iff \mathbb{Z}[i\sqrt{2}]/(p) \text{ n'est pas intègre.} \end{aligned}$$

Or $\mathbb{Z}[i\sqrt{2}] \simeq \mathbb{Z}[X]/(X^2+2)$ donc

$$\mathbb{Z}[i\sqrt{2}]/(p) \simeq \mathbb{Z}[X]/(X^2+2,p) \simeq \mathbb{F}_p[X]/(X^2+2).$$

D'où

$$\begin{aligned}(p) \text{ n'est pas premier} &\iff X^2+2 \text{ est réductible sur } \mathbb{F}_p \\ &\iff X^2+2 \text{ admet une racine dans } \mathbb{F}_p \\ &\iff -2 \text{ est un carré de } \mathbb{F}_p \\ &\iff \left(\frac{-2}{p}\right) = 1.\end{aligned}$$

Or

$$\left(\frac{-2}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}}.$$

On a alors $(-1)^{\frac{p-1}{2}} = 1 \iff p \equiv 1[4]$ et $(-1)^{\frac{p^2-1}{8}} = 1 \iff p \equiv \pm 1[8]$, donc

$$\left(\frac{-2}{p}\right) = 1 \iff p \equiv 1 \text{ ou } 3[8].$$

□

Théorème.
Soit $n \geq 2$ et $n = \prod_{p\in\mathcal{P}} p^{v_p(n)}$ sa décomposition en facteurs premiers.
Alors $n \in \Sigma$ si et seulement si pour tout $p \in \mathcal{P}$ vérifiant $p \equiv -1$ ou $-3[8]$, $v_p(n)$ est pair.

Démonstration. $\Leftarrow$: Σ est stable par multiplication et un carré est dans Σ.
$\Rightarrow$: Soit $p \equiv -1$ ou $-3[8]$, montrons le résultat par récurrence sur $v_p(n)$.
Si $v_p(n) = 0$, alors $v_p(n)$ est pair.
Sinon, p divise $n = a^2+2b^2 = (a+ib\sqrt{2})(a-ib\sqrt{2})$ et p est irréductible dans $\mathbb{Z}[i\sqrt{2}]$ (car $p \notin \Sigma$) donc on peut supposer sans perdre en généralité que p divise $a+ib\sqrt{2}$. Or $p \in \mathbb{Z}$ donc $p \mid a$ et $p \mid b$, donc $p^2 \mid n$.
Si on pose $a = pa'$ et $b = pb'$, alors $\frac{n}{p^2} = a'^2+2b'^2 \in \Sigma$ et $v_p\left(\frac{n}{p^2}\right) = v_p(n) - 2 \equiv 0[2]$ par hypothèse de récurrence.
Donc $v_p(n) \equiv 0[2]$.

□

Remarque. Cette démonstration s'adapte pour traiter l'équation $x^2 - dy^2 = p$ dès que $\mathbb{Z}[\sqrt{d}]$ (avec convention $\sqrt{-1} = i$) est euclidien, il suffit alors de calculer $\left(\frac{d}{p}\right)$ pour avoir le résultat. C'est le cas pour $d = -2, -1, 2, 3, 6, 7, 11, 19$. Toutefois, pour $d > 0$, on va seulement avoir p réductible dans $\mathbb{Z}[\sqrt{d}] \iff \pm p \in \Sigma$, ce qui ne donnera l'existence de solutions que pour $\pm p$. Cela vient du fait que la norme d'un élément de $\mathbb{Z}[\sqrt{d}]$ peut-être négative pour $d > 0$. Par exemple, pour $d = 3$, 3 est bien réductible dans $\mathbb{Z}[\sqrt{3}]$ mais $x^2 - 3y^2 = 3$ n'a pas de solutions

car en réduisant modulo 3 on obtient que $3 \mid x$, donc $x^2-3y^2=3$ a des solutions si et seulement si $3x^2-y^2=1$ en a, or en réduisant à nouveau modulo 3 on trouve que $y^2 \equiv -1[3]$, ce qui n'est pas possible. Par contre, $x^2-3y^2=-3$ a une solution triviale.

Détails supplémentaires

$\mathbb{Z}[i\sqrt{2}]$ est euclidien :
Soit $t, z \in \mathbb{Z}[i\sqrt{2}] \setminus \{0\}$, alors $\frac{z}{t} = x + iy\sqrt{2} \in \mathbb{C}$.
Soit $q = a + ib\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$ tel que $|x-a| \leq \frac{1}{2}$ et $|y-b| \leq \frac{1}{2}$.
Alors

$$\left|\frac{z}{t} - q\right| \leq \sqrt{\frac{1}{4}+\frac{1}{2}} < 1.$$

Soit $r := z - qt \in \mathbb{Z}[i\sqrt{2}]$, alors

$$|r| = |t|\left|\frac{z}{t} - q\right| < |t|$$

donc $N(r) < N(t)$.
D'où $z = qt + r$ avec $N(r) < N(t)$.

2.41 Un homéomorphisme réalisé par l'exponentielle matricielle

Référence :
– [MT94] page 62.

Théorème.
L'exponentielle sur $\mathcal{M}_n(\mathbb{R})$ réalise un homéomorphisme entre $\mathcal{S}_n(\mathbb{R})$ et $\mathcal{S}_n^{++}(\mathbb{R})$.
L'exponentielle sur $\mathcal{M}_n(\mathbb{C})$ réalise un homéomorphisme entre $\mathcal{H}_n(\mathbb{C})$ et $\mathcal{H}_n^{++}(\mathbb{C})$.

Démonstration. On fait la preuve dans $\mathbb{C}$, celle dans $\mathbb{R}$ est analogue. Soit $A \in \mathcal{H}_n(\mathbb{C})$, alors il existe U unitaire telle que

$$A = U \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} U^*$$

avec $\lambda_i \in \mathbb{R}$, d'où

$$\exp A = U \begin{pmatrix} e^{\lambda_1} & & 0 \\ & \ddots & \\ 0 & & e^{\lambda_n} \end{pmatrix} U^*,$$

donc $\exp A \in \mathcal{H}_n^{++}(\mathbb{R})$.

Montrons maintenant que l'exponentielle sur $\mathcal{H}_n(\mathbb{C})$ est surjective dans $\mathcal{H}_n^{++}(\mathbb{C})$. Soit $A \in \mathcal{H}_n^{++}(\mathbb{C})$, alors

$$A = U \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} U^*$$

avec U unitaire et $\lambda_i > 0$, donc la matrice hermitienne

$$B = U \begin{pmatrix} \ln \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \ln \lambda_n \end{pmatrix} U^*$$

vérifie $\exp B = A$.

Montrons que $\exp : \mathcal{H}_n(\mathbb{C}) \to \mathcal{H}_n^{++}(\mathbb{C})$ est injective. Soit H_1 et H_2 deux matrices hermitiennes telles que $\exp(H_1) = \exp(H_2)$. Puisque $\exp(H_1)$ est un polynôme en H_1, alors H_1 commute avec $\exp(H_2)$. D'autre part, H_2 est diagonalisable :

$$H_2 = PDP^{-1} \quad \text{avec } D = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}.$$

Soit Q un polynôme tel que $Q(e^{\lambda_i}) = \lambda_i$ pour tout i, alors

$$Q(\exp(H_2)) = Q(P \exp(D) P^{-1}) = PQ(\exp(D))P^{-1} = PDP^{-1} = H_2,$$

donc H_2 est un polynôme en $\exp(H_2)$ donc commute avec H_1. On en déduit que H_1 et H_2 sont diagonalisables dans une même base :

$$H_1 = PD_1P^{-1} \quad \text{et} \quad H_2 = PD_2P^{-1} \quad \text{avec } D_1 \text{ et } D_2 \text{ diagonales réelles.}$$

Donc $\exp(D_1) = \exp(D_2)$ et les valeurs propres de H_1 et H_2 sont réelles donc $D_1 = D_2$, d'où $H_1 = H_2$.

L'exponentielle étant continue, il reste à établir que sa réciproque est continue. Soit $(A_p)_{p\in\mathbb{N}}$ une suite de $\mathcal{H}_n^{++}(\mathbb{C})$ convergeant vers $A \in \mathcal{H}_n^{++}(\mathbb{C})$, on note $A_p = \exp(B_p)$ et $A = \exp(B)$ avec B_p et B hermitiennes, il s'agit de montrer que $(B_p)_{p\in\mathbb{N}}$ converge vers B.

On munit $\mathcal{M}_n(\mathbb{C})$ de la norme induite par la norme 2. On dispose alors d'un lemme :

Lemme.
Soit $A \in \mathcal{H}_n(\mathbb{C})$, alors $\|A\|_2 = \rho(A)$, où ρ désigne le rayon spectral.

Utilisons ce lemme pour montrer que la suite $(B_p)_{p\in\mathbb{N}}$ est bornée, on montrera ensuite qu'elle admet une unique valeur d'adhérence pour conclure.

Les matrices A_p sont définies positives, donc leurs valeurs propres sont dans $]0, +\infty[$. De plus, la suite $(A_p)_{p\in\mathbb{N}}$ converge vers A donc est bornée, or $\rho(A_p) =$

$\|A_p\|_2$ donc les valeurs propres des A_p sont bornées. De même, la suite $(A_p^{-1})_{p\in\mathbb{N}}$ converge vers A^{-1} donc les valeurs propres des A_p^{-1} sont bornées. On en déduit que les valeurs propres des matrices A_p sont contenues dans un compact de $]0,+\infty[$. En considérant l'image par le logarithme de ces valeurs propres, on obtient que les valeurs propres des matrices B_p sont bornées. De plus, $\rho(B_p) = \|B_p\|_2$, donc la suite $(B_p)_{p\in\mathbb{N}}$ est bornée.

Soit maintenant $B_0 \in \mathcal{H}_n(\mathbb{C})$ une valeur d'adhérence de $(B_p)_{p\in\mathbb{N}}$, alors, par convergence de $(A_p)_{p\in\mathbb{N}}$ vers A, $\exp(B_0) = \exp(B)$ et donc $B_0 = B$ par l'injectivité prouvée précédemment. La suite $(B_p)_{p\in\mathbb{N}}$ est donc bornée et admet B comme unique valeur d'adhérence donc converge vers B. □

Démonstration du lemme. $A \in \mathcal{H}_n(\mathbb{C})$ donc A est diagonalisable dans une base orthonormée $(e_1,\dots,e_n)$. Si $\lambda_1,\dots,\lambda_n$ désignent les valeurs propres de A et si $X := x_1e_1 + \cdots + x_ne_n$ est un vecteur de $\mathbb{C}^n$ de norme 1, on a

$$\|AX\|_2^2 = \sum_{k=1}^{n} |x_k|^2|\lambda_k|^2 \leq \rho(A)^2 \sum_{k=1}^{n} |x_k|^2 = \rho(A)^2,$$

donc $\|A\|_2 \leq \rho(A)$.

Soit k tel que $\rho(A) = |\lambda_k|$, alors

$$\rho(A) = |\lambda_k| = \|Ae_k\|_2,$$

d'où $\|A\|_2 = \rho(A)$. □

Chapitre 3

Autres développements

3.1 Classification des groupes de pavage du plan

Référence :
– [Gob98] page 311.

On se place dans P un plan affine euclidien et on considère $\vec{P}$ son plan vectoriel euclidien associé.

Un réseau est un sous-groupe additif $\mathcal{R} \subseteq \vec{P}$ ayant les propriétés :
– $\mathcal{R}$ engendre $\vec{P}$ comme espace vectoriel
– Toute partie bornée de $\mathcal{R}$ est finie.

Proposition.
Les réseaux sont les sous-groupes additifs de $\vec{P}$ de la forme $\mathbb{Z}\vec{u} \oplus \mathbb{Z}\vec{v}$, $\vec{u}$ et $\vec{v}$ non colinéaires.

Soit $\mathcal{R}$ un réseau, $\vec{u}$ de norme minimum parmi les vecteurs non nuls de $\mathcal{R}$, $\vec{v}$ de norme minimum parmi les vecteurs non colinéaires à $\vec{u}$. Alors $\mathcal{R} = \mathbb{Z}\vec{u} \oplus \mathbb{Z}\vec{v}$.

On note $T(P)$ le groupe des translations de P.
Un sous-groupe G de $\mathrm{Isom}(P)$ est un groupe de pavage si $T := G \cap T(P)$ est formé des $t_{\vec{w}}$ où $\vec{w}$ décrit un réseau $\mathcal{R}$ de $\vec{P}$.

Théorème.
*Soit G un groupe de pavage inclus dans $Isom^+(P)$ (*i.e. *G est composé de déplacements).*
Soit T le sous-groupe des translations de G et $\mathcal{R}$ le réseau associé.
On note $\overline{G}$ le groupe des rotations vectorielles de G.
Alors :
– *$\overline{G}$ est cyclique d'ordre $n \in \{1, 2, 3, 4, 6\}$.*
– *$G = T \rtimes \overline{G}$*

Il y a donc 5 groupes de pavage composés de déplacements à isomorphisme près.

Le produit semi-direct est le même que celui de $\mathrm{Isom}(P)$.

Démonstration. Soit $f \in G$. Pour tout $\vec{w} \in \mathcal{R}$, $f t_{\vec{w}} f^{-1} = t_{\vec{f}(\vec{w})} \in G$, donc $\vec{f}(\vec{w}) \in \mathcal{R}$, donc $\mathcal{R}$ est stable par $\vec{f}$.

Soit $(\vec{u}, \vec{v})$ une base de $\mathcal{R}$. Alors

$$\mathrm{Mat}_{(\vec{u},\vec{v})}(\vec{f}) := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

est à coefficients entiers.
Or $f \in \mathrm{Isom}^+(P)$ donc f est une rotation d'angle θ et on a :
$\mathrm{Tr}(f) = a + d = 2\cos\theta \in \{-2, -1, 0, 1, 2\}$, d'où :

$$\theta \in \left\{ \pi, \frac{2\pi}{3}, -\frac{2\pi}{3}, \frac{\pi}{2}, -\frac{\pi}{2}, \frac{\pi}{3}, -\frac{\pi}{3}, 0 \right\}$$

Le groupe $\overline{G}$ est donc un groupe de rotations vectorielles fini, donc cyclique (car isomorphe à un sous-groupe de $\mathbb{C}^*$) d'ordre appartenant à $\{1, 2, 3, 4, 6\}$.

Décrivons maintenant G en fonction de l'ordre n de $\overline{G}$. Pour cela, on définit :

$$\mathcal{E} := \left\{ M \in P \ / \ r_M := \mathrm{rot}\left(M, \frac{2\pi}{n}\right) \in G \right\}$$

et on va étudier l'action naturelle de T sur $\mathcal{E}$.

On pose aussi $\overline{G} =< r >$ où r est la rotation vectorielle $r := \mathrm{rot}\left(\frac{2\pi}{n}\right)$.

Si $n = 1$, alors $G = T$. On suppose dorénavant $n > 1$.

Montrons que $\mathcal{E}$ est un réseau affine dont le réseau vectoriel associé $\vec{\mathcal{E}}$ est image de $\mathcal{R}$ par l'application linéaire $(\vec{\mathrm{id}} - r)^{-1}$.

Soit $\Omega \in \mathcal{E}$. Alors

$$M \in \mathcal{E} \iff r_M \in G \iff t_{\vec{w}} := r_M r_\Omega^{-1} \in T$$

Cherchons le lien entre $\overrightarrow{\Omega M}$ et $\vec{w}$.

On a

$$t_{\vec{w}}\, r_\Omega = r_M = t_{\overrightarrow{\Omega M}}\, r_\Omega\, t_{\overrightarrow{M\Omega}}$$

L'expression de gauche donne $r_M(\Omega) = \Omega + \vec{w}$.

Soit $N = t_{\overrightarrow{M\Omega}}(\Omega)$ le symétrique de M par rapport à Ω,
i.e.

$$r_M(\Omega) = r_\Omega(N) + \overrightarrow{\Omega M}$$

Alors

$$r_\Omega(N) + \overrightarrow{\Omega M} = \Omega + \vec{w} = r_\Omega(\Omega) + \vec{w}$$

D'où

$$\vec{w} = r(\overrightarrow{\Omega N}) + \overrightarrow{\Omega M} = (\vec{\mathrm{id}} - r)(\overrightarrow{\Omega M})$$

On en déduit

$$M \in \mathcal{E} \iff \overrightarrow{\Omega M} = (\vec{\mathrm{id}} - r)^{-1}(\vec{w})$$

pour un certain $\vec{w} \in \mathcal{R}$.

– Supposons $n = 2$, alors $r = -\vec{\mathrm{id}}$.
$\vec{\mathcal{E}}$ est donc l'image de $\mathcal{R}$ par l'homothétie vectorielle de rapport $\frac{1}{2}$.
Il y a ici 4 orbites pour l'action de T : si $(\vec{u}, \vec{v})$ est une base de $\mathcal{R}$, les 4 orbites sont $\Omega + \mathcal{R}$, $\Omega + \frac{1}{2}\vec{u} + \mathcal{R}$, $\Omega + \frac{1}{2}\vec{v} + \mathcal{R}$ et $\Omega + \frac{1}{2}\vec{u} + \frac{1}{2}\vec{v} + \mathcal{R}$, où $\Omega \in \mathcal{R}$.

– Supposons $n \in \{3, 4, 6\}$.
Soit $\vec{u}$ un vecteur de $\mathcal{R}$ de norme minimum et $\vec{v} = r(\vec{u})$. Alors $\vec{v} \in \mathcal{R}$ et $\|\vec{v}\| = \|\vec{u}\|$ donc $\vec{v}$ est aussi de norme minimum non colinéaire à $\vec{u}$, donc $(\vec{u}, \vec{v})$ est une base de $\mathcal{R}$ par la proposition.
On pose $\zeta := \exp\left(\dfrac{2i\pi}{n}\right)$, on a $\zeta \in \{i, j, -j^2\}$.
Prenons la bijection définie par :

$$\begin{aligned} \mathbb{C} &\longrightarrow P \\ a + b\zeta &\longmapsto \Omega + a\vec{u} + b\vec{v} \end{aligned}$$

où $a, b \in \mathbb{R}$.
Alors le réseau affine $\Omega + \mathcal{R}$ est formé des points dont l'affixe est dans l'anneau $\mathbb{Z}[\zeta]$.
Le réseau $\mathcal{E}$ est formé des points dont l'affixe est $\dfrac{z}{1-\zeta}$ où $z \in \mathbb{Z}[\zeta]$ car $(\vec{\mathrm{id}} - r)^{-1}$ est identifié à $z \mapsto \dfrac{z}{1-\zeta}$ ici.
On veut maintenant compter le nombre d'orbites pour l'action de T.
Si $n = 6$,

$$\frac{1}{1-\zeta} = \frac{1}{1+j^2} = \frac{1}{-j} = -j^2 \in \mathbb{Z}[-j^2]$$

donc $\vec{\mathcal{E}} = \mathcal{R}$ et il n'y a qu'une orbite.
Si $n = 4$,

$$\frac{1}{1-\zeta} = \frac{1}{1-i} = \frac{1+i}{2} \notin \mathbb{Z}[i]$$

donc il y a 2 orbites ($2.\frac{1+i}{2} \in \mathbb{Z}[i]$).
Si $n = 3$,

$$\frac{1}{1-\zeta} = \frac{1}{1-j} = \frac{1-j^2}{3} \notin \mathbb{Z}[j]$$

donc il y a 3 orbites.

□

Détails supplémentaires

– La deuxième partie de la preuve peut sembler un peu obscure et on comprend mieux ce qu'on fait si on a la représentation graphique en tête. Cette représentation consiste à considérer pour chaque valeur de n un pavage du plan qui est préservé par G. Le dénombrement des orbites de l'action de T sur les centres de rotations de G revient alors à compter le nombre de

ces centres de rotations dans chaque parallélogramme porté par les vecteurs de base du réseau associé au pavage (ce parallélogramme est appelé domaine fondamental du réseau).

– *Démonstration de la proposition.*

  – Soit $(\vec{u}, \vec{v})$ une base de $\vec{P}$ et $\mathcal{R} := \mathbb{Z}\vec{u} \oplus \mathbb{Z}\vec{v}$.
  Alors $\mathcal{R}$ engendre bien $\vec{P}$.
  Les normes étant équivalentes, on choisit la norme infinie :

$$\|x\vec{u} + y\vec{v}\| = \max(|x|, |y|)$$

  Alors toute partie bornée pour cette norme est finie, donc $\mathcal{R}$ est un réseau.

  – Soit $\mathcal{R}$ un réseau et $r > 0$ tel que $\{\vec{w} \in \mathcal{R} \setminus \{\vec{0}\} \ / \ \|\vec{w}\| \leq r\} \neq \emptyset$.
  Cet ensemble étant fini, il existe $\vec{u}$ dans cet ensemble de norme minimum.
  De même, il existe $\vec{v} \in \mathcal{R}$ de norme minimum parmi les vecteurs non colinéaires à $\vec{u}$.
  Montrons que $\mathcal{R} = \mathbb{Z}\vec{u} \oplus \mathbb{Z}\vec{v}$.
  Soit $\vec{w} \in \mathcal{R}$, $\vec{w} = x\vec{u} + y\vec{v}$ avec $(x, y) \in \mathbb{R}^2$.
  Soit $(p, q) \in \mathbb{Z}^2$ tel que

$$|x - p| \leq \frac{1}{2}, |y - q| \leq \frac{1}{2}$$

  Posons

$$\lambda := x - p, \mu := y - q, \vec{W} := \lambda\vec{u} + \mu\vec{v} \in \mathcal{R}$$

  On a

$$\|\vec{W}\| \leq |\lambda|\|\vec{u}\| + |\mu|\|\vec{v}\|$$

  avec égalité si et seulement si $\lambda\vec{u}$ et $\mu\vec{v}$ sont colinéaires, donc si et seulement si $\lambda = 0$ ou $\mu = 0$.
  Donc pour λ, μ non nuls, on a

$$\|\vec{W}\| < |\lambda|\|\vec{u}\| + |\mu|\|\vec{v}\| \leq \frac{1}{2}(\|\vec{u}\| + \|\vec{v}\|) \leq \|\vec{v}\|$$

  Sous ces conditions, $\vec{W}$ doit donc être colinéaire à $\vec{u}$, ce qui contredit $\mu \neq 0$. Donc $\mu = 0$ et $\|\vec{W}\| \leq \frac{1}{2}\|\vec{u}\| < \|\vec{u}\|$, d'où $\lambda = 0$, ce qui conclut la preuve.

□

3.2 Densité des fonctions continues nulle part dérivables

Référence :

– [Gou08] page 401.
On note $I := [0,1]$ et $\mathcal{C} := \mathcal{C}([0,1], \mathbb{R})$ muni de la norme infinie.

Théorème.
Le sous-ensemble de $\mathcal{C}$ des fonctions continues nulle part dérivables est dense dans $\mathcal{C}$.

Démonstration. Pour $\varepsilon > 0$ et $n \in \mathbb{N}$ on considère

$$U_{\varepsilon,n} := \left\{ f \in \mathcal{C} \mid \forall x \in I, \exists y \in I, 0 < |y - x| < \varepsilon, \quad \left| \frac{f(y) - f(x)}{y - x} \right| > n \right\}.$$

Les étapes de la preuve sont les suivantes :

1. $U_{\varepsilon,n}$ est un ouvert de $\mathcal{C}$.
2. $U_{\varepsilon,n}$ est dense dans $\mathcal{C}$.
3. L'ensemble des fonctions continues nulle part dérivables contient une intersection dénombrable d'ensembles $U_{\varepsilon,n}$, ce qui permettra de conclure par le théorème de Baire.

1. Montrons que le complémentaire $F_{\varepsilon,n}$ de $U_{\varepsilon,n}$ dans $\mathcal{C}$ est fermé. On a

   $$F_{\varepsilon,n} = \{ f \in \mathcal{C} \mid \exists x \in E, \forall y \in I, |y - x| < \varepsilon, \quad |f(y) - f(x)| \leq n|y - x| \}.$$

   Soit $(f_p)_{p \in \mathbb{N}}$ une suite de $F_{\varepsilon,n}$ convergeant vers $f \in \mathcal{C}$, montrons que $f \in F_{\varepsilon,n}$.
   Pour tout $p \in \mathbb{N}, f_p \in F_{\varepsilon,n}$ donc il existe $x_p \in I$ tel que

   $$\forall y \in I, |y - x_p| < \varepsilon, \quad |f_p(y) - f_p(x_p)| \leq n|y - x_p|.$$

   La suite (x_p) prend ses valeurs dans le compact I donc quitte à extraire on peut supposer qu'elle converge vers $x \in I$.
   Soit $y \in I$ tel que $|y - x| < \varepsilon$. Il existe $P \in \mathbb{N}$ tel que $|y - x_p| < \varepsilon$ pour tout $p \geq P$. Ainsi

   $$\forall p \geq P, \qquad |f_p(y) - f_p(x_p)| \leq n|y - x_p|.$$

   En faisant tendre p vers l'infini on a alors $|f(y) - f(x)| \leq n|y - x|$. En effet, la suite (f_p) converge uniformément vers f continue donc $f_p(x_p) \longrightarrow f(x)$. On en déduit que $f \in F_{\varepsilon,n}$.
2. Soit désormais $f \in \mathcal{C}$ et $\delta > 0$. Pour montrer que $U_{\varepsilon,n}$ est dense, il s'agit de trouver $g \in U_{\varepsilon,n}$ tel que $\|f - g\|_\infty \leq \delta$. Cherchons g sous la forme $x \mapsto f(x) + \delta \sin(Nx)$. On a bien $\|f - g\|_\infty \leq \delta$.
   Soit $x \in I$. Pour $y \in I$ on a

   $$\left| \frac{g(y) - g(x)}{y - x} \right| \geq \delta \left| \frac{\sin(Ny) - \sin(Nx)}{y - x} \right| - \left| \frac{f(y) - f(x)}{y - x} \right|.$$

Le but étant de minorer ce terme par n pour un y proche de x. Il est alors nécessaire d'encadrer $|y-x|$.
Pour tout $N \geq 4\pi$, il existe $y \in I$ tel que

$$2\pi \leq |Nx - Ny| \leq 4\pi \qquad \text{et} \qquad |\sin(Nx) - \sin(Ny)| \geq 1.$$

On a alors

$$\frac{2\pi}{N} \leq |x-y| \leq \frac{4\pi}{N}.$$

D'où

$$\left|\frac{g(y)-g(x)}{y-x}\right| \geq \frac{\delta N}{4\pi} - |f(y)-f(x)|\frac{N}{2\pi}.$$

Or f est uniformément continue sur I compact donc :

$$\exists \alpha \in]0, \varepsilon[, \forall (x,y) \in I^2, |x-y| < \alpha, \quad |f(x)-f(y)| < \frac{\delta}{4}.$$

En choisissant N tel que $\frac{4\pi}{N} < \alpha$, on a alors

$$\left|\frac{g(y)-g(x)}{y-x}\right| > \frac{\delta N}{8\pi}.$$

Puis en choisissant N tel que $\frac{\delta N}{8\pi} > n$ on obtient la minoration souhaitée et on a bien $0 < |y-x| < \alpha < \varepsilon$.

3. Posons

$$R := \bigcap_{n \in \mathbb{N}^*} U_{1/n,n}.$$

Alors, par le théorème de Baire, R est dense dans $\mathcal{C}$ complet comme intersection dénombrable d'ouverts denses.
Soit $f \in R$, montrons que f est nulle part dérivable.
Soit $x \in I$. Pour tout n, $f \in U_{1/n,n}$ donc

$$\forall n \in \mathbb{N}^*, \exists x_n \in I, 0 < |x - x_n| < \frac{1}{n}, \quad \left|\frac{f(x)-f(x_n)}{x-x_n}\right| > n.$$

Donc $x_n \longrightarrow x$ et $\left|\frac{f(x)-f(x_n)}{x-x_n}\right| \longrightarrow +\infty$, donc f n'est pas dérivable en x.
Finalement, f est nulle part dérivable.

□

3.3 Espace de Sobolev $H^1(I)$

Référence :
– [Bre05] page 123.

Soit $I :=]a, b[$ un intervalle ouvert borné non vidé de $\mathbb{R}$. On note

$$H^1(I) := \{u \in L^2(I) \mid \exists v \in L^2(I), \forall \varphi \in \mathcal{C}_c^\infty(I), \int_I u\varphi' = -\int_I v\varphi\}.$$

Lorsqu'un tel v existe, il est unique et on le note u'. On munit alors $H^1(I)$ du produit scalaire

$$\begin{aligned} H^1(I) \times H^1(I) &\longrightarrow \mathbb{R} \\ \langle u, v\rangle_{H^1} &\longmapsto \int_I uv + \int_I u'v' \end{aligned}$$

et on note $\|\cdot\|_{H^1}$ la norme associée, elle vérifie

$$\|u\|_{H^1}^2 = \|u\|_{L^2}^2 + \|u'\|_{L^2}^2.$$

Théorème.
On a les propriétés suivantes :

(i) $H^1(I)$ *est un espace de Hilbert.*

(ii) $H^1(I)$ *s'injecte de façon compacte dans* $\mathcal{C}(\bar{I})$.

Démonstration. (i) $H^1(I)$ est un espace préhilbertien, il suffit donc de montrer qu'il est complet.

Soit $(u_n)_{n\in\mathbb{N}}$ une suite de Cauchy de $H^1(I)$. D'après la définition de la norme $\|\cdot\|_{H^1}$, $(u_n)_{n\in\mathbb{N}}$ et $(u_n')_{n\in\mathbb{N}}$ sont de Cauchy dans $L^2(I)$ qui est complet, donc admettent des limites respectives u et v. Montrons que $v = u'$: pour $\varphi \in \mathcal{C}_c^\infty(I)$, on a

$$\left|\int_I (v - u_n')\varphi\right| \leq \|v - u_n'\|_2 \|\varphi\|_2$$

par l'inégalité de Cauchy-Schwarz, d'où $\int_I v\varphi = \lim_{n\to+\infty} \int_I u_n'\varphi$. On a donc

$$\int_I v\varphi = \lim_{n\to+\infty} -\int_I u_n\varphi' = -\int_I u\varphi'$$

pour la même raison. On en déduit que $u \in H^1(I)$ et on a $\|u - u_n\|_{H^1} \xrightarrow[n\to+\infty]{} 0$, d'où le résultat.

(ii) Montrons d'abord que tout élément de $H^1(I)$ a un représentant dans $\mathcal{C}(\bar{I})$. Pour $u \in H^1(I)$, on pose

$$\tilde{u}(x) := \int_a^x u'(t)\,\mathrm{d}t.$$

I est borné donc $\tilde{u}$ est bien définie et c'est une fonction continue sur $[a, b]$.

Montrons que $\tilde{u} \in H^1(I)$ et que $\tilde{u}' = u'$: pour $\varphi \in \mathcal{C}_c^\infty(I)$, on a

$$\begin{aligned}\int_I \tilde{u}\varphi' &= \int_a^b \int_a^x u'(t)\,\mathrm{d}t\,\varphi'(x)\,\mathrm{d}x \\ &= \int_a^b \int_t^b \varphi'(x)\,\mathrm{d}x\,u'(t)\,\mathrm{d}t \quad \text{par Fubini} \\ &= \int_I -\varphi(t)u'(t)\,\mathrm{d}t \quad \text{car } \varphi \text{ est à support compact,}\end{aligned}$$

d'où le résultat. On en déduit qu'il existe $C \in \mathbb{R}$ tel que $u = \tilde{u} + C$ p.p., et donc que u admet un représentant continu. On remarque qu'on a aussi

$$u(y) - u(x) = \tilde{u}(y) - \tilde{u}(x) = \int_x^y u'(t)\,\mathrm{d}t.$$

Montrons que l'injection qu'on a obtenue dans $\mathcal{C}(\bar{I})$ est compacte. Soit B la boule unité de $H^1(I)$, montrons que B est relativement compacte dans $\mathcal{C}(\bar{I})$ grâce au théorème d'Ascoli.
– B est ponctuellement bornée : pour $x \in [a,b]$ et $u \in B$, on a

$$\begin{aligned}|u(x)| &= \left|\frac{1}{b-a}\int_a^b u(x)\,\mathrm{d}y\right| \\ &= \left|\frac{1}{b-a}\int_a^b \left(\int_y^x u'(t)\,\mathrm{d}t - u(y)\right)\,\mathrm{d}y\right| \\ &\leq \frac{1}{b-a}\int_a^b \int_y^x |u'(t)|\,\mathrm{d}t\,\mathrm{d}y - \frac{1}{b-a}\int_I |u| \\ &\leq \int_a^b |u'(t)|\,\mathrm{d}t + \frac{1}{b-a}\int_I |u| \\ &\leq \sqrt{b-a}\|u'\|_2 + \frac{1}{\sqrt{b-a}}\|u\|_2 \quad \text{par Cauchy-Schwarz} \\ &\leq \sqrt{b-a} + \frac{1}{\sqrt{b-a}}.\end{aligned}$$

– B est équicontinue : pour $x < y \in [a,b]$ et $u \in B$, on a

$$|u(x) - u(y)| \leq \int_x^y |u'(t)|\,\mathrm{d}t \leq \sqrt{y-x},$$

d'où le résultat.
Par le théorème d'Ascoli, B est relativement compact dans $\mathcal{C}(\bar{I})$ donc l'injection $H^1(I) \hookrightarrow \mathcal{C}(\bar{I})$ est compacte.

□

Détails supplémentaires

– Montrons l'unicité de u' : soit $v, w \in L^2$ telles que

$$\forall \varphi \in \mathcal{C}_c^\infty(I), \quad \int_I u\varphi' = -\int_I v\varphi = -\int_I w\varphi.$$

Alors pour tout $\varphi \in \mathcal{C}_c^\infty(I)$, $\int_I (v-w)\varphi = 0$, d'où $v = w$.

–

Lemme.
Soit $f \in L^1_{loc}$ telle que

$$\forall \varphi \in \mathcal{C}_c^\infty(I), \quad \int_I f\varphi' = 0.$$

Alors il existe une constante C telle que $f = C$ p.p.

Démonstration. Soit $\psi \in \mathcal{C}_c^\infty(I)$ telle que $\int_I \psi = 1$. Alors pour tout $w \in \mathcal{C}_c^\infty(I)$, il existe $\varphi \in \mathcal{C}_c^\infty(I)$ telle que

$$\varphi' = w - \left(\int_I w\right)\psi.$$

En effet, $h := w - \left(\int_I w\right)\psi$ est dans $\mathcal{C}_c^\infty(I)$ et $\int_I h = 0$ donc h admet une primitive à support compact. On a alors

$$0 = \int_I f\varphi' = \int_I f\left(w - \psi\int_I w\right),$$

et donc, pour tout $w \in \mathcal{C}_c^\infty(I)$,

$$\begin{aligned} 0 &= \int_I fw - \int_I\int_I w(x)f(y)\psi(y)\,\mathrm{d}y\,\mathrm{d}x \quad \text{par Fubini} \\ &= \int_I w\left(f - \int_I f\psi\right). \end{aligned}$$

Donc $f = \int_I f\psi =: C$ p.p. □

3.4 Inégalités de Kolmogorov

Références :
– [Gou94] page 81 ;
– [FGN03] page 259.

Théorème.
Soit $f \in \mathcal{C}^n(\mathbb{R}, \mathbb{C}), n \geq 2$.
Pour $k \in \{0, \dots, n\}$, on note $M_k = \sup_{x\in\mathbb{R}} |f^{(k)}(x)|$.
On suppose que M_0 et M_n sont finis.
Alors pour tout $k \in \{0, \dots, n\}$:

(i) M_k *est fini*

(ii) $M_1 \leq \sqrt{2M_0M_2}$

(iii) $M_k \leq 2^{\frac{k(n-k)}{2}} M_0^{1-\frac{k}{n}} M_n^{\frac{k}{n}}$.

Démonstration.

(i) Soit $x \in \mathbb{R}$. Pour tout $i \in \{1, \dots, n-1\}$, d'après l'inégalité de Taylor-Lagrange, on a :

$$\left| f(x+i) - f(x) - if'(x) - \cdots - \frac{i^{n-1}}{(n-1)!} f^{(n-1)}(x) \right| \leq \frac{i^n M_n}{n!}$$

D'où, par inégalité triangulaire,

$$\begin{aligned} \left| if'(x) + \cdots + \frac{i^{n-1}}{(n-1)!} f^{(n-1)}(x) \right| &\leq 2M_0 + \frac{i^n M_n}{n!} \\ &\leq 2M_0 + \frac{n^n M_n}{n!} \end{aligned}$$

Si on note $X(x)$ le vecteur colonne de $\mathbb{C}^{n-1}$ dont les composantes sont les $\frac{f^{(k)}(x)}{k!}, k \in \{1, \dots, n-1\}$, on en déduit $\|AX(x)\|_\infty \leq K := 2M_0 + \frac{n^n M_n}{n!}$ où :

$$A = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 2 & 2^2 & \cdots & 2^{n-1} \\ \vdots & \vdots & & \vdots \\ n-1 & (n-1)^2 & \cdots & (n-1)^{n-1} \end{pmatrix}$$

A est inversible car son déterminant est de Vandermonde, donc :

$$\forall x \in \mathbb{R}, \qquad \|X(x)\|_\infty \leq \|A^{-1}\| K$$

Les M_k sont donc finis.

(ii) Soit $x \in \mathbb{R}$, soit $h > 0$, par l'inégalité de Taylor-Lagrange on a :

$$|f(x+h) - f(x) - hf'(x)| \leq \frac{h^2 M_2}{2}$$

et :

$$|f(x-h) - f(x) + hf'(x)| \leq \frac{h^2 M_2}{2}$$

D'où :

$$|f(x+h) - f(x-h) - 2hf'(x)| \leq h^2 M_2$$

et :

$$2h|f'(x)| \leq h^2 M_2 + |f(x+h) - f(x-h)| \leq h^2 M_2 + 2M_0$$

On en déduit $M_1 \leq \frac{hM_2}{2} + \frac{M_0}{h}$ pour tout h.

Le membre de droite étant minimal en $h = \sqrt{\frac{2M_0}{M_2}}$, on obtient :

$$M_1 \leq \sqrt{2M_0M_2}$$

(iii) Montrons le résultat par récurrence sur n.

Pour $n = 2$ et $k = 1$, le résultat a été prouvé en (ii), pour $k = 0$ ou $k = n$ c'est évident.

Supposons le résultat vrai jusqu'au rang m et considérons f de classe $\mathcal{C}^{m+1}$.

Soit $j \in \{1, \ldots, m\}$. En appliquant le cas $n = 2, k = 1$ à $f^{(j-1)}$, on a :

$$M_j^2 \leq 2M_{j-1}M_{j+1}$$

Par hypothèse de récurrence dans le cas $n = j, k = j - 1$, on a :

$$M_{j-1} \leq 2^{\frac{j-1}{2}} M_0^{\frac{1}{j}} M_j^{\frac{j-1}{j}}$$

Par ailleurs, par hypothèse de récurrence dans le cas $n = m + 1 - j, k = 1$ sur la fonction $f^{(j)}$, on a :

$$M_{j+1} \leq 2^{\frac{m-j}{2}} M_j^{\frac{m-j}{m+1-j}} M_{m+1}^{\frac{1}{m+1-j}}$$

On obtient alors :

$$M_j^2 \leq 2^{\frac{m+1}{2}} M_0^{\frac{1}{j}} M_j^{\frac{j-1}{j} + \frac{m-j}{m+1-j}} M_{m+1}^{\frac{1}{m+1-j}}$$

En élevant le résultat à la puissance $\frac{j(m+1-j)}{m+1}$, on obtient finalement :

$$M_j \leq 2^{\frac{j(m+1-j)}{2}} M_0^{1-\frac{j}{m+1}} M_{m+1}^{\frac{j}{m+1}}$$

ce qui conclut la récurrence.

□

3.5 Irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$

Référence :
– [Gou09] page 92.

Théorème.
Φ_n est irréductible sur $\mathbb{Q}$.

Démonstration. Montrons d'abord que Φ_n s'écrit sous la forme :

$$\Phi_n = \prod_{i=1}^{r} F_i$$

avec $F_i \in \mathbb{Z}[X]$ irréductible sur $\mathbb{Q}$.

$\mathbb{Q}[X]$ est factoriel donc il existe un unique r-uplet $(G_1, \ldots, G_r)$ d'irréductibles de $\mathbb{Q}[X]$ tel que :

$$\Phi_n = \prod_{i=1}^{r} G_i$$

De plus, pour tout $i \in \{1, \ldots, r\}$, il existe $\alpha_i \in \mathbb{N}^*$ tel que $\alpha_i G_i \in \mathbb{Z}[X]$.
On a alors :

$$\left(\prod_{i=1}^{r} \alpha_i\right) \Phi_n = \prod_{i=1}^{r} \alpha_i G_i$$

Or Φ_n est unitaire donc, si c désigne le contenu d'un polynôme de $\mathbb{Z}[X]$, d'après le lemme de Gauss,

$$\prod_{i=1}^{r} \alpha_i = c\left(\left(\prod_{i=1}^{r} \alpha_i\right) \Phi_n\right) = \prod_{i=1}^{r} c(\alpha_i G_i)$$

Posons, pour $i \in \{1, \ldots, r\}$,

$$F_i := \frac{\alpha_i G_i}{c(\alpha_i G_i)}$$

Alors pour tout $i \in \{1, \ldots, r\}, F_i \in \mathbb{Z}[X]$ est unitaire et irréductible sur $\mathbb{Q}$ et :

$$\Phi_n = \prod_{i=1}^{r} F_i$$

Montrons maintenant par récurrence sur s la propriété suivante : pour tout entier $s \geq 1$, pour tout entier k premier avec n et de décomposition en facteurs premiers $k = p_1 \cdots p_s$ et pour toute racine ξ de F_1, on a $F_1(\xi^k) = 0$.

– $s = 1$.
Soit ξ une racine de F_1 et soit p un nombre premier tel que $p \nmid n$.
Montrons que $F_1(\xi^p) = 0$.

ξ est une racine de Φ_n donc est une racine primitive n-ième de l'unité. Comme $p \wedge n = 1$, ξ^p est également une racine primitive n-ième de l'unité donc une racine de Φ_n. Il existe donc i tel que $F_i(\xi^p) = 0$.

Les polynômes $F_1(X)$ et $F_i(X^p)$ ont ξ comme racine commune donc ne sont pas premiers entre eux dans $\mathbb{Q}[X]$.

Or F_1 est irréductible sur $\mathbb{Q}$ donc $F_1(X) \mid F_i(X^p)$ dans $\mathbb{Q}[X]$. De plus, le coefficient dominant de F_1 est inversible dans $\mathbb{Z}$, donc en effectuant la division euclidienne dans $\mathbb{Z}[X]$ et par unicité de celle-ci dans $\mathbb{Q}[X]$, on en déduit que :

$$F_1(X) \mid F_i(X^p) \text{ dans } \mathbb{Z}[X].$$

Si on note, pour $P \in \mathbb{Z}[X]$, $\overline{P} \in \mathbb{F}_p[X]$ la classe de P modulo p, on a alors $\overline{F_1}(X) \mid \overline{F_i}(X^p) = \overline{F_i}(X)^p$ dans $\mathbb{F}_p[X]$.
Soit $P \in \mathbb{F}_p[X]$ un facteur irréductible de $\overline{F_1}$ sur $\mathbb{F}_p$. Alors $P \mid \overline{F_i}^p$, donc par irréductibilité de P, $P \mid \overline{F_i}$.
On suppose que $i \neq 1$, alors $P^2 \mid \overline{\Phi_n} \mid X^n - \overline{1}$, donc $X^n - \overline{1} = P^2 S$ pour un $S \in F_p[X]$.
En dérivant, on obtient :

$$\overline{n} X^{n-1} = \overline{2} P P' S + P^2 S'$$

Donc $P \mid \overline{n} X^{n-1} \mid \overline{n} X^n$ dans $\mathbb{F}_p[X]$. Or :

$$P \mid X^n - 1 \mid \overline{n} X^n - \overline{n}$$

D'où $P \mid \overline{n} \neq 0$ (car $p \not| n$), donc P est constant, ce qui est absurde.
Finalement, $i = 1$ et $F_1(\xi^p) = 0$.

– Supposons la propriété vérifiée au rang $s \geq 1$.
Soit ξ une racine de F_1 et $k = p_1 \cdots p_{s+1}$ un entier premier avec n.
Alors $p_1 \cdots p_s \wedge n = 1$ donc par hypothèse de récurrence, $F_1(\xi^{p_1 \cdots p_s}) = 0$.
De plus, $p_{s+1} \wedge n = 1$ donc comme la propriété est vraie au rang 1 et que $\xi^{p_1 \cdots p_s}$ est une racine de F_1, on a $F((\xi^{p_1 \cdots p_s})^{p_{s+1}}) = 0$, d'où le résultat.

Pour conclure, fixons une racine ξ de F_1. Alors ξ est une racine de Φ_n donc $\mu_n^*(\mathbb{C}) = \{\xi^k \mid k \wedge n = 1\}$.

Les racines de Φ_n sont donc comprises dans celles de F_1, donc $\Phi_n \mid F_1$. Or $F_1 \mid \Phi_n$ et ces deux polynômes sont unitaires donc $F_1 = \Phi_n$, d'où le résultat. □

3.6 Le folium de Descartes

Référence :
– [Rou09] page 237.
Soit $f : (x, y) \mapsto x^3 + y^3 - 3xy$.
Soit $C := f^{-1}(0)$.
C est appelé folium de Descartes, le but de ce développement est de le décrire.

– Commençons par définir, dans l'équation de C, y comme fonction implicite de x, lorsque cela est possible.
f est de classe $\mathcal{C}^\infty$ de $\mathbb{R}^2$ dans $\mathbb{R}$. Le théorème des fonctions implicites lui est applicable au voisinage de (a, b) si :

$$f(a, b) = 0 \text{ et } \frac{\partial f}{\partial y}(a, b) = 3(b^2 - a) \neq 0$$

Il existe dans ce cas un voisinage V de a, un voisinage W de b et une fonction $\varphi : V \to W$ de classe $\mathcal{C}^\infty$ tels que :

$$(x \in V, y \in W \text{ et } (x,y) \in C) \iff (x \in V \text{ et } y = \varphi(x))$$

La tangente à C au point (a,b) a pour équation :

$$y - b = \varphi'(a)(x - a)$$

Pour $x \in V$, on a $f(x, \varphi(x)) = 0$ donc :

$$\frac{\partial f}{\partial x}(x,y) + \varphi'(x)\frac{\partial f}{\partial y}(x,y) = 0$$

d'où :

$$\varphi'(x) = -\frac{\frac{\partial f}{\partial x}(x,y)}{\frac{\partial f}{\partial y}(x,y)}$$

i.e.

$$\varphi'(x) = -\frac{x^2 - y}{y^2 - x}$$

La tangente à C au point (a,b) a donc pour équation :

$$(a^2 - b)(x - a) + (b^2 - a)(y - b) = 0$$

– Il y a deux couples (a,b) tels que $\frac{\partial f}{\partial y}(a,b) = 0$: $(a,b) = (0,0)$ et $(a,b) = (2^{2/3}, 2^{1/3}) = A$. Au point A, on a :

$$\frac{\partial f}{\partial x}(a,b) = 3(a^2 - b) = 3 \cdot 2^{1/3} \neq 0$$

On peut donc exprimer x comme fonction implicite de y au voisinage de ce point et puisque $\frac{\partial f}{\partial y}(a,b) = 0$, on a une tangente verticale en A.
À l'origine on a par contre $\frac{\partial f}{\partial y}(a,b) = \frac{\partial f}{\partial x}(a,b) = 0$ donc le théorème des fonctions implicites n'est pas applicable directement.

– Donnons maintenant une représentation paramétrique de C. Pour cela, on étudie l'intersection de C avec la droite $y = tx$:

$$\begin{cases} x^3 + y^3 - 3xy = 0 \\ y = tx \end{cases}$$

i.e.

$$\begin{cases} x^2((1+t^3)x - 3t) = 0 \\ y = tx \end{cases}$$

La première équation en x a 0 comme racine double, ce qui donne le point $(x,y) = (0,0)$, et une troisième racine, si $t \neq -1$, qui donne le point :

$$(x,y) = \left(\frac{3t}{1+t^3}, \frac{3t^2}{1+t^3}\right)$$

– Cette équation paramétrique nous permet d'établir le tableau de variation suivant :

t	$-\infty$			-1			0		$2^{-1/3}$		$2^{1/3}$		$+\infty$
x	0	$\nearrow$	$+\infty$	$\|\|$	$-\infty$	$\nearrow$	0	$\nearrow$	$2^{2/3}$	$\searrow$	$2^{1/3}$	$\searrow$	0
y	0	$\searrow$	$-\infty$	$\|\|$	$+\infty$	$\searrow$	0	$\nearrow$	$2^{1/3}$	$\nearrow$	$2^{2/3}$	$\searrow$	0

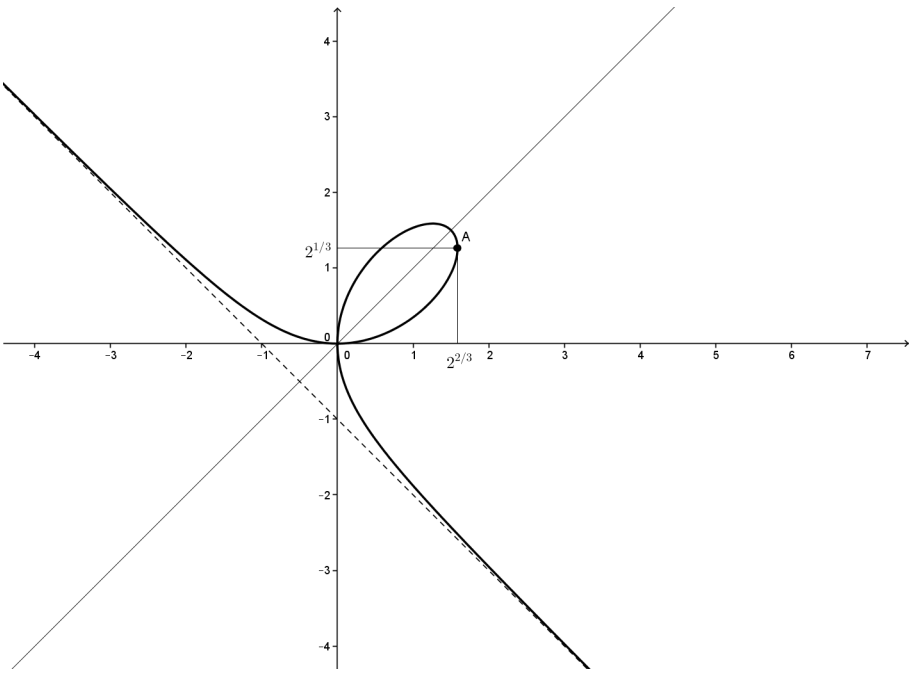
Il y a donc deux passages par l'origine : l'un pour $t = 0$, avec tangente horizontale car $y/x = t$ tend vers 0, et l'autre déduit du premier par symétrie par rapport à la première bissectrice (car $f(a, b) = f(b, a)$), avec tangente verticale (correspondant ici à $t \to \pm\infty$).
Étude de la branche infinie en $t \to -1$: $y/x = t$ tend vers -1 donc la direction asymptotique est celle de la droite $y = -x$. De plus,

$$y - (-1)x = \frac{3t^2 + 3t}{1 + t^3} = \frac{3t}{1 - t + t^2} \to -1$$

donc $x + y + 1 \to 0$ pour $t \to -1$ et la distance euclidienne du point (x, y) à la droite d'équation $ax + by + c = 0$ est $|ax + by + c|/\sqrt{a^2 + b^2}$, donc la droite d'équation $x + y + 1 = 0$ est asymptote à C.
On a enfin :

$$x + y + 1 = \frac{(1 + t)^3}{1 + t^3} = \frac{(1 + t)^2}{1 - t + t^2} > 0 \text{ pour } t \neq -1$$

donc C est au-dessus de l'asymptote.



3.7 Réduction des endomorphismes normaux

Référence :
– [Gou09] page 258.

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

$$Mat_B(u) = \begin{pmatrix} \lambda_1 & & & & & & \\ & \ddots & & & 0 & & \\ & & \lambda_r & & & & \\ & & & D_1 & & & \\ & 0 & & & \ddots & & \\ & & & & & D_s & \end{pmatrix}$$

avec $\lambda_i \in \mathbb{R}$ et $D_j = \begin{pmatrix} a_j & -b_j \\ b_j & a_j \end{pmatrix} \in \mathcal{M}_2(\mathbb{R})$.

Lemme.
Soit $u \in \mathcal{L}(E)$ et F un s.e.v de E stable par u, alors $F^\perp$ est stable par u^*.

Démonstration.

$$\forall x \in F, \forall y \in F^\perp, \langle u^*(y)|x\rangle = \langle y|u(x)\rangle = 0$$

car $u(x) \in F$, donc $u^*(y) \in F^\perp$. □

Lemme.
Soit $u \in \mathcal{L}(E)$ un endomorphisme normal, soit E_λ un sous-espace propre de u.
Alors $E_\lambda^\perp$ est stable par u.

Démonstration. u et u^* commutent donc E_λ est stable par u^*, donc $E_\lambda^\perp$ est stable par u d'après le lemme 1. □

Démonstration du théorème. On procède par récurrence sur $n := \dim E$.

Pour $n = 1$, c'est évident. Supposons le résultat vrai jusqu'au rang $n-1$.

– Si u admet une valeur propre réelle λ, alors $F := E_\lambda^\perp$ est stable par u (lemme 2) et par u^* (lemme 1). Comme $u_{|F}$ est normal et que $\dim F \leq n-1$, l'hypothèse de récurrence fournit une base orthonormale de F qui, concaténée avec une base orthonormale de E_λ, donne la forme voulue pour u.

– Sinon, u est sans valeur propre réelle.

Soit λ une valeur propre de u, on note

$$P := (X-\lambda)(X-\bar{\lambda}) = X^2 - (\lambda+\bar{\lambda})X + \lambda\bar{\lambda} \in \mathbb{R}[X].$$

Alors $P \mid \pi_u$ et donc $N := \ker((u-\lambda\mathrm{id})(u-\bar{\lambda}\mathrm{id}))$ est non réduit à $\{0\}$. N est stable par u et par u^* car u^* commute avec u. On pose $v := u_{|N}$, on a $v^* = u^*_{|N}$.

Alors v^*v est symétrique donc possède une valeur propre $\mu \in \mathbb{R}$. Soit x un vecteur propre associé et $F := \text{vect}(x, u(x))$.

u n'admet pas de valeur propre réelle donc $\dim F = 2$ et F est stable par u car $x \in N$ donc

$$u^2(x) = (\lambda + \bar{\lambda})u(x) - \lambda\bar{\lambda}x. \tag{3.1}$$

Montrons que F est stable par u^*. Par (1), on a que $F = \text{vect}(u(x), u^2(x))$ car $\lambda\bar{\lambda} \neq 0$. On a alors

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

et

$$u^*(u^2(x)) = u \circ u^*(u(x)) = u(\mu x) = \mu u(x) \in F.$$

Puisque $(u_{|F})^* = (u^*)_{|F}$, $u_{|F}$ est un endomorphisme normal d'un espace de dimension 2. On dispose alors du lemme suivant :

Lemme.
Soit E un espace euclidien de dimension 2. Soit $u \in \mathcal{L}(E)$ un endomorphisme normal n'admettant pas de valeurs propres réelles.

Alors pour toute base B orthonormale de E, on a

$$Mat_B(u) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

avec $b \neq 0$.

Ce lemme se prouve par le calcul en utilisant le fait que u n'est pas symétrique.

Il existe donc une base B_2 de F dans laquelle la matrice de $u_{|F}$ est de la forme de celle du lemme. De plus, F est stable par u et par u^* donc $F^\perp$ est stable par u^* et par u d'après le lemme 1.

$u_{|F^\perp}$ est normal et $\dim F^\perp = n - 2 < n$ donc l'hypothèse de récurrence fournit une base B_1 orthonormale de $F^\perp$ qui, concaténée avec B_2, donne la forme voulue pour u. □

Remarque. La première partie de cette démonstration montre qu'un endomorphisme normal d'un espace hermitien est diagonalisable dans une base orthonormale car $\mathbb{C}$ est algébriquement clos. Elle montre aussi qu'un endomorphisme symétrique d'un espace euclidien est diagonalisable en base orthonormale car toutes ses valeurs propres sont réelles.

3.8 Théorème d'Ascoli

Soit (X, d) un espace métrique compact et (X', d') un espace métrique.
Soit E une partie de $\mathcal{C}^0(X, X')$.

Définition.

- E est équicontinue si :

$$\forall x \in X, \forall \varepsilon > 0, \exists \eta > 0, \forall y \in X, \forall f \in E, d(x,y) < \eta \Rightarrow d'(f(x), f(y)) < \varepsilon$$

- E est uniformément équicontinue si :

$$\forall \varepsilon > 0, \exists \eta > 0, \forall x, y \in X, \forall f \in E, d(x,y) < \eta \Rightarrow d'(f(x), f(y)) < \varepsilon$$

- E est ponctuellement truc si :

$$\forall x \in X, \{f(x), f \in E\} \text{ est truc}$$

On rappelle que dans notre cas où X est compact, équicontinue est équivalent à uniformément équicontinue.

Démonstration. Il est évident que uniformément équicontinue implique équicontinue.

Supposons E équicontinue.

Soit $\varepsilon > 0$. Alors pour tout $x \in X$, il existe $\eta_x > 0$ tel que :

$$\forall y \in X, \forall f \in E, d(x,y) < \eta_x \Rightarrow d'(f(x), f(y)) < \varepsilon$$

$\bigcup_{x \in X} B\left(x, \frac{\eta_x}{2}\right)$ est un recouvrement d'ouverts de X, et X est compact, donc il existe $x_1, \ldots, x_n \in X$ tels que $X = \bigcup_{i=1}^{n} B\left(x_i, \frac{\eta_{x_i}}{2}\right)$.

On pose $\eta := \min_{1 \leq i \leq n} \frac{\eta_{x_i}}{2}$.

Soit $f \in E$ et $x, y \in X$ tels que $d(x,y) < \eta$.

Soit $i \in \{1, \ldots, n\}$ tel que $x \in B\left(x_i, \frac{\eta_{x_i}}{2}\right)$.

Alors $d(x, x_i) < \eta_{x_i}$ donc $d'(f(x), f(x_i)) < \varepsilon$ et :

$$d(y, x_i) \leq d(y,x) + d(x, x_i) < \eta + \frac{\eta_{x_i}}{2} \leq \eta_{x_i}$$

donc $d'(f(y), f(x_i)) < \varepsilon$.

Finalement :

$$d'(f(x), f(y)) \leq d'(f(x), f(x_i)) + d'(f(x_i), f(y)) < 2\varepsilon$$

Donc E est uniformément équicontinue. □

Théorème (Ascoli)**.**
E est relativement compact pour la topologie de la convergence uniforme si et seulement si E est équicontinue et ponctuellement relativement compacte.

Démonstration.

$\Rightarrow$: – Soit $x \in X$, on note $E(x) := \{f(x), f \in E\}$. Montrons que $E(x)$ est relativement compact.
L'application :

$$\begin{aligned} \Phi_x : \mathcal{C}^0(X, X') &\longrightarrow X' \\ f &\longmapsto f(x) \end{aligned}$$

est 1-lipschitzienne donc continue, donc $\overline{E}(x) = \Phi_x(\overline{E})$ est compact (car E est relativement compact).
Or $\overline{E(x)} \subset \overline{E}(x)$ et $\overline{E(x)}$ est fermé donc est compact.
– E est relativement compact donc E est précompact.
Soit $x \in X$, $\varepsilon > 0$ et $f_1, \ldots, f_N \in E$ tels que $E \subset \bigcup_{i=1}^{N} B(f_i, \varepsilon)$.
Pour tout i, f_i est continue en x donc :

$$\exists \eta_i > 0, \forall y \in X, d(x,y) < \eta_i \Rightarrow d'(f_i(x), f_i(y)) < \varepsilon$$

On pose $\eta := \min \eta_i$, alors :

$$\forall i, \forall y \in X, d(x,y) < \eta \Rightarrow d'(f_i(x), f_i(y)) < \varepsilon$$

Soit désormais $f \in E$, alors il existe i tel que $d_\infty(f, f_i) < \varepsilon$.
Soit $y \in X$ tel que $d(x,y) < \eta$, alors :

$$d'(f(x), f(y)) \leq d'(f(x), f_i(x)) + d'(f_i(x), f_i(y)) + d'(f_i(y), f(y)) < 3\varepsilon$$

Donc E est équicontinue.

$\Leftarrow$: Soit $(f_n)_{n\in\mathbb{N}}$ une suite d'éléments de E. Le but est de montrer qu'il existe une sous-suite de $(f_n)_n$ qui converge dans $(\mathcal{C}^0(X, X'), d_\infty)$.
X est compact donc X est séparable. Soit $D = \{x_k, k \in \mathbb{N}\}$ dense dans X.
E est ponctuellement relativement compact donc pour tout $k \in \mathbb{N}$, il existe $K_k \subset X'$ compact tel que $(f_n(x_k))_{n\in\mathbb{N}} \subset K_k$.
$(f_{n|D})_{n\in\mathbb{N}}$ est une suite de $\prod_{k\in\mathbb{N}} K_k$ compact par le théorème de Tykhonov, donc il existe une sous-suite $(f_{n_l})_{l\in\mathbb{N}}$ qui converge ponctuellement sur D.
Montrons que $(f_{n_l}(x))_{l\in\mathbb{N}}$ est de Cauchy pour tout $x \in X$.
Soit $\varepsilon > 0$, alors par équicontinuité de E il existe $\eta > 0$ tel que :

$$\forall x, y \in X, \forall l \in \mathbb{N}, d(x,y) < \eta \Rightarrow d'(f_{n_l}(x), f_{n_l}(y)) < \varepsilon$$

Soit $x \in X$, D est dense donc il existe k tel que $d(x, x_k) < \eta$. $(f_{n_l}(x_k))_{l\in\mathbb{N}}$ converge donc est de Cauchy :

$$\exists L_k, \forall l, l' \geq L_k, d'(f_{n_l}(x_k), f_{n_{l'}}(x_k)) < \varepsilon$$

D'où, pour tout $l, l' \geq L_k$,

$$\begin{aligned} d'(f_{n_l}(x), f_{n_{l'}}(x)) &\leq d'(f_{n_l}(x), f_{n_l}(x_k)) + d'(f_{n_l}(x_k), f_{n_{l'}}(x_k)) + d'(f_{n_{l'}}(x_k), f_{n_{l'}}(x)) \\ &< 3\varepsilon \end{aligned}$$

$(f_{n_l}(x))_{l\in\mathbb{N}}$ est de Cauchy et $\overline{E(x)}$ est compact donc complet, donc $(f_{n_l}(x))_{l\in\mathbb{N}}$ converge dans (X', d') vers $f(x)$ pour tout $x \in X$.
Montrons que la convergence est uniforme.
En conservant les notations précédentes, il existe $N \in \mathbb{N}$ tel que $X \subset \bigcup_{k=0}^{N} B(x_k, \eta)$.
On pose $L := \max_{0\leq k\leq N} L_k$, on a alors :

$$\forall l, l' \geq L, \forall x \in X, d'(f_{n_l}(x), f_{n_{l'}}(x)) < 3\varepsilon$$

En faisant tendre $l' \to \infty$, on obtient :

$$\forall l \geq L, d_\infty(f_{n_l}, f) < 3\varepsilon$$

□

3.9 Théorème d'échantillonnage de Shannon

Référence :
– [Wil95] page 126.
On définit, pour $u \in \mathcal{S}(\mathbb{R})$,

$$\hat{u}(y) = \int_{\mathbb{R}} u(x)e^{-2i\pi xy}\mathrm{d}x$$

la transformée de Fourier de u. Par densité de $\mathcal{S}(\mathbb{R})$ dans $L^2(\mathbb{R})$, on peut prolonger la transformée de Fourier à $L^2(\mathbb{R})$.
On définit :

$$BL^2 := \left\{u \in L^2(\mathbb{R}) \ / \ \text{supp } \hat{u} \subseteq \mathbb{I}\right\} \text{ où } \mathbb{I} := \left[-\frac{1}{2}, \frac{1}{2}\right]$$

On définit aussi le sinus-cardinal sur $\mathbb{R}$ par :

$$\text{sinc } x := \begin{cases} \frac{\sin \pi x}{\pi x} \text{ si } x \neq 0 \\ 1 \text{ sinon} \end{cases}$$

Théorème.
BL^2 vérifie les propriétés suivantes :

(i) BL^2 est un espace de Hilbert.

(ii) Tout $u \in BL^2$ possède un représentant dans $\mathcal{C}_0(\mathbb{R})$ (i.e. u est presque partout égale à une fonction de $\mathcal{C}_0(\mathbb{R})$).

(iii) La suite $(sinc(. - k))_{k\in\mathbb{Z}}$ est une base hilbertienne de BL^2.

(iv) Pour $u \in BL^2$,

$$u(x) = \sum_{k\in\mathbb{Z}} u(k)sinc(x - k),$$

la série convergeant uniformément et dans $L^2(\mathbb{R})$.

Lemme.
Si $u \in L^1(\mathbb{R})$, alors $\hat{u} \in \mathcal{C}_0(\mathbb{R})$ et :

$$\|\hat{u}\|_\infty \leq \|u\|_1$$

Démonstration. Soit $u \in L^1(\mathbb{R})$. Pour $y \in \mathbb{R}$, on a :

$$|\hat{u}(y)| \leq \int_{\mathbb{R}} |u(x)| \mathrm{d}x = \|u\|_1$$

donc $\|\hat{u}\|_\infty \leq \|u\|_1$.

Par densité de $\mathcal{D} := \{u \in \mathcal{C}^\infty(\mathbb{R}) \text{ / supp } u \text{ est compact}\}$ dans $L^1(\mathbb{R})$, il existe une suite (u_n) de $\mathcal{D}$ convergeant vers u dans $L^1(\mathbb{R})$. On a donc :

$$\|\hat{u} - \widehat{u_n}\|_\infty \leq \|u - u_n\|_1 \underset{n\to\infty}{\longrightarrow} 0$$

De plus, $u_n \in \mathcal{S}(\mathbb{R})$ donc $\widehat{u_n} \in \mathcal{S}(\mathbb{R}) \subseteq \mathcal{C}_0(\mathbb{R})$. Or $\mathcal{C}_0(\mathbb{R})$ est fermé dans $\mathcal{C}_b(\mathbb{R})$ donc $\hat{u} \in \mathcal{C}_0(\mathbb{R})$. □

Démonstration du théorème.

(i) Pour montrer que BL^2 est complet, il suffit de prouver que c'est un sous-espace fermé de $L^2(\mathbb{R})$.
Soit $(u_n)_n$ une suite de BL^2 convergeant vers u dans $L^2(\mathbb{R})$.
Par continuité de la transformée de Fourier dans $L^2(\mathbb{R})$, $(\widehat{u_n})_n$ converge vers $\hat{u}$ dans $L^2(\mathbb{R})$, donc en particulier dans $L^2(\Omega)$ où $\Omega := \mathbb{R} \setminus \mathbb{I}$.
Par définition de BL^2, $\widehat{u_n}_{|\Omega} = 0$, donc $\hat{u}_{|\Omega} = 0$ et $u \in BL^2$.

(ii) Soit $u \in BL^2$. Par définition, $\hat{u} \in L^2(\mathbb{I})$ donc $\hat{u} \in L^1(\mathbb{I})$ ($\mathbb{I}$ de mesure finie).
$\hat{u} = 0$ en dehors de $\mathbb{I}$ donc $\hat{u} \in L^1(\mathbb{R})$.
Par inversion de Fourier, on a alors :

$$\begin{aligned} u(x) &= \int_{\mathbb{R}} \hat{u}(y) e^{2i\pi xy} \mathrm{d}y \qquad \text{p.p.} \\ &= \int_{\mathbb{I}} \hat{u}(y) e^{2i\pi xy} \mathrm{d}y \qquad \text{p.p.} \end{aligned}$$

Par le lemme, u a un représentant dans $\mathcal{C}_0(\mathbb{R})$.
On déduit aussi de l'inégalité de Cauchy-Schwarz et de l'égalité de Plancherel que, pour $x \in \mathbb{R}$,

$$|u(x)| \leq \|\hat{u}\|_{L^2(\mathbb{I})} = \|\hat{u}\|_{L^2(\mathbb{R})} = \|u\|_{L^2(\mathbb{R})}$$

donc

$$\|u\|_\infty \leq \|u\|_2$$

(iii) Posons

$$e_k(x) := \begin{cases} e^{2i\pi kx} \text{ si } |x| \leq 1/2 \\ 0 \text{ sinon} \end{cases}$$

On remarque que $\widehat{e_k}(y) = \text{sinc}(y-k)$.
D'où, par conservation du produit scalaire,

$$\int_{\mathbb{R}} \text{sinc}(x-j)\ \text{sinc}(x-k)\mathrm{d}x = \int_{\mathbb{R}} e_j\overline{e_k} = \int_{\mathbb{I}} e_j\overline{e_k} = \delta_{j,k}$$

La suite $(\text{sinc}(.-k))_{k\in\mathbb{Z}}$ est donc orthonormée.
Pour montrer que cette suite est une base hilbertienne de BL^2, il suffit désormais de montrer qu'elle est totale, donc de montrer que son orthogonal dans BL^2 est réduit à $\{0\}$.
Soit donc $u \in BL^2$ tel que pour tout $k \in \mathbb{Z}$,

$$\int_{\mathbb{R}} u(x)\ \text{sinc}(x-k)\mathrm{d}x = 0$$

On a alors :

$$0 = \int_{\mathbb{R}} u\widehat{e_k} = \int_{\mathbb{R}} \hat{u}e_k = \int_{\mathbb{I}} \hat{u}e_k \quad \forall k \in \mathbb{Z}$$

Donc $\hat{u}(y) = 0$ presque partout sur $\mathbb{I}$ car $(e_k)_{k\in\mathbb{Z}}$ est une base hilbertienne de $L^2(\mathbb{R})$. Par conséquent, $\hat{u} = 0$ donc $u = 0$ et $(\text{sinc}(.-k))_{k\in\mathbb{Z}}$ est totale.

(iv) Par (iii), on a, pour $u \in BL^2$ et $x \in \mathbb{R}$,

$$u(x) = \sum_{k\in\mathbb{Z}} \langle u,\ \text{sinc}(.-k)\rangle\ \text{sinc}(x-k)$$

la convergence étant uniforme par l'inégalité prouvée à la fin de (ii).
En particulier, pour $x = j \in \mathbb{Z}$, on a

$$u(j) = \langle u,\ \text{sinc}(.-j)\rangle$$

D'où le résultat recherché.

□

3.10 Théorème d'inversion locale

Référence :
– [Rou09] page 222.

Théorème.
Soit E, F deux espaces de Banach.
Soit U un voisinage ouvert d'un point $x_0 \in E$.
Soit $f : U \to F$ une application de classe $\mathcal{C}^1$.

Si $Df(x_0)$ est une bijection continue de E dans F, alors f est un $\mathcal{C}^1$-difféomorphisme d'un voisinage V de x_0 sur $f(V)$.

Démonstration. En posant $g(x) := (Df(x_0))^{-1}(f(x_0+x)-f(x_0))$, on se ramène au cas où $E = F, x_0 = f(x_0) = 0$ et $Df(0) = \mathrm{Id}$.

En effet :

$$\begin{aligned} Dg(0) &= D(Df(x_0))^{-1}(0) \circ Df(x_0) \\ &= Df(x_0)^{-1} \circ Df(x_0) \\ &= \mathrm{Id} \end{aligned}$$

On pose désormais $u(x) := f(x) - x$, u est de classe $\mathcal{C}^1$ et $Du(0) = 0$.

$z \mapsto Du(z)$ est continue (car u est $\mathcal{C}^1$) donc il existe $r > 0$ tel que :

$$\forall z \in B(0,r), \|Du(z)\| \leq \frac{1}{2}$$

On a :

$$u(y) - u(x) = \int_0^1 Du(x + t(y-x)).(y-x)\,\mathrm{dt}$$

donc $u_{|B(0,r)}$ est $\frac{1}{2}$-lipschitzienne.

Pour $x, y \in B(0,r)$, on a donc :

$$|f(x) - f(y)| = |x + u(x) - y - u(y)| \geq \frac{1}{2}|x-y|$$

Donc $f_{|B(0,r)}$ est injective.

Soit $a \in B(0, \frac{r}{2}), x \in B(0,r)$, on a :

$$\begin{aligned} |a - u(x)| &\leq |a| + |u(x) - u(0)| \\ &\leq |a| + \frac{1}{2}|x| \\ &\leq r \end{aligned}$$

Donc l'application $\frac{1}{2}$-lipschitzienne $x \mapsto a - u(x)$ envoie $B(0,r)$ dans elle-même et $B(0,r)$ est complet.

En appliquant le théorème du point fixe, il existe un unique $y \in B(0,r)$ tel que $a - u(y) = y$, c'est-à-dire $a = f(y)$.

On pose $W := B(0, \frac{r}{2})$ et $V := f^{-1}(W) \cap B(0,r)$, alors $f_{|V}$ est surjective dans W qui est un voisinage de 0, donc f est bijective sur un voisinage de 0.

Pour $z \in B(0,r), \|Du(z)\| \leq \frac{1}{2}$, donc la série $\sum_{k\geq 0}(-Du(z))^k$ converge vers l'inverse de $\mathrm{Id} + Du(z) = Df(z)$, donc $Df(z)$ est inversible pour $z \in B(0,r)$.

Montrons maintenant que f^{-1} est différentiable sur W.

Soit $y, y_0 \in W, x, x_0 \in V$ tels que $f(x) = y$ et $f(x_0) = y_0$.

Alors :

$$y - y_0 = f(x) - f(x_0) = Df(x_0).(x - x_0) + o(|x - x_0|)$$

Or :

$$\begin{aligned}|x - x_0| &= |f(x) - f(x_0) - (u(x) - u(x_0))| \\ &\leq |y - y_0| + \frac{1}{2}|x - x_0|\end{aligned}$$

Donc $|x - x_0| \leq 2|y - y_0|$, donc $|f^{-1}(y) - f^{-1}(y_0)| \leq 2|y - y_0|$, donc f^{-1} est lipschitzienne (et en particulier continue).

Donc $o(|x - x_0|) = o(|y - y_0|)$, d'où :

$$\begin{aligned}Df(x_0).(x - x_0) &= y - y_0 + o(|y - y_0|) \\ x - x_0 &= Df(x_0)^{-1}.(y - y_0) + o(|y - y_0|)\end{aligned}$$

Donc f^{-1} est différentiable en y_0 de différentielle $Df(x_0)^{-1}$.

Finalement, f^{-1} est de classe $\mathcal{C}^1$ sur W car Df^{-1} est la composée des applications continues suivantes :

$$y \mapsto f^{-1}(y) \mapsto Df(f^{-1}(y)) \mapsto Df(f^{-1}(y))^{-1} = Df^{-1}(y)$$

□

3.11 Théorème de Burnside

Référence :

– [FGN09a]

Un groupe G est dit d'exposant fini s'il existe $N \in \mathbb{N}^*$ tel que pour tout $g \in G, g^N = e$.

Théorème.
Soit G un sous-groupe de $GL_n(\mathbb{C})$. Alors G est fini si et seulement si G est d'exposant fini.

Lemme.
Soit $\mathbb{K}$ un sous-corps de $\mathbb{C}$. Soit $A \in \mathcal{M}_n(\mathbb{K})$ telle que $\forall k \geq 1, \mathrm{tr}(A^k) = 0$.
Alors A est nilpotente.

Démonstration. Supposons A non nilpotente. On note $\lambda_1, \ldots, \lambda_r$ ses valeurs propres complexes non nulles distinctes et $m_1, \ldots, m_r$ leurs multiplicités respectives.
Alors par trigonalisation de A sur $\mathbb{C}$, on a

$$\forall k \geq 1, \quad 0 = \mathrm{tr}(A^k) = \sum_{i=1}^{r} m_i \lambda_i^k.$$

On en déduit que $\begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix}$ est dans le noyau de la matrice de Vandermonde

$$\begin{pmatrix} \lambda_1 & \cdots & \lambda_r \\ \lambda_1^2 & \cdots & \lambda_r \\ \vdots & & \vdots \\ \lambda_1^r & \cdots & \lambda_r^r \end{pmatrix}.$$

Or les λ_i sont distincts, donc c'est absurde. □

Démonstration du théorème. $\Rightarrow$: Par le théorème de Lagrange.

$\Leftarrow$: Soit $(M_1, \ldots, M_m)$ une base du sous-espace vectoriel $\langle G \rangle_{\mathbb{C}}$ de $\mathcal{M}_n(\mathbb{C})$, avec $M_i \in G$. Considérons

$$\begin{aligned} f : G &\longrightarrow \mathbb{C}^m \\ A &\longmapsto (\mathrm{tr}(AM_i))_{1 \leq i \leq m} \end{aligned}$$

Montrons que f est injective. Soit $A, B \in G$ tels que $f(A) = f(B)$. Alors

$$\forall M \in \langle G \rangle_{\mathbb{C}}, \quad \mathrm{tr}(AM) = \mathrm{tr}(BM)$$

par linéarité de la trace. En posant $D := AB^{-1} \in G$, on a, pour $k \geq 1$,

$$\begin{aligned} \mathrm{tr}(D^k) &= \mathrm{tr}(AB^{-1}D^{k-1}) \\ &= \mathrm{tr}(BB^{-1}D^{k-1}) \\ &= \mathrm{tr}(D^{k-1}) \\ &= \mathrm{tr}(I_n) \quad \text{par récurrence} \\ &= n. \end{aligned}$$

D'où

$$\begin{aligned} \mathrm{tr}((D - I_n)^k) &= \mathrm{tr}\left(\sum_{j=0}^{k} \binom{k}{j} (-1)^j D^{k-j} \right) \\ &= \sum_{j=0}^{k} \binom{k}{j} (-1)^j \mathrm{tr}(D^{k-j}) \\ &= n(1-1)^k = 0. \end{aligned}$$

Donc $D - I_n$ est nilpotente par le lemme.
Or G est d'exposant fini donc toutes ses matrices sont diagonalisables, donc D est diagonalisable et $D - I_n$ aussi. $D - I_n$ étant nilpotente, $D = I_n$ et donc $A = B$. f est donc injective.
Les valeurs propres d'éléments de G sont racines de $X^N - 1$ donc sont en nombre fini, donc les traces d'éléments de G sont en nombre fini. Donc $f(G)$ est fini et donc G aussi par injectivité de f.

□

3.12 Théorème des fonctions implicites

Référence :
– [Rou09] page 259.
Dans toute la suite, on note $B_r := B(0,r) \subset \mathbb{R}^n$ et $B_s := B(0,s) \subset \mathbb{R}^p$.

Théorème.
Soit U un voisinage ouvert de $(0,0)$ dans $\mathbb{R}^n \times \mathbb{R}^p$.
Soit $f : (x,y) \mapsto f(x,y)$ une application de classe $\mathcal{C}^1$ de U dans $\mathbb{R}^p$.
On suppose $f(0,0) = 0$ et $D_y f(0,0)$ inversible.
Alors il existe $r > 0, s > 0$ et un unique $\varphi : B_r \to B_s$ tels que :

$$(x \in B_r, y \in B_s, f(x,y) = 0) \iff (x \in B_r, y = \varphi(x))$$

De plus, φ est de classe $\mathcal{C}^1$ sur B_r.

Démonstration. On note $A := D_y f(0,0)$ et $F_x(y) := y - A^{-1} f(x,y)$. On a :

$$DF_x(y) = \mathrm{Id} - A^{-1} D_y f(x,y)$$

Donc $DF_0(0) = 0$ et $(x,y) \mapsto DF_x(y)$ est continue en x et y, donc, pour des certains $r > 0$ et $s > 0$, on a $\|DF_x(y)\| \leq \frac{1}{2}$ pour $x \in B_r, y \in B_s$.

On a :

$$F_x(y) = F_x(0) + (F_x(y) - F_x(0))$$

Donc par l'inégalité des accroissement finis, pour $x \in B_s, y \in B_r$, on a :

$$\|F_x(y)\| \leq \|F_x(0)\| + \frac{1}{2}\|y\|$$

et $x \mapsto F_x(0)$ est continue donc, quitte à diminuer r, on a :

$$\|F_x(y)\| < s$$

Donc $F_x(\overline{B_s}) \subset B_s$ pour $x \in B_r$.

$\overline{B_s}$ est complet donc, d'après le théorème du point fixe, il existe un unique $y \in \overline{B_s}$ tel que $F_x(y) = y$, *i.e.* $f(x,y) = 0$ et $y \in B_s$ car $F_x(y) = y$ et $F_x(\overline{B_s}) \subset B_s$.

Donc on a bien ce qu'on voulait en posant $\varphi(x) = y$.

Montrons que φ est de classe $\mathcal{C}^1$. Soit $x, x_0 \in B_r$, on pose $y = \varphi(x), y_0 = \varphi(x_0)$, on a :

$$\begin{aligned} y - y_0 &= F_x(y) - F_{x_0}(y_0) \\ &= (F_x(y) - F_x(y_0)) + (F_x(y_0) - F_{x_0}(y_0)) \\ &= F_x(y) - F_x(y_0) - A^{-1}(f(x,y_0) - f(x_0,y_0)) \end{aligned}$$

On a :

$$\|F_x(y) - F_x(y_0)\| \leq \frac{1}{2}\|y - y_0\|$$

et :

$$\|f(x,y_0)-f(x_0,y_0)\| \leq M\|x-x_0\|$$

où $M = \max_{\|x\|\leq r} \|D_x f(x,y_0)\|$, d'où :

$$\|y-y_0\| \leq 2M\|A^{-1}\|\|x-x_0\|$$

i.e.

$$\|\varphi(x)-\varphi(x_0)\| \leq C\|x-x_0\|$$

Donc φ est lipschitzienne donc continue sur B_r.

$\|DF_x(y)\| \leq \frac{1}{2}$ donc $\sum_{k\geq 0}(DF_x(y))^k$ converge vers l'inverse de $\mathrm{Id} - DF_x(y)$, *i.e.* l'inverse de $A^{-1}D_y f(x,y)$, donc $D_y f(x,y)$ est inversible.

f est différentiable en (x_0,y_0) donc :

$$0 = f(x,y)-f(x_0,y_0) = D_x f(x_0,y_0).(x-x_0)+D_y f(x_0,y_0)+o(\|x-x_0\|+\|y-y_0\|)$$

De plus, φ est lipschitzienne donc $o(\|x-x_0\|+\|y-y_0\|) = o(\|x-x_0\|)$. D'où :

$$\varphi(x)-\varphi(x_0) = -D_y f(x_0,y_0)^{-1} \circ D_x f(x_0,y_0).(x-x_0) + o(\|x-x_0\|)$$

□

3.13 Théorème taubérien fort

Référence :

– [Gou08] page 289.

Théorème.
Soit $(a_n) \in \mathbb{R}^{\mathbb{N}}$ telle que $a_n = O(\frac{1}{n})$.

On suppose que la série entière $\sum a_n z^n$ a un rayon de convergence ≥ 1 et que sa somme F vérifie $\lim_{x\to 1^-} F(x) = l < \infty$.

Alors $\sum a_n$ converge et $\sum_{n=0}^{+\infty} a_n = l$.

Démonstration. Quitte à remplacer a_0 par $a_0 - l$ on peut supposer $l = 0$.

On considère

$$\Phi := \left\{ \varphi : [0,1] \to \mathbb{R} \mid \forall x \in [0,1[, \sum_{n\geq 0} a_n \varphi(x^n) \text{ converge et } \lim_{x\to 1^-} \sum_{n=0}^{+\infty} a_n \varphi(x^n) = 0 \right\}.$$

On introduit la fonction $g : [0,1] \to \mathbb{R}$ définie par $g(x) := \mathbf{1}_{[\frac{1}{2},1]}(x)$.

Le but est de montrer que $g \in \Phi$. En effet, on a $x^n < \frac{1}{2}$ dès que $n > -\frac{\ln 2}{\ln x}$. En notant $N_x := \left\lfloor -\frac{\ln 2}{\ln x} \right\rfloor$, on a

$$\forall x \in [0,1[, \quad \sum_{n=0}^{+\infty} a_n g(x^n) = \sum_{n=0}^{N_x} a_n$$

et $\lim_{x\to 1^-} N_x = +\infty$. On a notamment la convergence de $\sum a_n g(x^n)$ pour $x \in [0,1[$.

Nous allons d'abord montrer que toute fonction polynôme s'annulant en 0 est élément de Φ, puis nous encadrerons g par deux fonctions polynômes proches en norme 1. Nous en déduirons le résultat après un travail éprouvant de majoration de $\sum a_n g(x^n)$ au voisinage de 1.

• Pour montrer que $X\mathbb{R}[X] \subset \Phi$, il suffit de le vérifier pour tout monôme $X^k, k \geq 1$.

$\sum a_n (x^k)^n$ converge pour $x \in [0,1[$ et de plus

$$\forall x \in [0,1[, \quad \sum_{n=0}^{+\infty} a_n (x^n)^k = F(x^k) \quad \text{donc} \quad \lim_{x\to 1^-} \sum_{n=0}^{+\infty} a_n (x^n)^k = 0.$$

• On veut encadrer g par deux polynômes P_i tels que $P_i(0) = 0$ et $P_i(1) = 1$. On écrit donc g sous la forme $g(x) = x + x(1-x)h(x)$, ce qui revient à considérer

$$h(x) := \frac{g(x) - x}{x(1-x)} = \begin{cases} \frac{1}{x-1} & \text{si } 0 \leq x < \frac{1}{2} \\ \frac{1}{x} & \text{sinon.} \end{cases}$$

Soit $\varepsilon > 0$. Il existe s_1 et s_2 deux fonctions continues telles que $s_1 \leq h \leq s_2$ et $\int_0^1 s_2 - s_1 < \varepsilon$. De plus, par le théorème de Weierstrass, il existe deux polynômes t_1 et t_2 tels que $|t_i - s_i| < \varepsilon$ sur $[0,1]$. En posant $u_1 := t_1 - \varepsilon$ et $u_2 := t_2 + \varepsilon$, on a alors $u_1 \leq h \leq u_2$ et

$$\int_0^1 u_2 - u_1 = \int_0^1 t_2 - t_1 + 2\varepsilon \leq \int_0^1 s_2 - s_1 + 4\varepsilon < 5\varepsilon.$$

On définit maintenant les deux polynômes $p_i(x) := x + x(1-x)u_i(x)$.

On a alors $p_i(0) = 0, p_i(1) = 1$ et $p_1 \leq g \leq p_2$. De plus,

$$\text{le polynôme} \quad q(x) := \frac{p_2(x) - p_1(x)}{x(1-x)} = u_2(x) - u_1(x) \quad \text{vérifie} \quad \int_0^1 q < 5\varepsilon.$$

• $a_n = O(\frac{1}{n})$ donc il existe $M > 0$ tel que $|a_n| \leq \frac{M}{n}$ pour tout n. Comme $p_1 \leq g \leq p_2$, on a par ailleurs pour tout $x \in [0,1[$

$$\begin{aligned} \left| \sum_{n=0}^{+\infty} a_n g(x^n) - \sum_{n=0}^{+\infty} a_n p_1(x^n) \right| &\leq \sum_{n=1}^{+\infty} |a_n| (p_2 - p_1)(x^n) \\ &\leq M \sum_{n=1}^{+\infty} \frac{x^n(1-x^n)}{n} q(x^n) \\ &\leq M(1-x) \sum_{n=0}^{+\infty} x^n q(x^n) \end{aligned}$$

car $1 - x^n = (1-x)(1 + \cdots + x^{n-1}) \leq n(1-x)$.

D'où

$$\left|\sum_{n=0}^{+\infty} a_n g(x^n)\right| \leq \left|\sum_{n=0}^{+\infty} a_n p_1(x^n)\right| + M(1-x)\sum_{n=0}^{+\infty} x^n q(x^n).$$

Or $p_1 \in \Phi$ donc

$$\exists \lambda \in [0,1[, \forall x \in [\lambda, 1[, \quad \left|\sum_{n=0}^{+\infty} a_n p_1(x^n)\right| < \varepsilon.$$

D'où, pour $x \in [\lambda, 1[$,

$$\left|\sum_{n=0}^{+\infty} a_n g(x^n)\right| < \varepsilon + M(1-x)\sum_{n=0}^{+\infty} x^n q(x^n).$$

Pour conclure, on a le lemme suivant :

Lemme.
Soit $f \in \mathbb{R}[X]$, alors

$$(1-x)\sum_{n=0}^{+\infty} x^n f(x^n) \xrightarrow[x\to 1^-]{} \int_0^1 f.$$

En effet, avec ce résultat, on aura

$$(1-x)\sum_{n=0}^{+\infty} x^n q(x^n) \xrightarrow[x\to 1^-]{} \int_0^1 q < 5\varepsilon$$

ce qui terminera la preuve du théorème.

Démonstration du lemme. On peut se limiter au cas où $f(x) = x^k$ par linéarité. On a alors pour $x \in [0,1[$

$$\begin{aligned}(1-x)\sum_{n=0}^{+\infty} x^n f(x^n) &= (1-x)\sum_{n=0}^{+\infty} (x^{k+1})^n \\ &= \frac{1-x}{1-x^{k+1}} \\ &= \frac{1}{1+\cdots+x^k} \xrightarrow[x\to 1^-]{} \frac{1}{k+1} = \int_0^1 t^k \mathrm{d}t\end{aligned}$$

□

□

Bibliographie

[Ale99] Michel Alessandri. *Thèmes de géométrie : groupes en situation géométrique*. Dunod, 1999.

[BMP05] Vincent Beck, Jérome Malick, and Gabriel Peyré. *Objectif Agrégation*. H&K, 2005.

[BP06] Marc Briane and Gilles Pagès. *Théorie de l'intégration (4e édition)*. Vuibert, 2006.

[Bre05] Haïm Brezis. *Analyse fonctionnelle*. Dunod, 2005.

[Car89] Jean-Claude Carrega. *Théorie des corps : la règle et le compas*. Hermann, 1989.

[CGCDM11] Marie Cottrell, Valentin Genon-Catalot, Christian Duhamel, and Thierry Meyre. *Exercices de probabilités*. Cassini, 2011.

[CL05] Antoine Chambert-Loir. *Algèbre corporelle*. Les éditions de l'école Polytechnique, 2005.

[Cog02] Michel Cognet. *Algèbre bilinéaire*. Bréal, 2002.

[Dem06] Jean-Pierre Demailly. *Analyse numérique et équations différentielles*. EDP Sciences, 2006.

[Esc04] Jean-Pierre Escofier. *Théorie de Galois*. Dunod, 2004.

[FGN03] Serge Francinou, Hervé Gianella, and Serge Nicolas. *Oraux X – ENS Analyse 1*. Cassini, 2003.

[FGN07] Serge Francinou, Hervé Gianella, and Serge Nicolas. *Oraux X – ENS Algèbre 1 (2e édition)*. Cassini, 2007.

[FGN08] Serge Francinou, Hervé Gianella, and Serge Nicolas. *Oraux X – ENS Algèbre 3*. Cassini, 2008.

[FGN09a] Serge Francinou, Hervé Gianella, and Serge Nicolas. *Oraux X – ENS Algèbre 2*. Cassini, 2009.

[FGN09b] Serge Francinou, Hervé Gianella, and Serge Nicolas. *Oraux X – ENS Analyse 2*. Cassini, 2009.

[FGN12] Serge Francinou, Hervé Gianella, and Serge Nicolas. *Oraux X – ENS Analyse 4*. Cassini, 2012.

[Gob98] Rémi Goblot. *Thèmes de géométrie*. Masson, 1998.

[Gou94] Xavier Gourdon. *Analyse*. Ellipses, 1994.

[Gou08] Xavier Gourdon. *Analyse (2e édition)*. Ellipses, 2008.

[Gou09] Xavier Gourdon. *Algèbre (2e édition)*. Ellipses, 2009.

[GT98] Stéphane Gonnord and Nicolas Tosel. *Calcul différentiel*. Ellipses, 1998.

[Lei99a] Eric Leichtnam. *Exercices d'oraux X-ENS : tome Algèbre et géométrie*. Ellipses, 1999.

[Lei99b] Eric Leichtnam. *Exercices d'oraux X-ENS : tome Analyse*. Ellipses, 1999.

[Mér06] Jean-Yves Mérindol. *Nombres et algèbre*. EDP Sciences, 2006.

[MT94] Rached Mneimné and Frédéric Testard. *Introduction à la théorie des groupes de Lie classiques*. Hermann, 1994.

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

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

[QZ06] Hervé Queffélec and Claude Zuily. *Analyse pour l'agrégation (3e édition)*. Dunod, 2006.

[Rou09] François Rouvière. *Petit guide de calcul différentiel à l'usage de la licence et de l'agrégation (3e édition)*. Cassini, 2009.

[RWM10] Jean-Pierre Ramis, André Warusfel, and François Moulin. *Cours de mathématiques pures et appliquées – Volume 1*. De Boeck, 2010.

[SP99] Philippe Saux Picart. *Cours de calcul formel : Algorithmes fondamentaux*. Ellipses, 1999.

[Tau05] Patrice Tauvel. *Géométrie*. Dunod, 2005.

[Ulm12] Felix Ulmer. *Théorie des groupes*. Ellipses, 2012.

[Wil95] Michel Willem. *Analyse harmonique réelle*. Hermann, 1995.

[Zav13] Maxime Zavidovique. *Un Max de Maths*. Calvage & Mounet, 2013.